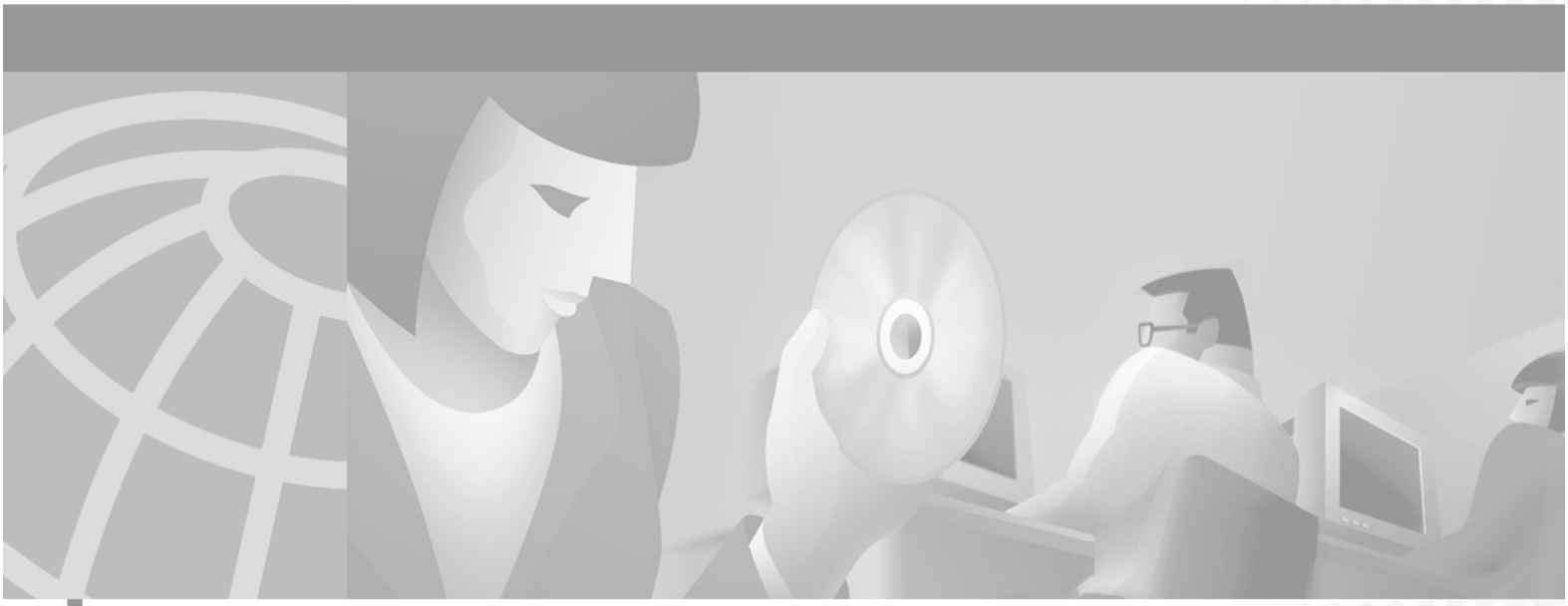


Catalyst 6000 Family Command Reference

Release 7.1

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

Customer Order Number: DOC-7813563=
Text Part Number: 78-13563-01

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

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

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

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

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

AccessPath, AtmDirector, Browse with Me, CCIP, CCSI, CD-PAC, *CiscoLink*, the Cisco *Powered* Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Cisco Unity, Fast Step, Follow Me Browsing, FormShare, FrameShare, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, ScriptBuilder, ScriptShare, SMARTnet, TransPath, Voice LAN, Wavelength Router, and WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and Discover All That's Possible are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, GigaStack, IOS, IP/TV, LightStream, MICA, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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. (0110R)

Catalyst 6000 Family Command Reference
Copyright © 1999–2001, Cisco Systems, Inc.
All rights reserved.

CONTENTS

Preface xxiii

- Audience xxiii
- Organization xxiii
- Related Documentation xxiii
- Conventions xxiv
- Obtaining Documentation xxv
  - World Wide Web xxv
  - Documentation CD-ROM xxv
  - Ordering Documentation xxv
  - Documentation Feedback xxv
- Obtaining Technical Assistance xxvi
  - Cisco.com xxvi
  - Technical Assistance Center xxvi

CHAPTER 1

Command-Line Interfaces 1-1

- Switch CLI 1-1
  - Accessing the Switch CLI 1-1
  - Operating the Switch CLI 1-3
- ROM Monitor CLI 1-13
  - Accessing the ROM Monitor CLI 1-13
  - Operating the ROM Monitor CLI 1-13

CHAPTER 2

Catalyst 6000 Family Switch and ROM Monitor Commands 2-1

- alias 2-2
- boot 2-4
- cd 2-5
- clear alias 2-6
- clear arp 2-7
- clear banner motd 2-8
- clear boot auto-config 2-9
- clear boot device 2-10
- clear boot system 2-11
- clear cam 2-12

clear channel statistics 2-13
clear config 2-14
clear config pvlan 2-16
clear cops 2-17
clear counters 2-19
clear crypto key rsa 2-20
clear dot1x config 2-21
clear gmrp statistics 2-22
clear gvrp statistics 2-23
clear igmp statistics 2-24
clear ip alias 2-25
clear ip dns domain 2-26
clear ip dns server 2-27
clear ip permit 2-28
clear ip route 2-30
clear kerberos clients mandatory 2-31
clear kerberos credentials forward 2-32
clear kerberos creds 2-33
clear kerberos realm 2-34
clear kerberos server 2-35
clear key config-key 2-36
clear lacp-channel statistics 2-37
clear lda 2-38
clear log 2-40
clear log command 2-41
clear logging buffer 2-42
clear logging level 2-43
clear logging server 2-45
clear mls cef 2-46
clear mls entry 2-47
clear mls entry cef adjacency 2-49
clear mls exclude protocol 2-50
clear mls multicast statistics 2-51
clear mls nde flow 2-52
clear mls statistics 2-53

clear mls statistics entry 2-55
clear module password 2-57
clear multicast router 2-58
clear ntp server 2-59
clear ntp timezone 2-60
clear pbf 2-61
clear port broadcast 2-62
clear port cops 2-63
clear port host 2-64
clear port qos cos 2-65
clear port security 2-66
clear pvlan mapping 2-67
clear qos acl 2-68
clear qos config 2-70
clear qos cos-dscp-map 2-71
clear qos dscp-cos-map 2-72
clear qos ipprec-dscp-map 2-73
clear qos mac-cos 2-74
clear qos map 2-75
clear qos policed-dscp-map 2-77
clear qos policer 2-78
clear qos statistics 2-80
clear radius 2-81
clear rcp 2-82
clear rgmp statistics 2-83
clear security acl 2-84
clear security acl capture-ports 2-86
clear security acl log flow 2-87
clear security acl map 2-88
clear snmp access 2-90
clear snmp community 2-91
clear snmp group 2-92
clear snmp notify 2-93
clear snmp targetaddr 2-94
clear snmp targetparams 2-95

clear snmp trap 2-96
clear snmp user 2-97
clear snmp view 2-98
clear spantree mst 2-99
clear spantree portcost 2-100
clear spantree portinstancecost 2-101
clear spantree portinstancepri 2-103
clear spantree portpri 2-104
clear spantree portvlancost 2-105
clear spantree portvlanpri 2-107
clear spantree root 2-108
clear spantree statistics 2-110
clear spantree uplinkfast 2-112
clear tacacs key 2-113
clear tacacs server 2-114
clear timezone 2-115
clear top 2-116
clear trunk 2-117
clear vlan 2-118
clear vlan counters 2-119
clear vlan mapping 2-120
clear vmps rcp 2-122
clear vmps server 2-123
clear vmps statistics 2-124
clear vtp pruneeligible 2-125
clear vtp statistics 2-126
commit 2-127
commit lda 2-129
configure 2-130
confreg 2-132
context 2-134
copy 2-136
delete 2-142
dev 2-143
dir—ROM monitor 2-144

dir—switch 2-145
disable 2-147
disconnect 2-148
download 2-149
enable 2-153
format 2-154
frame 2-156
history—ROM monitor 2-157
history—switch 2-158
l2trace 2-159
meminfo 2-162
ping 2-163
pwd 2-166
quit 2-167
reconfirm vmps 2-168
reload 2-169
repeat 2-170
reset—ROM monitor 2-172
reset—switch 2-173
restore counters 2-177
rollback 2-178
session 2-179
set 2-180
set accounting commands 2-181
set accounting connect 2-182
set accounting exec 2-183
set accounting suppress 2-185
set accounting system 2-186
set accounting update 2-188
set aclmerge algo 2-189
set aclmerge bdd 2-190
set alias 2-191
set arp 2-192
set authentication enable 2-194
set authentication login 2-196

set authorization commands 2-198
set authorization enable 2-200
set authorization exec 2-202
set banner lcd 2-204
set banner motd 2-205
set boot auto-config 2-206
set boot config-register 2-207
set boot config-register auto-config 2-210
set boot device 2-213
set boot sync now 2-215
set boot system flash 2-216
set cam 2-217
set cdp 2-219
set channelprotocol 2-221
set channel vlancost 2-223
set config acl nvram 2-225
set config mode 2-226
set cops 2-227
set crypto key rsa 2-229
set default portstatus 2-231
set dot1q-all-tagged 2-232
set dot1x 2-234
set enablepass 2-237
set errdisable-timeout 2-238
set errordetection 2-240
set feature agg-link-partner 2-242
set feature mdg 2-243
set garp timer 2-244
set gmrp 2-245
set gmrp fwdall 2-246
set gmrp registration 2-247
set gmrp timer 2-248
set gvrp 2-250
set gvrp applicant 2-251
set gvrp dynamic-vlan-creation 2-252

set gvrp registration 2-253
set gvrp timer 2-255
set igmp 2-257
set igmp fastleave 2-258
set igmp mode 2-259
set igmp querier 2-260
set igmp ratelimit 2-261
set inlinepower defaultallocation 2-263
set interface 2-264
set ip alias 2-267
set ip dns 2-268
set ip dns domain 2-269
set ip dns server 2-270
set ip fragmentation 2-271
set ip http port 2-272
set ip http server 2-273
set ip permit 2-274
set ip redirect 2-276
set ip route 2-277
set ip unreachable 2-279
set kerberos clients mandatory 2-280
set kerberos credentials forward 2-281
set kerberos local-realm 2-282
set kerberos realm 2-283
set kerberos server 2-284
set kerberos srvtab entry 2-285
set kerberos srvtab remote 2-287
set key config-key 2-288
set lacp-channel system-priority 2-289
set lcperroraction 2-290
set lda 2-291
set length 2-294
set logging buffer 2-295
set logging console 2-296
set logging history 2-297

set logging level 2-298
set logging server 2-301
set logging session 2-303
set logging telnet 2-304
set logging timestamp 2-305
set logout 2-307
set mls agingtime 2-308
set mls cef load-balance 2-310
set mls exclude protocol 2-311
set mls flow 2-312
set mls nde 2-314
set mls statistics protocol 2-318
set mls verify 2-319
set module 2-321
set module name 2-323
set module power 2-324
set module shutdown 2-325
set msfcautostate 2-326
set msmautostate 2-328
set multicast router 2-329
set ntp broadcastclient 2-330
set ntp broadcastdelay 2-331
set ntp client 2-332
set ntp server 2-333
set ntp summertime 2-334
set ntp timezone 2-336
set password 2-337
set pbf 2-338
set port auxiliaryvlan 2-340
set port broadcast 2-342
set port channel 2-344
set port cops 2-347
set port debounce 2-348
set port disable 2-350
set port dot1qtunnel 2-351

set port dot1x 2-353
set port duplex 2-355
set port enable 2-356
set port flowcontrol 2-357
set port gmrp 2-360
set port gvrp 2-361
set port host 2-363
set port inlinepower 2-364
set port jumbo 2-365
set port lacp-channel 2-366
set port membership 2-368
set port name 2-370
set port negotiation 2-371
set port protocol 2-372
set port qos 2-374
set port qos cos 2-376
set port qos policy-source 2-377
set port qos trust 2-379
set port qos trust-ext 2-381
set port rsvp dsbm-election 2-382
set port security 2-383
set port speed 2-385
set port sync-restart-delay 2-386
set port trap 2-387
set port voice interface dhcp 2-388
set power redundancy 2-390
set prompt 2-391
set protocolfilter 2-392
set pvlan 2-393
set pvlan mapping 2-395
set qos 2-397
set qos acl default-action 2-398
set qos acl ip 2-400
set qos acl ipx 2-405
set qos acl mac 2-408

set qos acl map 2-410
set qos bridged-microflow-policing 2-412
set qos cos-dscp-map 2-413
set qos drop-threshold 2-414
set qos dscp-cos-map 2-416
set qos ipprec-dscp-map 2-417
set qos mac-cos 2-419
set qos map 2-420
set qos policed-dscp-map 2-423
set qos policer 2-424
set qos policy-source 2-426
set qos rsvp 2-428
set qos rxq-ratio 2-430
set qos statistics export 2-431
set qos statistics export aggregate 2-432
set qos statistics export destination 2-433
set qos statistics export interval 2-434
set qos statistics export port 2-435
set qos txq-ratio 2-436
set qos wred 2-437
set qos wrr 2-439
set radius deadtime 2-441
set radius key 2-442
set radius retransmit 2-443
set radius server 2-444
set radius timeout 2-446
set rcp username 2-447
set rgmp 2-448
set rspan 2-449
set security acl adjacency 2-452
set security acl capture-ports 2-453
set security acl ip 2-454
set security acl ipx 2-459
set security acl log 2-462
set security acl mac 2-463

set security acl map 2-465
set snmp access 2-467
set snmp community 2-469
set snmp extendedrmon netflow 2-471
set snmp group 2-472
set snmp notify 2-473
set snmp rmon 2-474
set snmp rmonmemory 2-475
set snmp targetaddr 2-476
set snmp targetparams 2-478
set snmp trap 2-480
set snmp user 2-483
set snmp view 2-485
set span 2-487
set spantree backbonefast 2-490
set spantree bpdu-skewing 2-491
set spantree channelcost 2-492
set spantree channelvlancost 2-494
set spantree defaultcostmode 2-495
set spantree disable 2-497
set spantree enable 2-499
set spantree fwddelay 2-501
set spantree global-default 2-503
set spantree guard 2-505
set spantree hello 2-507
set spantree macreduction 2-509
set spantree maxage 2-510
set spantree mode 2-512
set spantree mst config 2-514
set spantree mst link-type 2-516
set spantree mst maxhops 2-517
set spantree mst redetect-protocol 2-518
set spantree mst vlan 2-519
set spantree portcost 2-520
set spantree portfast 2-522

set spantree portfast bpdu-filter 2-524
set spantree portfast bpdu-guard 2-525
set spantree portinstancecost 2-526
set spantree portinstancepri 2-528
set spantree portpri 2-530
set spantree portvlancost 2-531
set spantree portvlanpri 2-533
set spantree priority 2-534
set spantree root 2-536
set spantree uplinkfast 2-539
set summertime 2-541
set system baud 2-543
set system contact 2-544
set system core-dump 2-545
set system core-file 2-547
set system countrycode 2-548
set system crossbar-fallback 2-549
set system highavailability 2-550
set system highavailability versioning 2-551
set system location 2-553
set system modem 2-554
set system name 2-555
set system switchmode 2-556
set tacacs attempts 2-558
set tacacs directedrequest 2-559
set tacacs key 2-560
set tacacs server 2-561
set tacacs timeout 2-562
set test diaglevel 2-563
set time 2-564
set timezone 2-565
set traffic monitor 2-566
set trunk 2-567
set udld 2-570
set udld aggressive-mode 2-572

set udld interval 2-573
set vlan 2-574
set vlan mapping 2-578
set vmps downloadmethod 2-580
set vmps downloadserver 2-581
set vmps server 2-582
set vmps state 2-584
set vtp 2-585
set vtp pruneeligible 2-587
show accounting 2-588
show aclmerge 2-591
show alias 2-592
show arp 2-593
show authentication 2-594
show authorization 2-595
show banner 2-596
show boot 2-597
show boot device 2-598
show cam 2-599
show cam agingtime 2-601
show cam count 2-602
show cam msfc 2-603
show cdp 2-604
show channel 2-607
show channel group 2-612
show channel hash 2-616
show channel mac 2-617
show channelprotocol 2-618
show channel traffic 2-619
show config 2-620
show config mode 2-626
show config qos acl 2-627
show cops 2-628
show counters 2-631
show crypto key 2-637

show default 2-638
show dot1q-all-tagged 2-639
show dot1x 2-640
show dvlan statistics 2-641
show environment 2-642
show errdisable-timeout 2-646
show errordetection 2-647
show fabric channel 2-648
show file 2-651
show flash 2-652
show garp timer 2-655
show gmrp configuration 2-656
show gmrp statistics 2-657
show gmrp timer 2-658
show gvrp configuration 2-659
show gvrp statistics 2-661
show ifindex 2-663
show igmp mode 2-664
show igmp ratelimit-info 2-665
show igmp statistics 2-666
show imagemib 2-668
show interface 2-669
show ip alias 2-671
show ip dns 2-672
show ip http 2-673
show ip permit 2-675
show ip route 2-677
show kerberos 2-679
show lacp-channel 2-681
show lcperroraction 2-685
show lda 2-686
show log 2-690
show log command 2-692
show logging 2-693
show logging buffer 2-695

show mac 2-696
show microcode 2-699
show mls 2-700
show mls acl-route 2-702
show mls cef interface 2-703
show mls cef mac 2-705
show mls cef summary 2-707
show mls entry 2-709
show mls entry cef 2-715
show mls entry netflow-route 2-719
show mls exclude protocol 2-721
show mls multicast 2-722
show mls nde 2-727
show mls netflow-route 2-728
show mls statistics 2-729
show mls verify 2-732
show module 2-733
show moduleinit 2-736
show msfcautostate 2-738
show msmautostate 2-739
show multicast group 2-740
show multicast group count 2-742
show multicast protocols status 2-743
show multicast router 2-744
show netstat 2-746
show ntp 2-753
show pbf 2-755
show port 2-758
show port auxiliaryvlan 2-766
show port broadcast 2-768
show port capabilities 2-769
show port cdp 2-773
show port channel 2-775
show port cops 2-781
show port counters 2-783

show port debounce 2-785
show port dot1qtunnel 2-786
show port dot1x 2-787
show port flowcontrol 2-789
show port inlinepower 2-791
show port jumbo 2-792
show port lacp-channel 2-793
show port mac 2-796
show port mac-address 2-798
show port negotiation 2-800
show port protocol 2-801
show port qos 2-802
show port rsvp 2-804
show port security 2-805
show port spantree 2-807
show port status 2-808
show port sync-restart-delay 2-809
show port trap 2-810
show port trunk 2-811
show port voice 2-813
show port voice active 2-816
show port voice fdl 2-820
show port voice interface 2-822
show proc 2-823
show protocolfilter 2-827
show pvlan 2-828
show pvlan capability 2-830
show pvlan mapping 2-832
show qos acl editbuffer 2-834
show qos acl info 2-835
show qos acl map 2-837
show qos acl resource-usage 2-839
show qos bridged-packet-policing 2-840
show qos info 2-841
show qos mac-cos 2-846

show qos maps 2-848
show qos policer 2-851
show qos policy-source 2-853
show qos rsvp 2-854
show qos statistics 2-856
show qos statistics export info 2-858
show qos status 2-859
show radius 2-860
show rcp 2-862
show reset 2-863
show rgmp group 2-864
show rgmp statistics 2-865
show rspan 2-866
show running-config 2-868
show security acl 2-871
show security acl capture-ports 2-874
show security acl log 2-875
show security acl map 2-878
show security acl resource-usage 2-879
show snmp 2-880
show snmp access 2-882
show snmp community 2-884
show snmp context 2-886
show snmp counters 2-887
show snmp engineid 2-891
show snmp group 2-892
show snmp notify 2-894
show snmp rmonmemory 2-896
show snmp targetaddr 2-897
show snmp targetparams 2-899
show snmp user 2-901
show snmp view 2-903
show span 2-905
show spantree 2-907
show spantree backbonefast 2-910

show spantree blockedports 2-911
show spantree bpdu-skewing 2-912
show spantree conflicts 2-914
show spantree defaultcostmode 2-916
show spantree guard 2-917
show spantree mapping 2-919
show spantree mistp-instance 2-921
show spantree mst 2-923
show spantree mst config 2-925
show spantree portfast 2-927
show spantree portinstancecost 2-928
show spantree portvlancost 2-929
show spantree statistics 2-930
show spantree summary 2-937
show spantree uplinkfast 2-940
show startup-config 2-942
show summertime 2-945
show system 2-946
show system highavailability 2-949
show system switchmode 2-950
show tacacs 2-951
show tech-support 2-953
show test 2-956
show time 2-961
show timezone 2-962
show top 2-963
show top report 2-965
show traffic 2-967
show trunk 2-968
show udld 2-972
show users 2-974
show version 2-975
show vlan 2-978
show vlan counters 2-983
show vmps 2-985

show vmps mac 2-987
show vmps statistics 2-988
show vmps vlan 2-989
show vtp domain 2-990
show vtp statistics 2-992
slip 2-994
squeeze 2-995
stack 2-996
switch 2-997
switch console 2-998
switch fabric 2-999
sync 2-1000
sysret 2-1001
telnet 2-1002
test snmp trap 2-1003
traceroute 2-1004
unalias 2-1007
undelete 2-1008
unset=varname 2-1009
varname= 2-1010
verify 2-1011
wait 2-1012
whichboot 2-1013
write 2-1014
write tech-support 2-1017

APPENDIX A **Acronyms** A-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 6000 family switches.

Organization

This publication is organized as follows:

Chapter	Title	Description
Chapter 1	Command-Line Interfaces	Describes the two types of CLIs found on Catalyst 6000 family switches
Chapter 2	Catalyst 6000 Family Switch and ROM Monitor Commands	Lists alphabetically and provides detailed information for all Catalyst 6000 family switch and ROM-monitor commands
Appendix A	Acronyms	Defines the acronyms used in this publication

Related Documentation

Other documents in the Catalyst 6000 family switch documentation set include:

- *Catalyst 6000 Family Installation Guide*
- *Catalyst 6000 Family Module Installation Guide*
- *Catalyst 6000 Family Software Configuration Guide*
- *System Message Guide—Catalyst 6000 Family, 4000 Family, Catalyst 2948G, and Catalyst 2980G Switches*
- *Catalyst 6000 Family Quick Software Configuration Guide*

- *ATM Software Configuration Guide and Command Reference for the Catalyst 5000 Family and 6000 Family Switches*
- *Release Notes for Catalyst 6000 Family*

For information about MIBs, refer to:

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

Conventions

This publication uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[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.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
italic screen font	Arguments for which you supply values are in *italic screen* font.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Notes use the following conventions:

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

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

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

http://www.cisco.com

Translated documentation is available at the following URL:

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

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.

- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

http://www.cisco.com/register/

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

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

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

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

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

CHAPTER 1

Command-Line Interfaces

This chapter describes the command-line interfaces (CLI) available on the Catalyst 6000 family switches and contains these sections:

- Switch CLI, page 1-1
- ROM Monitor CLI, page 1-13

For information regarding the ATM CLI and commands, refer to the *ATM Software Configuration Guide and Command Reference—Catalyst 5000 Family and 6000 Family Switches* publication.

For information regarding the IDSM CLI and commands, refer to the *Catalyst 6000 Intrusion Detection System Module Installation and Configuration Note* publication.

For definitions of terms and acronyms listed in this publication, see Appendix A, "Acronyms."

Switch CLI

Catalyst 6000 family switches are multimodule systems. Commands you enter from the CLI can apply to the entire system or to a specific module, port, or VLAN.

You can configure and maintain the Catalyst 6000 family switches by entering commands from the switch CLI. The CLI is a basic command-line interpreter similar to the UNIX C shell. Using the CLI **session** command, you can access the router configuration software and perform tasks such as history substitution and alias creation.

Note The Catalyst 6000 family consists of the Catalyst 6000 and 6500 series switches. The Catalyst 6000 series consists of the Catalyst 6006 and 6009 switches; the Catalyst 6500 series consists of the Catalyst 6506, 6509, 6509-NEB, and 6513 switches. Throughout this publication and all Catalyst 6000 family documents, the phrase *Catalyst 6000 family switches* refers to these switches, unless otherwise noted.

Accessing the Switch CLI

You can access the switch CLI from a console terminal connected to an EIA/TIA-232 port or through a Telnet session. The CLI allows fixed baud rates. Telnet sessions disconnect automatically after remaining idle for a user-defined time period.

Note EIA/TIA-232 was known as RS-232 before its acceptance as a standard by the Electronic Industries Alliance and Telecommunications Industry Association.

Accessing the Switch CLI via the Console Port (EIA/TIA-232)

To access the switch through the console (EIA/TIA-232) port, perform these steps:

	Task	Command
Step 1	From the Cisco Systems Console prompt, press **Return**.	
Step 2	At the prompt, enter the system password. The Console> prompt appears indicating that you have accessed the CLI in normal mode.	*<password>*
Step 3	Enter the necessary commands to complete your desired tasks.	Appropriate commands
Step 4	When finished, exit the session.	**quit**

After connecting through the console port, you see this display:

```
Cisco Systems Console
Enter password:
Console>
Console>
```

Accessing the Switch CLI via Telnet

To access the switch through a Telnet session, you must first set the IP address for the switch. You can open multiple sessions to the switch via Telnet.

To access the switch from a remote host with Telnet, perform these steps:

	Task	Command
Step 1	From the remote host, enter the **telnet** command and the name or IP address of the switch you want to access.	**telnet** *hostname* | *ip_addr*
Step 2	At the prompt, enter the password for the CLI. If no password has been configured, press **Return**.	*<password>*
Step 3	Enter the necessary commands to complete your desired tasks.	Appropriate commands
Step 4	When finished, exit the Telnet session.	**quit**

After connecting through a Telnet session, you see this display:

```
host% telnet cat6000-1.cisco.com
Trying 172.16.44.30 ...
Connected to cat6000-1.
```

Operating the Switch CLI

This section describes command modes and functions that allow you to operate the switch CLI.

Accessing the Command Modes

The CLI has two modes of operation: normal and privileged. Both are password-protected. Use normal-mode commands for everyday system monitoring. Use privileged commands for system configuration and basic troubleshooting.

After you log in, the system enters normal mode, which gives you access to normal-mode commands only. You can enter privileged mode by entering the **enable** command followed by the enable password. Privileged mode is indicated by the word "enable" in the system prompt. To return to normal mode, enter the **disable** command at the prompt.

The following example shows how to enter privileged mode:

```
Console> enable
Enter password: <password>
Console> (enable)
```

Using Command-Line Processing

Switch commands are not case sensitive. You can abbreviate commands and parameters as long as they contain enough letters to be different from any other currently available commands or parameters. You can scroll through the last 20 commands stored in the history buffer, and enter or edit the command at the prompt. (See Table 1-1.)

Table 1-1 Command-Line Processing Keystroke

Keystroke	Function
Ctrl-A	Jumps to the first character of the command line.
Ctrl-B or the left arrow key	Moves the cursor back one character.
Ctrl-C	Escapes and terminates prompts and tasks.
Ctrl-D	Deletes the character at the cursor.
Ctrl-E	Jumps to the end of the current command line.
Ctrl-F or the right arrow key[1]	Moves the cursor forward one character.
Ctrl-K	Deletes from the cursor to the end of the command line.
Ctrl-L; Ctrl-R	Repeats current command line on a new line.
Ctrl-N or the down arrow key[1]	Enters next command line in the history buffer.
Ctrl-P or the up arrow key[1]	Enters previous command line in the history buffer.
Ctrl-U; Ctrl-X	Deletes from the cursor to the beginning of the command line.
Ctrl-W	Deletes last word typed.

Table 1-1 Command-Line Processing Keystroke (continued)

Keystroke	Function
Esc B	Moves the cursor back one word.
Esc D	Deletes from the cursor to the end of the word.
Esc F	Moves the cursor forward one word.
Delete key or Backspace key	Erases mistake when entering a command; reenter command after using this key.

1. The arrow keys function only on ANSI-compatible terminals such as VT100s.

Using the Command-Line Editing Features

Catalyst 6000 family switch software includes an enhanced editing mode that provides a set of editing key functions similar to those of the Emacs editor. You can enter commands in uppercase, lowercase, or a mix of both. Only passwords are case sensitive. You can abbreviate commands and keywords to the number of characters that allow a unique abbreviation.

For example, you can abbreviate the **show** command to **sh**. After entering the command at the system prompt, press **Return** to execute the command.

Moving Around on the Command Line

Perform one of these tasks to move the cursor around on the command line for corrections or changes:

Task	Keystrokes
• Move the cursor back one character.	Press **Ctrl-B** or press the left arrow key[1].
• Move the cursor forward one character.	Press **Ctrl-F** or press the right arrow key[1].
• Move the cursor to the beginning of the command line.	Press **Ctrl-A**.
• Move the cursor to the end of the command line.	Press **Ctrl-E**.
• Move the cursor back one word.	Press **Esc B**.
• Move the cursor forward one word.	Press **Esc F**.

1. The arrow keys function only on ANSI-compatible terminals such as VT100s.

Completing a Partial Command Name

If you cannot remember a complete command name, press the **Tab** key to allow the system to complete a partial entry. To do so, perform this task:

Task	Keystrokes
Complete a command name.	Enter the first few letters and press the **Tab** key.

If your keyboard does not have a Tab key, press **Ctrl-I** instead.

In the following example, when you enter the letters **conf** and press the **Tab** key, the system provides the complete command:

```
Console> (enable) conf<Tab>

Console> (enable) configure
```

If you enter a set of characters that could indicate more than one command, the system beeps to indicate an error. Enter a question mark (?) to obtain a list of commands that begin with that set of characters. Do not leave a space between the last letter and the question mark (?). For example, three commands in privileged mode start with co. To see what they are, enter co? at the privileged prompt. The system displays all commands that begin with co, as follows:

```
Console> (enable) co?
configure  connect  copy
```

Pasting in Buffer Entries

The system provides a buffer that contains the last ten items you deleted. You can recall these items and paste them in the command line by performing this task:

Task	Keystrokes
• Recall the most recent entry in the buffer.	Press **Ctrl-Y**.
• Recall the next buffer entry.	Press **Esc Y**.

The buffer contains only the last ten items you have deleted or cut. If you press **Esc Y** more than ten times, you cycle back to the first buffer entry.

Editing Command Lines That Wrap

The new editing command set provides a wraparound feature for commands that extend beyond a single line on the screen. When the cursor reaches the right margin, the command line shifts ten spaces to the left. You cannot see the first ten characters of the line, but you can scroll back and check the syntax at the beginning of the command. To scroll back, perform this task:

Task	Keystrokes
Return to the beginning of a command line to verify that you have entered a lengthy command correctly.	Press **Ctrl-B** or the left arrow key repeatedly until you scroll back to the beginning of the command entry, or press **Ctrl-A** to return directly to the beginning of the line[1].

1. The arrow keys function only on ANSI-compatible terminals such as VT100s.

Use line wrapping with the command history feature to recall and modify previous complex command entries. See the "Using History Substitution" section on page 1-8 for information about recalling previous command entries.

The system assumes your terminal screen is 80 columns wide. If your screen has a different width, enter the terminal width command to tell the router the correct width of your screen.

Deleting Entries

Perform one of these tasks to delete command entries if you make a mistake or change your mind:

Task	Keystrokes
• Erase the character to the left of the cursor.	Press the **Delete** or **Backspace** key.
• Delete the character at the cursor.	Press **Ctrl-D**.
• Delete from the cursor to the end of the command line.	Press **Ctrl-K**.
• Delete from the cursor to the beginning of the command line.	Press **Ctrl-U** or **Ctrl-X**.
• Delete the word to the left of the cursor.	Press **Ctrl-W**.
• Delete from the cursor to the end of the word.	Press **Esc D**.

Scrolling Down a Line or a Screen

When you use the help facility to list the commands in a particular mode, the list is often longer than the terminal screen can display. In such cases, a ---More--- prompt is displayed at the bottom of the screen. To view the next line or screen, perform these tasks:

Task	Keystrokes
• Scroll down one line.	Press the **Return** key.
• Scroll down one screen.	Press the **Spacebar**.

Note The ---More--- prompt is used for any output that has more lines than can be displayed on the terminal screen, including **show** command output.

Scrolling to Specified Text

If you enter /*text* and press the **Return** key at the --More-- prompt, the display starts two lines above the line containing the *text* string. If the text string is not found, “Pattern Not Found” is displayed. You can also enter “**n**” at the --More-- prompt to search for the last entered *text* string. You can use this search method on all **show** commands that use the more buffer to display screen by screen ouput. The following is a list of **show** commands that do not use the more buffer and do not support this feature:

- **show cam**
- **show mls**
- **show tech-support**

Redisplaying the Current Command Line

If you enter a command and the system suddenly sends a message to your screen, you can recall your current command line entry. To do so, perform this task:

Task	Keystrokes
Redisplay the current command line.	Press **Ctrl-L** or **Ctrl-R**.

Transposing Mistyped Characters

If you mistype a command entry, you can transpose the mistyped characters by performing this task:

Task	Keystrokes
Transpose the character to the left of the cursor with the character located at the cursor.	Press **Ctrl-T**.

Controlling Capitalization

You can change words to uppercase or lowercase, or capitalize a set of letters, with simple keystroke sequences:

Task	Keystrokes
• Capitalize at the cursor.	Press **Esc C**.
• Change the word at the cursor to lowercase.	Press **Esc L**.
• Capitalize letters from the cursor to the end of the word.	Press **Esc U**.

Designating a Keystroke as a Command Entry

You can use a particular keystroke as an executable command. Perform this task:

Task	Keystrokes
Insert a code to indicate to the system that the keystroke immediately following should be treated as a command entry, *not* an editing key.	Press **Ctrl-V** or **Esc Q**.

Using Command Aliases

Like regular commands, aliases are not case sensitive. However, unlike regular commands, some aliases cannot be abbreviated. See Table 1-2 for a list of switch CLI aliases that cannot be abbreviated.

Table 1-2 Switch CLI Command Aliases

Alias	Command
batch	**configure**
di	**show**
earl	**cam**
exit	**quit**
logout	**quit**

Using History Substitution

Commands that you enter during each terminal session are stored in a history buffer, which stores the last 20 commands you entered during a terminal session. History substitution allows you to access these commands without retyping them by using special abbreviated commands. (See Table 1-3.)

Table 1-3 History Substitution Commands

Command	Function
To repeat recent commands:	
!!	Repeat the most recent command.
!-nn	Repeat the nnth most recent command.
!n	Repeat command n.
!aaa	Repeat the command beginning with string aaa.
!?aaa	Repeat the command containing the string aaa.
To modify and repeat the most recent command:	
^aaa^bbb	Replace string aaa with string bbb in the most recent command.
To add a string to the end of a previous command and repeat it:	
!!aaa	Add string aaa to the end of the most recent command.
!n aaa	Add string aaa to the end of command n.
!aaa bbb	Add string bbb to the end of the command beginning with string aaa.
!?aaa bbb	Add string bbb to the end of the command containing string aaa.

Accessing Command Help

To see a list of top-level commands and command categories, type **help** in normal or privileged mode. Context-sensitive help (usage and syntax information) for individual commands can be seen by appending **help** to any specific command. If you enter a command using the wrong number of arguments or inappropriate arguments, usage and syntax information for that command is displayed. Additionally, appending **help** to a command category displays a list of commands in that category.

Top-Level Commands and Command Categories

In normal mode, use the **help** command to display a list of top-level commands and command categories, as follows:

```
Console> help
Commands:
------------------------------------------------------------------------
cd                          Set default flash device
dir                         Show list of files on flash device
enable                      Enable privileged mode
help                        Show this help screen
history                     Show contents of history substitution buffer
l2trace                     Layer2 trace between hosts
ping                        Send echo packets to hosts
pwd                         Show default flash device
quit                        Exit from the Admin session
session                     Tunnel to ATM or Router module
set                         Set commands, use 'set help' for more info
show                        Show commands, use 'show help' for more info
traceroute                  Trace the route to a host
verify                      Verify checksum of file on flash device
wait                        Wait for x seconds
whichboot                   Which file booted
Console>
```

In privileged mode, enter the **help** command to display a list of top-level commands and command categories, as follows:

```
Console> (enable) help
Commands:
------------------------------------------------------------------------
cd                        Set default flash device
clear                     Clear, use 'clear help' for more info
commit                    Commit ACL to hardware and NVRAM
configure                 Configure system from network
copy                      Copy files between TFTP/RCP/module/flash devices
delete                    Delete a file on flash device
dir                       Show list of files on flash device
disable                   Disable privileged mode
disconnect                Disconnect user session
download                  Download code to a processor
enable                    Enable privileged mode
format                    Format a flash device
help                      Show this help screen
history                   Show contents of history substitution buffer
l2trace                   Layer2 trace between hosts
ping                      Send echo packets to hosts
pwd                       Show default flash device
quit                      Exit from the Admin session
reconfirm                 Reconfirm VMPS
reload                    Force software reload to linecard
reset                     Reset system or module
rollback                  Rollback changes made to ACL in editbuffer
```

```
session                  Tunnel to ATM or Router module
set                      Set commands, use 'set help' for more info
show                     Show commands, use 'show help' for more info
slip                     Attach/detach Serial Line IP interface
squeeze                  Reclaim space used by deleted files
switch                   Switch to standby <clock|supervisor>
telnet                   Telnet to a remote host
test                     Test command, use 'test help' for more info
undelete                 Undelete a file on flash device
upload                   Upload code from a processor
verify                   Verify checksum of file on flash device
wait                     Wait for x seconds
whichboot                Which file booted
write                    Write system configuration to terminal/network
Console> (enable)
```

Command Categories

On some commands (such as **clear**, **set**, and **show**), typing **help** after the command provides a list of commands in that category. For example, this display shows a partial list of commands for the **clear** category:

```
Console> (enable) clear help

Clear commands:
--------------------------------------------------------------------------
clear alias                  Clear aliases of commands
clear arp                    Clear ARP table entries
clear banner                 Clear Message Of The Day banner
clear boot                   Clear booting environment variable
clear cam                    Clear CAM table entries
clear channel                Clear PAgP statistical information
.
.
.
```

Context-Sensitive Help

Usage and syntax information for individual commands can be seen by appending **help** to any specific command. For example, the following display shows usage and syntax information for the **set length** command:

```
Console> set length help
Usage: set length <screenlength> [default]
       (screenlength = 5..512, 0 to disable 'more' feature)
Console>
```

Designating Modules, Ports, and VLANs

The Catalyst 6000 family modules (module slots), ports, and VLANs are numbered starting with 1. The supervisor engine module is module 1, residing in the top slot. On each module, port 1 is the leftmost port. To reference a specific port on a specific module, the command syntax is *mod/port*. For example, **3/1** denotes module 3, port 1. In some commands, such as **set trunk**, **set cam**, and **set vlan**, you can enter lists of ports and VLANs.

You can designate ports by entering the module and port number pairs, separated by commas. To specify a range of ports, use a dash (-) between the module number and port number pairs. Dashes take precedence over commas. The following examples show several ways of designating ports:

Example 1: **2/1,2/3** denotes module 2, port 1 and module 2, port 3.

Example 2: **2/1-12** denotes module 2, ports 1 through 12.

Example 3: **2/1-2/12** also denotes module 2, ports 1 through 12.

Each VLAN is designated by a single number. You can specify lists of VLANs the same way you do for ports. Individual VLANs are separated by commas (,); ranges are separated by dashes (-). In the following example, VLANs 1 through 10 and VLAN 1000 are specified:

```
1-10,1000
```

Designating MAC Addresses, IP and IPX Addresses, and IP Aliases

Some commands require a MAC address that you must designate in a standard format. The MAC address format must be six hexadecimal numbers separated by hyphens, as shown in this example:

```
00-00-0c-24-d2-fe
```

Some commands require an IP address. The IP address format is 32 bits, written as four octets separated by periods (dotted decimal format). IP addresses are made up of a network section, an optional subnet section, and a host section, as shown in this example:

```
126.2.54.1
```

If DNS is configured properly on the switch, you can use IP host names instead of IP addresses. For information on configuring DNS, refer to the *Catalyst 6000 Family Software Configuration Guide*.

If the IP alias table is configured, you can use IP aliases in place of the dotted decimal IP address. This is true for most commands that use an IP address, except commands that define the IP address or IP alias.

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

- IPX net 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)

Using Command Completion Features

The command completion features consist of these functions:

- Using Command Self-Repeat
- Using Keyword Lookup
- Using Partial Keyword Lookup
- Using Command Completion

Using Command Self-Repeat

Use the command self-repeat function to display matches to all possible keywords if a string represents a unique match. If a unique match is not found, the longest matching string is provided. To display the matches, enter a space after the last parameter and enter **?**. Once the matches are displayed, the system comes back to the prompt and displays the last command without the **?**. In the following example, notice how the system repeats the command entered without the **?**.

```
Console> (enable) set mls nde
  disable              Disable multilayer switching data export filter
  enable               Enable multilayer switching data export filter
  engineer             Engineer setting of the export filter
  flow                 Setting multilayer switching export filter
  <collector_ip>       IP address
Console> (enable) set mls nde
```

Using Keyword Lookup

Use the keyword-lookup function to display a list of valid keywords and arguments for a command. To display the matches, enter a space after the last parameter and enter **?**. For example, five parameters are used by the **set mls** command. To see these parameters, enter **set mls ?** at the privileged prompt. In the following example, notice how the system repeats the command entered without the **?**:

```
Console> (enable) set mls ?
  agingtime                 Set agingtime for MLS cache entry
  exclude                   Set MLS excluded protocol ports
  flow                      Set minimum flow mask
  nde                       Configure Netflow Data Export
  statistics                Add protocols to protocol statistics list
Console> (enable) set mls
```

Using Partial Keyword Lookup

Use the partial keyword-lookup function to display a list of commands that begin with a specific set of characters. To display the matches, enter **?** immediately after the last parameter. For example, enter **co?** at the privileged prompt to display a list of commands that start with **co**. The system displays all commands that begin with **co** and repeats the command entered without the **?**:

```
Console> (enable) co?
  commit               Commit ACL to hardware and NVRAM
  configure            Configure system from network
  copy                 Copy files between TFTP/RCP/module/flash devices
Console> (enable) co
```

Using Command Completion

Use the command completion function to complete a command or keyword. When you enter a unique partial character string and press **Tab**, the system completes the command or keyword on the command line. For example, if you enter **co** at the privileged prompt and press **Tab**, the system completes the command as **configure** because it is the only command that matches the criteria.

If no completion can be done, no action is carried out and the system returns to the prompt and the last command. The cursor appears immediately after the keyword, allowing you to enter additional information.

ROM Monitor CLI

The ROM monitor is a ROM-based program that executes upon platform power-up, reset, or when a fatal exception occurs.

Accessing the ROM Monitor CLI

The system enters ROM-monitor mode if the switch does not find a valid system image, if the NVRAM configuration is corrupted, or if the configuration register is set to enter ROM-monitor mode. From the ROM-monitor mode, you can load a system image manually from Flash memory, from a network server file, or from bootflash. You can also enter ROM-monitor mode by restarting the switch and pressing the **Break** key during the first 60 seconds of startup.

Note Break is always enabled for 60 seconds after rebooting the system, regardless of whether Break is configured to be off by configuration register settings.

To connect through a terminal server, escape to the Telnet prompt, and enter the **send break** command to break back to the ROM-monitor mode.

Operating the ROM Monitor CLI

The ROM monitor commands are used to load and copy system images, microcode images, and configuration files. System images contain the system software. Microcode images contain microcode to be downloaded to various hardware devices. Configuration files contain commands to customize Catalyst 6000 family software.

The manual **boot** command has the following syntax:

Note Enter the **copy** *file-id* {**tftp** | **flash** | *file-id*} command to obtain an image from the network.

- **boot**—Boot from ROM
- **boot** [*-xv*] [*device***:**][*imagename*]—Boot from the local device. If you do not specify an image name, the system defaults to the first valid file in the device. The image name is case sensitive.

Once you are in ROM-monitor mode, the prompt changes to rommon 1>. While you are in ROM-monitor mode, each time you enter a command, the number in the prompt increments by one.

CHAPTER 2

Catalyst 6000 Family Switch and ROM Monitor Commands

This chapter contains an alphabetical listing of all switch and ROM monitor commands available on the Catalyst 6000 family switches.

For information regarding ATM module-related commands, refer to the *ATM Software Configuration Guide and Command Reference for the Catalyst 5000 Family and 6000 Family Switches*.

For information regarding IDS module-related commands, refer to the *Catalyst 6000 Intrusion Detection System Module Installation and Configuration Note*.

Except where specifically differentiated, the Layer 3 switching engine refers to either:

- Supervisor Engine 1 with Layer 3 Switching Engine WS-F6K-PFC (Policy Feature Card)
- Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2)

alias

Use the **alias** command to set and display command aliases.

alias [*name*=*value*]

Syntax Description

name=	(Optional) Name you give to the alias.
value	(Optional) Value of the alias.

Defaults

This command has no default settings.

Command Types

ROM monitor command.

Command Modes

Normal.

Usage Guidelines

If *value* contains white space or other special (shell) characters, you must use quotation marks. If *value* has a space as its last character, the next command line word is checked for an alias (normally, only the first word on a command line is checked).

Without an argument, this command prints a list of all aliased names with their values.

An equal sign (=) is required between the name and value of the alias.

You must issue a **sync** command to save your change. If you do not issue a **sync** command, the change is not saved and a **reset** removes your change.

Examples

This example shows how to display a list of available **alias** commands and how to create an alias for the **set** command:

```
rommon 1 > alias
r=repeat
h=history
?=help
b=boot
ls=dir
i=reset
k=stack
rommon 2 > alias s=set
rommon 3 > alias
r=repeat
h=history
?=help
b=boot
ls=dir
i=reset
```

```
k=stack
s=set
rommon 4 > s
PS1=rommon ! >
BOOT=bootflash:RTSYNC_llue_11,1;slot0:f1,1;
==========================================================================
```

Related Commands unalias

boot

Use the **boot** command to boot up an external process.

boot [**-x**] [**-v**] [*device***:**][*imagename*]

Syntax Description

-x	(Optional) Load the image but do not execute.
-v	(Optional) Toggle verbose mode.
*device***:**	(Optional) ID of the device.
imagename	(Optional) Name of the image.

Defaults

This command has no default settings.

Command Types

ROM monitor command.

Command Modes

Normal.

Usage Guidelines

With no arguments, **boot** will boot the first image in bootflash. Specify an image by typing its name. Specify the device by typing the device ID.

If no device is given with an *imagename*, the image is not booted.

If a device name is not recognized by the monitor, the monitor passes the device ID to the boot helper image.

This command will not boot the MSFC if the PFC is not present in the Catalyst 6000 family switch.

Examples

This example shows how to use the **boot** command:

```
rommon 2 > boot bootflash:cat6000-sup.6-1-1.bin
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Uncompressing file:
############################################################################################
############################################################################################
#################################################################################
```

cd

Use the **cd** command to set the default Flash device for the system.

cd [[*m/*]*device***:**]

Syntax Description

m/	(Optional) Module number of the supervisor engine containing the Flash device.
*device***:**	(Optional) Valid devices include **bootflash** and **slot0**.

Defaults

The default Flash device is bootflash.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

A colon (:) is required after the specified device.

For those commands where device is an option, the device set by **cd** is used if the default device is not specified.

Examples

This example shows how to set the system default Flash device to bootflash:

```
Console> cd bootflash:
Default flash device set to bootflash.
Console>
```

Related Commands

pwd

clear alias

Use the **clear alias** command to clear the abbreviated versions of commands.

clear alias {*name* | **all**}

Syntax Description

name	Alternate identifier of the command.
all	Keyword to clear every alternate identifier previously created.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to erase the arpdel alias:

```
Console> (enable) clear alias arpdel
Command alias deleted.
Console> (enable)
```

This example shows how to erase all the aliases:

```
Console> (enable) clear alias all
Command alias table cleared. (1)
Console> (enable)
```

(1) indicates the number of command aliases cleared.

Related Commands

set alias
show alias

clear arp

Use the **clear arp** command to delete a specific entry or all entries from the ARP table.

clear arp [**all** | **dynamic** | **permanent** | **static**] {*ip_addr*}

Syntax Description

all	(Optional) Keyword to clear all ARP entries.
dynamic	(Optional) Keyword to clear all dynamic ARP entries.
permanent	(Optional) Keyword to clear all permanent ARP entries.
static	(Optional) Keyword to clear all static ARP entries.
ip_addr	IP address to clear from the ARP table.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to remove IP address 198.133.219.209 from the ARP table:

```
Console> (enable) clear arp 198.133.219.209
ARP entry deleted.
Console> (enable)
```

This example shows how to remove all entries from the ARP table:

```
Console> (enable) clear arp all
ARP table cleared. (1)
Console> (enable)
```

(1) indicates the number of entries cleared.

This example shows how to remove all dynamically learned ARP entries:

```
Console> (enable) clear arp dynamic
Unknown host
Dynamic ARP entries cleared. (3)
Console> (enable)
```

This example shows how to clear all permanently entered ARP entries:

```
Console> (enable) clear arp permanent
Unknown host
Permanent ARP entries cleared.(5)
Console> (enable)
```

Related Commands

set arp
show arp

clear banner motd

Use the **clear banner motd** command to clear the message-of-the-day banner.

clear banner motd

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear the message-of-the-day banner:

```
Console> (enable) clear banner motd
MOTD banner cleared
Console> (enable)
```

Related Commands

set banner motd

clear boot auto-config

Use the **clear boot auto-config** command to clear the contents of the CONFIG_FILE environment variable used to specify the configuration files used during bootup.

clear boot auto-config [*mod*]

Syntax Description

mod	(Optional) Module number of the supervisor engine containing the Flash device.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear the auto-config file:

```
Console> (enable) clear boot auto-config
CONFIG_FILE variable =
Console> (enable)
```

Related Commands

set boot auto-config
show boot

clear boot device

Use the **clear boot device** command to clear the contents of the CONFIG_FILE environment variable used to specify the NAM startup configuration files used.

clear boot device *mod*

Syntax Description

mod	Number of the module containing the Flash device.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is supported by the NAM module only.

Examples

This example shows how to clear the NAM boot string from NVRAM for module 2:

```
Console> (enable) clear boot device 2
Device BOOT variable =
Console> (enable)
```

Related Commands

set boot device
show boot device

clear boot system

Use the **clear boot system** command to clear the contents of the BOOT environment variable and the configuration register setting.

clear boot system all [*mod*]

clear boot system flash *device***:**[*filename*] [*mod*]

Syntax Description

all	Keyword to clear the whole BOOT environment variable.
mod	(Optional) Module number of the supervisor engine containing the Flash device.
flash	(Optional) Keyword to clear the Flash device.
*device***:**	Name of the Flash device.
filename	(Optional) Filename of the Flash device.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear the whole BOOT environment variable:

```
Console> (enable) clear boot system all
BOOT variable =
Console> (enable)
```

This example shows how to clear a specific device; note how the specified device is not listed:

```
Console> (enable) clear boot system flash bootflash:cat6000-sup.5-5-1.bin
BOOT variable = bootflash:cat6000-sup.6-1-1.bin,1;bootflash:cat6000-sup.5-5-2.
bin,1;
Console> (enable)
```

Related Commands

set boot system flash
show boot

clear cam

Use the **clear cam** command to delete a specific entry or all entries from the CAM table.

clear cam *mac_addr* [*vlan*]

clear cam {**dynamic** | **static** | **permanent**} [*vlan*]

Syntax Description

mac_addr	One or more MAC addresses.
vlan	(Optional) Number of the VLAN; valid values are from **1** to **1000** and from **1025** to **4094**.
dynamic	Keyword to clear the dynamic CAM entries from the CAM table.
static	Keyword to clear the static CAM entries from the CAM table.
permanent	Keyword to clear the permanent CAM entries from the CAM table.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to remove MAC address 00-40-0b-a0-03-fa from the CAM table:

```
Console> (enable) clear cam 00-40-0b-a0-03-fa
CAM table entry cleared.
Console> (enable)
```

This example shows how to clear dynamic entries from the CAM table:

```
Console> (enable) clear cam dynamic
Dynamic CAM entries cleared.
Console> (enable)
```

Related Commands

set cam
show cam

clear channel statistics

Use the **clear channel statistics** command to clear PAgP statistical information.

clear channel statistics

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Types Switch command.

Command Modes Privileged.

Examples This example shows how to clear PAgP statistical information:

```
Console> (enable) clear channel statistics
PAgP statistics cleared.
Console> (enable)
```

Related Commands **show channel**

clear config

Use the **clear config** command to clear the system or module configuration information stored in NVRAM.

clear config {*mod* | **rmon** | **all** | **snmp** | **acl nvram**}

Syntax Description

mod	Number of the module.
rmon	Keyword to clear all RMON configurations, including the historyControlTable, the alarmTable, the eventTable, and the ringStation ControlTable.
all	Keyword to clear all module and system configuration information, including the IP address.
snmp	Keyword to clear all SNMP configurations.
acl nvram	Keywords to clear all ACL configurations.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When using an MSM, entering the **clear config** command clears the portion of the MSM configuration kept by the Catalyst 6000 family switch supervisor engine. You must clear the portion of the configuration kept by the MSM at the router level (router> prompt).

Before using the **clear config all** command, save a backup of the configuration using the **copy** command.

Examples

This example shows how to delete the configuration information in NVRAM on module 2:

```
Console> (enable) clear config 2
This command will clear module 2 configuration.
Do you want to continue (y/n) [n]? y
.............................
Module 2 configuration cleared.
Console> (enable)
```

This example shows how to delete the configuration information stored in NVRAM on module 1 (the supervisor engine):

```
Console> (enable) clear config 1
This command will clear module 1 configuration.
Do you want to continue (y/n) [n]? y
......
Module 1 configuration cleared.
host%
```

This example shows how to delete all the configuration information for the Catalyst 6000 family switches:

```
Console> (enable) clear config all
This command will clear all configuration in NVRAM.
Do you want to continue (y/n) [n]? y
.....................................
Connection closed by foreign host
host%
```

This example shows how to delete all the SNMP configuration information for the Catalyst 6000 family switches:

```
Console> (enable) clear config snmp
This command will clear SNMP configuration in NVRAM.
Do you want to continue (y/n) [n]? y
.....................................
Connection closed by foreign host
host%
```

This example shows how to delete all ACL configuration information from NVRAM:

```
Console> (enable) clear config acl nvram
ACL configuration has been deleted from NVRAM.
Warning:Use the copy commands to save the ACL configuration to a file
and the 'set boot config-register auto-config' commands to configure the
auto-config feature.
Console> (enable)
```

Related Commands

set config acl nvram
show config qos acl

clear config pvlan

Use the **clear config pvlan** command to clear all private VLAN configurations in the system including port mappings.

clear config pvlan

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear all private VLAN configurations in the system:

```
Console> (enable) clear config pvlan
This command will clear all private VLAN configurations.
Do you want to continue (y/n) [n]? y
VLAN 15 deleted
VLAN 16 deleted
VLAN 17 deleted
VLAN 18 deleted
Private VLAN configuration cleared.
Console> (enable)
```

Related Commands

clear pvlan mapping
clear vlan
configure
set vlan
set pvlan
set pvlan mapping
show config
show pvlan
show pvlan mapping
show vlan

clear cops

Use the **clear cops** command to clear COPS configurations.

clear cops roles *role1* [*role2*]...

clear cops all-roles

clear cops server all [**diff-serv** | **rsvp**]

clear cops server *ipaddr* [**diff-serv** | **rsvp**]

clear cops domain-name

Syntax Description

roles *role#*	Keyword and variable to specify the roles to clear.
all-roles	Keyword to clear all roles.
server	Keyword to specify the COPS server.
all	Keyword to clear all server tables.
diff-serv	(Optional) Keyword to specify the differentiated services server table.
rsvp	(Optional) Keyword to specify the RSVP+ server table.
ipaddr	IP address or IP alias of the server.
domain-name	Keyword to specify the domain name of the server.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can use the **clear cops all-roles** command to clear all roles from all ports.

Examples

This example shows how to clear specific roles:

```
Console> (enable) clear cops roles backbone_port main_port
Roles cleared.
Console> (enable)
```

This example shows how to clear all roles:

```
Console> (enable) clear cops all-roles
All roles cleared.
Console> (enable)
```

This example shows how to clear all COPS servers:

```
Console> (enable) clear cops server all
All COPS servers cleared.
Console> (enable)
```

This example shows how to clear a specific COPS server:

```
Console> (enable) clear cops server my_server1
All COPS servers cleared.
Console> (enable)
```

This example shows how to clear the COPS domain name:

```
Console> (enable) clear cops domain-name
Domain name cleared.
Console> (enable)
```

Related Commands

set cops
show cops

clear counters

Use the **clear counters** command to clear MAC counters, EtherChannel MAC counters, port counters, and the channel traffic percentile.

clear counters [**all** | *mod/ports*]

Syntax Description

all	(Optional) Keyword to specify all ports.
mod/ports	(Optional) Number of the module and the ports on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not specify a range of ports to be cleared, then all ports on the switch are cleared.

Examples

This example shows how to reset MAC and port counters to zero:

```
Console> (enable) clear counters
This command will reset all MAC and port counters reported in CLI and SNMP.
Do you want to continue (y/n) [n]? y

MAC and Port counters cleared.
Console> (enable)
```

This example shows how to reset MAC and port counters to zero for a specific module and port:

```
Console> (enable) clear counters 5/1
This command will reset MAC and port counters reported by the CLI for port(s) 5/1.
Do you want to continue (y/n) [n]? y

MAC and Port counters cleared.
Console> (enable)
```

Related Commands

restore counters
show port counters

clear crypto key rsa

Use the **clear crypto key rsa** command to remove all RSA public-key pairs.

clear crypto key rsa

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **crypto** commands are supported on systems that run these image types only:

- supk9 image—for example, cat6000-supk9.6-1-3.bin
- supcvk9 image—for example, cat6000-supcvk9.6-1-3.bin

Examples

This example shows how to clear RSA key pairs:

```
Console> (enable) clear crypto key rsa
Do you really want to clear RSA keys (y/n) [n]? y
RSA keys has been cleared.
Console> (enable)
```

Related Commands

set crypto key rsa
show crypto key

clear dot1x config

Use the **clear dot1x config** command to disable dot1x on all ports and return values to the default settings.

clear dot1x config

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to disable dot1x and return values to the default settings:

```
Console> (enable) clear dot1x config
This command will disable Dot1x and take values back to factory default.

Do you want to continue (y/n) [n]? y
Dot1x config cleared.
Console> (enable)
```

Related Commands

set port dot1x
show dot1x
show port dot1x

clear gmrp statistics

Use the **clear gmrp statistics** command to clear all the GMRP statistics information from a specified VLAN or all VLANs.

clear gmrp statistics {*vlan* | **all**}

Syntax Description

vlan	Number of the VLAN; valid values are from **1** to **1000** and from **1025** to **4094**.
all	Keyword to specify all VLANs.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear GMRP statistical information from all VLANs:

```
Console> (enable) clear gmrp statistics all
GMRP statistics cleared.
Console> (enable)
```

This example shows how to clear GMRP statistical information from VLAN 1:

```
Console> (enable) clear gmrp statistics 1
GMRP statistics cleared from VLAN 1.
Console> (enable)
```

Related Commands

show gmrp statistics

clear gvrp statistics

Use the **clear gvrp statistics** command to clear all the GVRP statistics information.

clear gvrp statistics {*mod/port* | **all**}

Syntax Description

mod/port	Number of the module and port.
all	Keyword to specify all ports.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear all GVRP statistical information:

```
Console> (enable) clear gvrp statistics all
GVRP statistics cleared for all ports.
Console> (enable)
```

This example shows how to clear GVRP statistical information for module 2, port 1:

```
Console> (enable) clear gvrp statistics 2/1
GVRP statistics cleared on port 2/1.
Console> (enable)
```

Related Commands

set gvrp
show gvrp configuration

clear igmp statistics

Use the **clear igmp statistics** command to clear IGMP snooping statistical information.

clear igmp statistics

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear IGMP statistical information:

```
Console> (enable) clear igmp statistics
IGMP statistics cleared.
Console> (enable)
```

Related Commands

set igmp
show igmp statistics

clear ip alias

Use the **clear ip alias** command to clear IP aliases that were set using the **set ip alias** command.

clear ip alias {*name* | **all**}

Syntax Description

name	IP address alias to delete.
all	Keyword to specify that all previously set IP address aliases be deleted.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to delete a previously defined IP alias named babar:

```
Console> (enable) clear ip alias babar
IP alias deleted.
Console> (enable)
```

Related Commands

set ip alias
show ip alias

clear ip dns domain

Use the **clear ip dns domain** command to clear the default DNS domain name.

clear ip dns domain

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear the default DNS domain name:

```
Console> (enable) clear ip dns domain
Default DNS domain name cleared.
Console> (enable)
```

Related Commands

set ip dns domain
show ip dns

clear ip dns server

Use the **clear ip dns server** command to remove a DNS server from the DNS server listing.

clear ip dns server {*ip_addr* | **all**}

Syntax Description

ip_addr	IP address of the DNS server you want to remove. An IP alias or a host name that can be resolved through DNS can also be used.
all	Keyword to specify all the IP addresses in the DNS server listing to be removed.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to remove the DNS server at IP address 198.92.30.32 from the DNS server listing:

```
Console> (enable) clear ip dns server 198.92.30.32
198.92.30.32 cleared from DNS table.
Console> (enable)
```

This example shows how to remove all DNS servers from the DNS server listing:

```
Console> (enable) clear ip dns server all
All DNS servers cleared
Console> (enable)
```

Related Commands

set ip dns server
show ip dns

clear ip permit

Use the **clear ip permit** command to remove a specified IP address and mask or all IP addresses and masks from the permit list.

clear ip permit all

clear ip permit {*ip_addr*} [*mask*] [**telnet** | **ssh** | **snmp** | **all**]

Syntax Description

ip_addr	IP address to be cleared. An IP alias or a host name that can be resolved through DNS can also be used.
mask	(Optional) Subnet mask of the specified IP address.
telnet	(Optional) Keyword to clear the entries in the Telnet permit list.
ssh	(Optional) Keyword to clear the entries in the SSH permit list.
snmp	(Optional) Keyword to clear the entries in the SNMP permit list.
all	(Optional) Keyword to clear all permit lists.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **clear ip permit all** command clears the permit list but does not change the state of the IP permit feature. A warning is displayed if all IP addresses are cleared from the permit list, and the feature is enabled. If a mask other than the default (255.255.255.255) has been configured, you must provide both the address and mask to clear a specific entry.

If the **telnet**, **ssh**, **snmp**, or **all** keyword is not specified, the IP address is removed from both the SNMP and Telnet permit lists.

Examples

These examples show how to remove IP addresses:

```
Console> (enable) clear ip permit 172.100.101.102
172.100.101.102 cleared from IP permit list.
Console> (enable)

Console> (enable) clear ip permit 172.160.161.0 255.255.192.0 snmp
172.160.128.0 with mask 255.255.192.0 cleared from snmp permit list.
Console> (enable)

Console> (enable) clear ip permit 172.100.101.102 telnet
172.100.101.102 cleared from telnet permit list.
Console> (enable)
```

```
Console> (enable) clear ip permit all
IP permit list cleared.
WARNING
IP permit list is still enabled.
Console> (enable)
```

Related Commands

set ip permit
show ip permit

clear ip route

Use the **clear ip route** command to delete IP routing table entries.

clear ip route *destination gateway*

Syntax Description

destination	IP address of the host or network. An IP alias or a host name that can be resolved through DNS can also be used.
gateway	IP address or alias of the gateway router.

Defaults

The default is *destination*. If the destination is not the active default gateway, the actual destination is the default.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to delete the routing table entries using the **clear ip route** command:

```
Console> (enable) clear ip route 134.12.3.0 elvis
Route deleted.
Console> (enable)
```

Related Commands

set ip route
show ip route

clear kerberos clients mandatory

Use the **clear kerberos clients mandatory** command to disable mandatory Kerberos authentication for services on the network.

clear kerberos clients mandatory

Syntax Description

This command has no arguments or keywords.

Defaults

Kerberos clients are NOT set to mandatory.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not make Kerberos authentication mandatory and Kerberos authentication fails, the application attempts to authenticate users using the default method of authentication for that network service. For example, Telnet prompts for a password.

Examples

This example shows how to clear mandatory Kerberos authentication:

```
Console> (enable) clear  kerberos clients mandatory
Kerberos clients mandatory cleared
Console> (enable)
```

Related Commands

set kerberos clients mandatory
show kerberos

clear kerberos credentials forward

Use the **clear kerberos credentials forward** command to disable credentials forwarding.

clear kerberos credentials forward

Syntax Description

This command has no arguments or keywords.

Defaults

The default is forwarding is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you have a TGT and are authenticated to a Kerberized switch, you can use the TGT to authenticate to a host on the network. However, if forwarding is not enabled and you try to list credentials after authenticating to a host, the output will show no Kerberos credentials are present.

Examples

This example shows how to disable Kerberos credentials forwarding:

```
Console> (enable) clear kerberos credentials forward
Kerberos credentials forwarding disabled
Console> (enable)
```

Related Commands

set kerberos clients mandatory
set kerberos credentials forward
show kerberos

clear kerberos creds

Use the **clear kerberos creds** command to delete all the Kerberos credentials.

clear kerberos creds

Syntax Description

This command has no arguments or keywords.

Defaults

The command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you have a TGT and are authenticated to a Kerberized switch, you can use the TGT to authenticate to a host on the network.

Examples

This example shows how to delete all Kerberos credentials:

```
Console> (enable) clear kerberos creds
Console> (enable)
```

Related Commands

set kerberos credentials forward
show kerberos

clear kerberos realm

Use the **clear kerberos realm** command to clear an entry that maps the name of a Kerberos realm to a DNS domain name or a host name.

clear kerberos realm {*dns_domain* | *host*} *kerberos_realm*

Syntax Description

dns_domain	DNS domain name to map to a Kerberos realm.
host	IP address or name to map to a Kerberos realm.
kerberos_realm	IP address or name of a Kerberos realm.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can map the name of a Kerberos realm to a DNS domain name or a host name with the **set kerberos realm** command.

Examples

This example shows how to clear an entry mapping a Kerberos realm to a domain name:

```
Console> (enable) clear kerberos realm CISCO CISCO.COM
Kerberos DnsDomain-Realm entry CISCO - CISCO.COM deleted
Console> (enable)
```

Related Commands

set kerberos local-realm
set kerberos realm
show kerberos

clear kerberos server

Use the **clear kerberos server** command to clear a specified KDC entry.

clear kerberos server *kerberos_realm* {*hostname* | *ip_address*} [*port_number*]

Syntax Description

kerberos_realm	Name of a Kerberos realm.
hostname	Name of the host running the KDC.
ip_address	IP address of the host running the KDC.
port_number	(Optional) Number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can specify to the switch which KDC to use in a Kerberos realm. This command clears a server entry from the table.

Examples

This example shows how to clear a KDC server entered on the switch:

```
Console> (enable) clear kerberos server CISCO.COM 187.0.2.1 750
Kerberos Realm-Server-Port entry CISCO.COM-187.0.2.1-750  deleted
Console> (enable)
```

Related Commands

set kerberos server
show kerberos

clear key config-key

Use the **clear key config-key** command to remove a private 3DES key.

clear key config-key *string*

Syntax Description

string	Name of the 3DES key; the name should be no longer than 8 bytes.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to remove a private 3DES key:

```
Console> (enable)  clear key config-key abcd
Kerberos config key deleted
Console> (enable)
```

Related Commands

set key config-key

clear lacp-channel statistics

Use the **clear lacp-channel statistics** command to clear Link Aggregation Control Protocol (LACP) statistical information.

clear lacp-channel statistics

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

For differences between PAgP and LACP, refer to the "Guidelines for Port Configuration" section of the "Configuring EtherChannel" chapter of the *Catalyst 6000 Family Software Configuration Guide*.

Examples

This example shows how to clear LACP statistical information:

```
Console> (enable) clear lacp-channel statistics
LACP channel counters are cleared.
Console> (enable)
```

Related Commands

set channelprotocol
set lacp-channel system-priority
set port lacp-channel
set spantree channelcost
set spantree channelvlancost
show lacp-channel
show port lacp-channel

clear lda

Use the **clear lda** command to remove the ASLB MLS entries or MAC addresses from the switch.

clear lda mls

clear lda mls [**destination** *ip_addr_spec*] [**source** *ip_addr_spec*] [**protocol** *protocol* **src-port** *src_port* **dst-port** *dst_port*]

clear lda vip {**all** | *vip* | *vip tcp_port*}

clear lda mac {**all** | *router_mac_address*}

Syntax Description

mls	Keyword to remove configured LDs.
destination *ip_addr_spec*	(Optional) Full destination IP address or a subnet address in these formats: *ip_addr*, *ip_addr/netmask*, or *ip_addr/maskbit*.
source *ip_addr_spec*	(Optional) Full source IP address or a subnet address in these formats: *ip_addr*, *ip_addr/netmask*, or *ip_addr/maskbit*.
protocol *protocol*	(Optional) Keyword and variable to specify additional flow information (protocol family and protocol port pair) to be matched; valid values include **tcp**, **udp**, **icmp**, or a decimal number for other protocol families.
src-port *src_port*	(Optional) Keyword and variable to specify the number of the TCP/UDP source port (decimal). Used with **dst-port** to specify the port pair if the protocol is **tcp** or **udp**. **0** indicates “do not care.”
dst-port *dst_port*	(Optional) Keyword and variable to specify the number of the TCP/UDP destination port (decimal). Used with **src-port** to specify the port pair if the protocol is **tcp** or **udp**. **0** indicates “do not care.”
vip all	Keywords to remove all VIP couples (set using the **set lda** command).
vip *vip*	Keyword and variable to specify a VIP.
vip *vip tcp_port*	Keyword and variables to specify a VIP and port couple.
mac all	Keywords to clear all ASLB router MAC addresses.
mac *router_mac_address*	Keyword and variable to clear a specific router MAC address.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is supported only on switches configured with the Supervisor Engine 1 with Layer 3 Switching Engine WS-F6K-PFC (Policy Feature Card).

Entering the **destination** keyword specifies the entries matching the destination IP address specification, entering the **source** keyword specifies the entries matching the source IP address specification, and entering an *ip_addr_spec* can specify a full IP address or a subnet address. If you do not specify a keyword, it is treated as a wildcard, and all entries are displayed.

When entering the *ip_addr_spec*, use the full IP address or a subnet address in one of the following formats: *ip_addr, ip_addr/netmask,* or *ip_addr/maskbit*.

If you do not enter any keywords, the LD is removed from the switch and the LD configuration is removed from NVRAM.

If you do not enter any keywords with the **clear lda mls** command, all ASLB MLS entries are cleared.

Examples

This example shows how to clear the ASLB MLS entry at a specific destination address:

```
Console> (enable) clear lda mls destination 172.20.26.22
MLS IP entry cleared.
Console> (enable)
```

This example shows how to delete a VIP and port pair (VIP 10.0.0.8, port 8):

```
Console> (enable) clear lda vip 10.0.0.8 8
Successfully deleted vip/port pairs.
Console> (enable)
```

This example shows how to clear all ASLB router MAC addresses:

```
Console> (enable) clear lda mac all
Successfully cleared Router MAC address.
Console> (enable)
```

This example shows how to clear a specific ASLB router MAC address:

```
Console> (enable) clear lda mac 1-2-3-4-5-6
Successfully cleared Router MAC address.
Console> (enable)
```

Related Commands

commit lda
set lda
show lda

clear log

Use the **clear log** command to delete module, system error log, or dump log entries.

clear log [*mod*]

clear log dump

Syntax Description

mod	(Optional) Module number.
dump	Keyword to clear dump log entries.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not specify a module number, the system error log for the entire system is erased.

Examples

This example shows how to clear the system error log:

```
Console> (enable) clear log
System error log cleared.
Console> (enable)
```

This example shows how to clear the dump log:

```
Console> (enable) clear log dump
Console> (enable)
```

Related Commands

show log

clear log command

Use the **clear log command** command to clear the command log entry table.

clear log command [*mod*]

Syntax Description

mod	(Optional) Number of the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The command log entry table is a history log of the commands input to the switch from the console or Telnet.

Examples

This example shows how to clear the command log table for the switch:

```
Console> (enable) clear log command
Local-log cleared
Console> (enable)
```

This example shows how to clear the command log table for a specific module:

```
Console> (enable) clear log command 3
Module 3 log cleared.
Console> (enable)
```

Related Commands

show log command

clear logging buffer

Use the **clear logging buffer** command to clear the system logging buffer.

clear logging buffer

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear the system logging buffer:

```
Console> (enable) clear logging buffer
System logging buffer cleared.
Console> (enable)
```

Related Commands

show logging buffer

clear logging level

Use the **clear logging level** command to reset the logging level for a facility or for all facilities to their default settings.

clear logging level {*facililty* | **all**}

Syntax Description

facility	Name of the facility to reset; facility types are listed in Table 2-1.
all	Keyword to reset all facilities.

Table 2-1 Facility Types

Facility Name	Definition
all	All facilities
acl	access control list
cdp	Cisco Discovery Protocol
cops	Common Open Policy Service Protocol
dtp	Dynamic Trunking Protocol
dvlan	Dynamic VLAN
earl	Enhanced Address Recognition Logic
filesys	file system facility
gvrp	GARP VLAN Registration Protocol
ip	Internet Protocol
kernel	Kernel
ld	ASLB facility
mcast	Multicast
mgmt	Management
mls	Multilayer Switching
pagp	Port Aggregation Protocol
protfilt	Protocol Filter
pruning	VTP pruning
privatevlan	Private VLAN facility
qos	Quality of Service
radius	Remote Access Dial-In User Service
rsvp	ReSerVation Protocol
security	Security
snmp	Simple Network Management Protocol

Table 2-1 Facility Types (continued)

Facility Name	Definition
spantree	Spanning Tree Protocol
sys	System
tac	Terminal Access Controller
tcp	Transmission Control Protocol
telnet	Terminal Emulation Protocol
tftp	Trivial File Transfer Protocol
udld	User Datagram Protocol
vmps	VLAN Membership Policy Server
vtp	Virtual Terminal Protocol

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to reset a specific facility back to its default settings:

```
Console> (enable) clear logging level dtp
Current session and default severities of facility <dtp> set to factory default values.
Console> (enable)
```

This example shows how to reset all facilities back to their default settings:

```
Console> (enable) clear logging level all
Current session and default severities of all facilities set to factory default values.
Console> (enable)
```

Related Commands

set logging level
show logging

clear logging server

Use the **clear logging server** command to delete a syslog server from the system log server table.

clear logging server *ip_addr*

Syntax Description

ip_addr	IP address of the syslog server to be deleted.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to delete a syslog server from the configuration:

```
Console> (enable) clear logging server 171.69.192.207
System log server 171.69.192.207 removed from system log server table.
Console> (enable)
```

Related Commands

set logging server
show logging

clear mls cef

Use the **clear mls cef** command to clear CEF summary statistics.

clear mls cef

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is supported on Catalyst 6000 family switches configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) only.

Examples

This example shows how to clear CEF summary information:

```
Console> (enable) clear mls cef
CEF statistics cleared.
Console> (enable)
```

Related Commands

show mls cef summary

clear mls entry

Use the **clear mls entry** command to clear MLS entries in the Catalyst 6000 family switches.

clear mls entry [**ip** | **ipx**] **all**

clear mls entry ip destination *ip_addr_spec* [**source** *ip_addr_spec*] [**protocol** *protocol*] [**src-port** *src_port*] [**dst-port** *dst_port*]

clear mls entry ipx destination *ipx_addr_spec*

Syntax Description

ip	(Optional) Keyword to specify IP MLS.
ipx	(Optional) Keyword to specify IPX MLS.
all	Keyword to clear all MLS entries.
destination	Keyword to specify the destination IP address.
ip_addr_spec	Full IP address or a subnet address in these formats: *ip_addr*, *ip_addr/netmask*, or *ip_addr/maskbit*.
source *ip_addr_spec*	(Optional) Keyword and variable to specify the source IP address.
protocol *protocol*	(Optional) Keyword and variable to specify additional flow information (protocol family and protocol port pair) to be matched; valid values are **0** to **255** or **ip**, **ipinip**, **icmp**, **igmp**, **tcp**, and **udp**.
src-port *src_port*	(Optional) Keyword and variable to specify the source port IP address; valid values are **1** to **65535**, **dns**, **ftp**, **smtp**, **telnet**, **x** (X-Windows), **www**.
dst-port *dst_port*	(Optional) Keyword and variable to specify the destination port IP address; valid values are **1** to **65535**, **dns**, **ftp**, **smtp**, **telnet**, **x** (X-Windows), **www**.
ipx_addr_spec	Full IPX address or a subnet address in these formats: *src_net/*[*mask*], *dest_net.dest_node*, or *dest_net/mask*.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported on systems configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2). To clear entries on systems configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2), you must enter the **clear mls entry cef adjacency** command.

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

- IPX net 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)

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

To use a router as an MLS, you must meet these conditions:

- The router must be included (either explicitly or automatically) in the MLS-SE.
- The MLS feature must be enabled in the Catalyst 6000 family switches.
- The Catalyst 6000 family switches must know the router's MAC-VLAN pairs.

Use the following syntax to specify an IP subnet address:

- *ip_subnet_addr*—This is the 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.
- *ip_addr/subnet_mask*—This is the 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* is a full host address, such as 172.22.253.1/255.255.252.00.
- *ip_addr/maskbits*—This is the 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* is a full host address, such as 193.22.253.1/22, which has the same subnet address as the *ip_subnet_addr*.

If you do not use the **all** argument in the **clear mls entry** command, you must specify at least one of the other three keywords (**source**, **destination**, or **protocol**) and its arguments.

If no value or 0 is entered for *src_port* and *dest_port*, all entries are cleared.

When you remove an MSM from the Catalyst 6000 family switch, it is removed immediately from the inclusion list and all the MLS entries for the MSM are removed.

Examples

This example shows how to clear the MLS entries with destination IP address 172.20.26.22:

```
Console> (enable) clear mls entry destination 172.20.26.22
Multilayer switching entry cleared.
Console> (enable)
```

This example shows how to clear specific IP MLS entries for destination IP address 172.20.26.22:

```
Console> (enable) clear mls entry ip destination 172.20.26.22 source 172.20.22.113 protocol tcp 520 320
Multilayer switching entry cleared
Console> (enable)
```

This example shows how to clear specific IPX MLS entries for a destination IPX address:

```
Console> (enable) clear mls entry ipx destination 1.00e0.fefc.6000 source 3.0034.1245.AB45
IPX Multilayer switching entry cleared
Console> (enable)
```

Related Commands

show mls entry

clear mls entry cef adjacency

Use the **clear mls entry cef adjacency** command to clear CEF adjacency statistics.

clear mls entry cef adjacency

clear mls entry cef ip [[*ip_addr*/]*mask_len*] **adjacency**

clear mls entry cef ipx [[*ipx_addr*/]*mask_len*] **adjacency**

Syntax Description

ip	Keyword to specify IP entries.
ipx	Keyword to specify IPX entries.
ip_addr	(Optional) IP address of the entry.
mask_len	(Optional) Mask length associated with the IP or IPX address of the entry; valid values are from **0** to **32**.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is supported on Catalyst 6000 family switches configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2).

To clear MLS entries on systems configured with the Supervisor Engine 1 with Layer 3 Switching Engine WS-F6K-PFC (Policy Feature Card), enter the **clear mls entry** command.

The *ipx_addr* is entered as 32-bit hexadecimal digits.

Examples

This example shows how to clear all adjacencies associated with CEF entries:

```
Console> (enable) clear mls cef entry adjacency
Adjacency statistics has been cleared.
Console> (enable)
```

Related Commands

show mls entry cef

clear mls exclude protocol

Use the **clear mls exclude protocol** command to remove a protocol port that has been been excluded from shortcutting using the **set mls exclude protocol** command.

clear mls exclude protocol tcp | **udp** | **both** *port*

Syntax Description

tcp	Keyword to specify a TCP port.
udp	Keyword to specify a UDP port.
both	Keyword to specify that the port be applied to both TCP and UDP traffic.
port	Number of the port.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to set TCP packets in a protocol port to be hardware switched:

```
Console> (enable) clear mls exclude protocol tcp 25
TCP packets with protocol port 25 will be MLS switched.
Console> (enable)
```

Related Commands

set mls exclude protocol
show mls exclude protocol

clear mls multicast statistics

Use the **clear mls multicast statistics** command to remove MLS multicast statistics maintained per the MSFC on the switch.

clear mls multicast statistics [*mod*]

Syntax Description

mod	(Optional) Number of the MSFC; valid values are **15** and **16**.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you enter the **clear mls multicast statistics** command on a Catalyst 6000 family switch without MLS, this warning message is displayed:

```
MLS Multicast is not supported on feature card.
```

If you place the MFSC on a supervisor engine installed in slot 1, then the MFSC is recognized as module 15. If you install the supervisor engine in slot 2, the MFSC is recognized as module 16.

The *mod* option is not supported on switches configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2).

Examples

This example shows how to clear MLS statistics on a switch configured with the Supervisor Engine 1 with Layer 3 Switching Engine WS-F6K-PFC (Policy Feature Card):

```
Console> (enable) clear mls multicast statistics
All statistics for the MLS routers in include list are cleared.
Console> (enable)
```

This example shows how to clear MLS statistics on a switch configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2):

```
Console> (enable) clear mls multicast statistics
All statistics cleared.
Console> (enable)
```

Related Commands

show mls statistics

clear mls nde flow

Use the **clear mls nde flow** command to reset the NDE filters in the Catalyst 6000 family switches.

clear mls nde flow

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Clearing both exclusion and inclusion filters results in exporting of all flows.

Examples

This example shows how to clear the NDE exclusion and inclusion filters and export all flows:

```
Console> (enable) clear mls nde flow
Netflow data export filter cleared.
Console> (enable)
```

Related Commands

set mls nde
show mls exclude protocol

clear mls statistics

Use the **clear mls statistics** command to clear hardware-installed MLS statistics entries.

clear mls statistics

clear mls statistics protocol {*protocol port*} | **all**

Syntax Description

statistics	Keyword to clear total packets switched and total packets exported (for NDE).
statistics protocol	Keywords to clear protocols for statistics collection.
protocol	Number of the protocol in the protocol statistics list.
port	Number of the port.
all	Keyword to clear all entries from the statistics protocol list.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

To use a router as an MLS, you must meet these conditions:

- The router must be included (either explicitly or automatically) in the MLS-SE.
- The MLS feature must be enabled in the Catalyst 6000 family switches.
- Catalyst 6000 family switches must know the router's MAC-VLAN pairs.

If you enter any of the **clear mls statistics** commands on a Catalyst 6000 family switch without MLS, this warning message displays:

```
Feature not supported in hardware.
```

When you remove an MSM from the Catalyst 6000 family switch, it is removed immediately from the inclusion list and all the MLS entries for the MSM are removed.

Examples

This example shows how to clear IP MLS statistics, including total packets switched and total packets exported (for NDE):

```
Console> (enable) clear mls statistics
Netflow data export statistics cleared.
Console> (enable)
```

This example shows how to clear protocol 17, port 19344 from the statistics collection:

```
Console> (enable) clear mls statistics protocol 17 19344
Protocol 17 port 1934 cleared from protocol statistics list.
Console> (enable)
```

Related Commands

set mls statistics protocol
show mls statistics

clear mls statistics entry

Use the **clear mls statistics entry** command to clear statistics for MLS entries.

clear mls statistics entry [**ip** | **ipx**] **all**

clear mls statistics entry ip [**destination** *ip_addr_spec*] [**source** *ip_addr_spec*] [**protocol** *protocol*] [**src-port** *src_port*] [**dst-port** *dst_port*]

clear mls statistics entry ipx destination *ipx_addr_spec*

Syntax Description

ip	(Optional) Keyword to specify IP MLS.
ipx	(Optional) Keyword to specify IPX MLS.
all	Keyword to purge all matching MLS entries.
destination	(Optional) Keyword to specify the destination IP address.
ip_addr_spec	(Optional) Full IP address or a subnet address in these formats: *ip_addr*, *ip_addr/netmask*, or *ip_addr/maskbit*.
source	(Optional) Keyword to specify the source IP address.
protocol *protocol*	(Optional) Keyword and variable to specify additional flow information (protocol family and protocol port pair) to be matched; valid values are from **0** to **255** or **ip**, **ipinip**, **icmp**, **igmp**, **tcp**, and **udp**.
src-port *src_port*	(Optional) Keyword and variable to specify the source port IP address; valid values are from **1** to **65535**, **dns**, **ftp**, **smtp**, **telnet**, **x** (X-Windows), **www**.
dst-port *dst_port*	(Optional) Keyword and variable to specify the destination port IP address; valid values are from **1** to **65535**, **dns**, **ftp**, **smtp**, **telnet**, **x** (X-Windows), **www**.
ipx_addr_spec	(Optional) Full IPX address or a subnet address in these formats: *src_net/*[*mask*], *dest_net.dest_node*, or *dest_net/mask*.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When specifying the **ip** | **ipx** keyword, if you specify **ip** or do not enter a keyword, this means that the command is for IP MLS. If you specify **ipx**, this means the command is for IPX only.

When you remove an MSM from the Catalyst 6000 family switch, it is removed immediately from the inclusion list and all the MLS entries for the MSM are removed.

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

- IPX net 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)

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

To use a router as an MLS, you must meet these conditions:

- The router must be included (either explicitly or automatically) in the MLS-SE.
- The MLS feature must be enabled in the Catalyst 6000 family switches.
- Catalyst 6000 family switches must know the router's MAC-VLAN pairs.

Use the following syntax to specify an IP subnet address:

- *ip_subnet_addr*—This is the 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.
- *ip_addr/subnet_mask*—This is the 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* is a full host address, such as 172.22.253.1/255.255.252.00.
- *ip_addr/maskbits*—This is the 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* is a full host address, such as 193.22.253.1/22, which has the same subnet address as the *ip_subnet_addr*.

A 0 value for *src_port* and *dest_port* clears all entries. Unspecified options are treated as wildcards, and all entries are cleared.

If you enter any of the **clear mls** commands on a Catalyst 6000 family switch without MLS, this warning message displays:

```
Feature not supported in hardware.
```

Examples

This example shows how to clear all specific MLS entries:

```
Console> (enable) clear mls statistics entry ip all
Multilayer switching entry cleared
Console> (enable)
```

This example shows how to clear specific IPX MLS entries for a destination IPX address:

```
Console> (enable) clear mls statistics entry ipx destination 1.0002.00e0.fefc.6000
MLS IPX entry cleared.
Console> (enable)
```

Related Commands

show mls

clear module password

Use the **clear module password** command to clear the password set by the **password** [*username*] NAM command.

clear module password *mod*

Syntax Description

mod	Number of the NAM.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is supported by the NAM only.

The **password** [*username*] command is a NAM command and not a supervisor engine console command.

A message is displayed when the password is successfully cleared. See the "Examples" section for an example of the message.

Examples

This example shows how to clear the password from the NAM:

```
Console> (enable) clear module password 6
Module 6 password cleared.
Console> (enable) 2000 Apr 07 11:03:06 %SYS-5-MOD_PASSWDCLR:Module 6 password cl
eared from telnet/10.6.1.10/tester
Console> (enable)
```

Related Commands

password (refer to the *NAM Installation and Configuration Note*)

clear multicast router

Use the **clear multicast router** command to clear manually configured multicast router ports from the multicast router port list.

clear multicast router {*mod/port* | **all**}

Syntax Description

mod/port	Number of the module and the port on the module.
all	Keyword to specify all multicast router ports to be cleared.

Defaults

The default configuration has no multicast router ports configured.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear multicast router port 1 on module 3:

```
Console> (enable) clear multicast router 3/1
Port 3/1 cleared from multicast router port list.
Console> (enable)
```

Related Commands

set multicast router
show multicast router

clear ntp server

Use the **clear ntp server** command to remove one or more servers from the NTP server table.

clear ntp server {*ip_addr* | **all**}

Syntax Description

ip_addr	IP address of the server to remove from the server table.
all	Keyword to specify all server addresses in the server table to be removed.

Defaults

The default configuration has no NTP servers configured.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to remove a specific NTP server from the server table:

```
Console> (enable) clear ntp server 172.20.22.191
NTP server 172.20.22.191 removed.
Console> (enable)
```

This example shows how to remove all NTP servers from the server table:

```
Console> (enable) clear ntp server all
All NTP servers cleared.
Console> (enable)
```

Related Commands

set ntp server
show ntp

clear ntp timezone

Use the **clear ntp timezone** command to return the time zone to its default, UTC.

clear ntp timezone

Syntax Description

This command has no arguments or keywords.

Defaults

The default time zone is UTC.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **clear ntp timezone** command functions only when NTP is running. If you set the time manually and NTP is disengaged, the **clear ntp timezone** command has no effect.

Examples

This example shows how to clear the time zone:

```
Console> (enable) clear ntp timezone
This command will clear NTP timezone and summertime zonename
Do you want to continue (y/n) [n]? y
Timezone name and offset cleared
Console> (enable)
```

Related Commands

set ntp timezone
show ntp

clear pbf

Use the **clear pbf** command to remove the MAC address for the PFC2.

clear pbf

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Refer to the "Configuring Policy-Based Forwarding" section of Chapter 16, "Configuring Access Control," in the *Catalyst 6000 Family Software Configuration Guide* for detailed information about PBF.

Examples

```
Console> (enable) clear pbf
PBF cleared
Console> (enable)
```

Related Commands

set pbf
show pbf

clear port broadcast

Use the **clear port broadcast** command to disable broadcast/multicast suppression on one or more ports.

clear port broadcast *mod/port*

Syntax Description

mod/port	Number of the module and the port on the module.

Defaults

The default configuration has broadcast/multicast suppression cleared (that is, unlimited broadcast/multicast traffic allowed).

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to disable broadcast/multicast suppression:

```
Console> (enable) clear port broadcast 2/1
Broadcast traffic unlimited on ports 2/1.
Console> (enable)
```

Related Commands

set port broadcast
show port broadcast

clear port cops

Use the **clear port cops** command to clear port roles.

clear port cops *mod*/*port* **roles** *role1* [*role2*]...

clear port cops *mod*/*port* **all-roles**

Syntax Description

mod/port	Number of the module and the port on the module.
roles *role#*	Keyword and variable to specify the roles to clear.
all-roles	Keyword to clear all roles.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **clear port cops** command detaches the roles from the port only; it does not remove them from the global table.

Examples

This example shows how to remove specific roles from a port:

```
Console> (enable) clear port cops 3/1 roles backbone_port main_port
Roles cleared for port(s) 3/1-4.
Console> (enable)
```

This example shows how to remove all roles from a port:

```
Console> (enable) clear port cops 3/1 all-roles
All roles cleared for port 3/1-4.
Console> (enable)
```

Related Commands

set port cops
show port cops

clear port host

Use the **clear port host** command to clear the port configuration for optimizing a host connection.

clear port host *mod/port*

Syntax Description

mod/port	Number of the module and the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

The **clear port host** command sets channel mode to auto, disables spanning tree PortFast, and sets the trunk mode to auto.

Examples

This example shows how to remove specific roles from a port:

```
Console> (enable) clear port host 5/5
Port(s)  5/5 trunk mode set to auto.
Spantree port  5/5 fast start disabled.
Port(s) 5/5 channel mode set to auto.
Console> (enable)
```

Related Commands

set port host

clear port qos cos

Use the **clear port qos cos** command to return the values set by the **set port qos cos** command to the default settings for all specified ports.

clear port qos *mod/ports..* **cos**

Syntax Description

mod/ports..	Number of the module and ports on the module.

Defaults

The default CoS for a port is 0.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to return the values set by the **set port qos cos** command to the default settings for module 2, port 1:

```
Console> (enable) clear port qos 2/1 cos
Port 2/1 qos cos setting cleared.
Console> (enable)
```

Related Commands

set port qos cos
show port qos

clear port security

Use the **clear port security** command to clear all MAC addresses or a specific MAC address from the list of secure MAC addresses on a port.

clear port security *mod*/*port* {*mac_addr* | **all**}

Syntax Description

mod/*port*	Number of the module and the port on the module.
mac_addr	MAC address to be deleted.
all	Keyword to remove all MAC addresses.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to remove a specific MAC address from a port's list of secure addresses:

```
Console> (enable) clear port security 4/1 00-11-22-33-44-55
00-11-22-33-44-55 cleared from secure address list list for port 4/1.
Console> (enable)
```

Related Commands

set port security
show port security

clear pvlan mapping

Use the **clear pvlan mapping** command to delete a private VLAN mapping.

clear pvlan mapping *primary_vlan* {*isolated_vlan* | *community_vlan* | *twoway_community_vlan*} *mod/port*

clear pvlan mapping *mod/port*

Syntax Description

primary_vlan	Number of the primary VLAN.
isolated_vlan	Number of the isolated VLAN.
community_vlan	Number of the community VLAN.
twoway_community_vlan	Number of the two-way community VLAN.
mod/port	Number of the module and promiscuous port.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not specify the mapping to clear, all the mappings of the specified promiscuous ports are cleared.

Examples

This example shows how to clear the mapping of VLAN 902 to 901, previously set on ports 3/2-5:

```
Console> (enable) clear pvlan mapping 901 902 3/2-5
Successfully cleared mapping between 901 and 902 on 3/2-5
Console> (enable)
```

Related Commands

clear config pvlan
clear vlan
set pvlan
set pvlan mapping
set vlan
show pvlan
show pvlan mapping
show vlan

clear qos acl

Use the **clear qos acl** command to remove various ACL configurations.

clear qos acl *acl_name* [*editbuffer_index*]

clear qos acl default-action {**ip** | **ipx** | **mac** | **all**}

clear qos acl map {*acl_name*} {*mod/port* | *vlan*}

clear qos acl map {*acl_name* | *mod/port* | *vlan* | **all**}

Syntax Description

acl_name	Unique name that identifies the list to which the entry belongs.
editbuffer_index	(Optional) ACE position in the ACL.
default-action	Keyword to remove default actions.
ip	Keyword to clear IP ACE default actions.
ipx	Keyword to clear IPX ACE default actions.
mac	Keyword to clear MAC-layer ACE default actions.
all	Keyword to clear all ACE default actions.
map	Keyword to detach an ACL.
mod/port	Number of the module and the port on the module.
vlan	Number of the VLAN; valid values are from **1** to **1000** and from **1025** to **4094**.
all	Keyword to detach an ACL from all interfaces.

Defaults

The default is no ACLs are attached.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Changes you make by entering this command are saved to NVRAM and hardware only after you enter the **commit** command.

Use the **show qos acl editbuffer** command to display the ACL list.

Examples

This example shows how to detach an ACL from all interfaces:

```
Console> (enable) clear qos acl map my_acl all
Hardware programming in progress...
ACL my_acl is detached from all interfaces.
Console> (enable)
```

This example shows how to detach an ACL from a specific VLAN:

```
Console> (enable) clear qos acl map ftp_acl 4
Hardware programming in progress...
ACL ftp_acl is detached from vlan 4.
Console> (enable)
```

This example shows how to delete a specific ACE:

```
Console> (enable) clear qos acl my_ip_acl 1
ACL my_ip_acl ACE# 1 is deleted.
my_ip_acl editbuffer modified. Use ‘commit’ command to apply changes.
Console> (enable)
```

This example shows how to delete an ACL:

```
Console> (enable) clear qos acl my_ip_acl
ACL my_ip_acl is deleted.
my_ip_acl editbuffer modified. Use ‘commit’ command to apply changes.
Console> (enable)
```

This example shows how to detach a specific ACL from all interfaces:

```
Console> (enable) clear qos acl map my_acl all
Hardware programming in progress...
ACL my_acl is detached from all interfaces.
Console> (enable)
```

This example shows how to detach a specific ACL from a specific VLAN:

```
Console> (enable) clear qos acl map ftp_acl 4
Hardware programming in progress...
ACL ftp_acl is detached from vlan 4.
Console> (enable)
```

This example shows how to delete IP ACE default actions configured by the **set qos acl default-action** command:

```
Console> (enable) clear qos acl default-action ip
Hardware programming in progress...
QoS default-action for IP ACL is restored to default setting.
Console> (enable)
```

Related Commands

commit
rollback
show qos acl editbuffer

clear qos config

Use the **clear qos config** command to return the values set by the **set qos** command to the default settings and delete the CoS assigned to MAC addresses.

clear qos config

Syntax Description

This command has no arguments or keywords.

Defaults

The default is QoS is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to return the values set by the **set qos** command to the default settings and delete the CoS assigned to MAC addresses:

```
Console> (enable) clear qos config
This command will disable QoS and take values back to factory default.
Do you want to continue (y/n) [n]? y
QoS config cleared.
Console> (enable)
```

Related Commands

set qos
show qos info

clear qos cos-dscp-map

Use the **clear qos cos-dscp-map** command to clear CoS-to-DSCP mapping set by the **set qos cos-dscp-map** command and return to the default setting.

clear qos cos-dscp-map

Syntax Description

This command has no arguments or keywords.

Defaults

The default CoS-to-DSCP configuration is listed in Table 2-2.

Table 2-2 CoS-to-DSCP Default Mapping

CoS	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear the CoS-to-DSCP mapping table:

```
Console> (enable) clear qos cos-dscp-map
QoS cos-dscp-map setting restored to default.
Console> (enable)
```

Related Commands

set qos cos-dscp-map
show qos maps

clear qos dscp-cos-map

Use the **clear qos dscp-cos-map** command to clear DSCP-to-CoS mapping set by the **set qos dscp-cos-map** command and return to the default setting.

clear qos dscp-cos-map

Syntax Description

This command has no arguments or keywords.

Defaults

The default DSCP-to-CoS configuration is listed in Table 2-3.

Table 2-3 DSCP-to-CoS Default Mapping

DSCP	0 to 7	8 to 15	16 to 23	24 to 31	32 to 39	40 to 47	48 to 55	56 to 63
CoS	0	1	2	3	4	5	6	7

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear the DSCP-to-CoS mapping table:

```
Console> (enable) clear qos dscp-cos-map
QoS dscp-cos-map setting restored to default.
Console> (enable)
```

Related Commands

set qos dscp-cos-map
show qos maps

clear qos ipprec-dscp-map

Use the **clear qos ipprec-dscp-map** command to reset the mapping set by the **set qos ipprec-dscp-map** command to the default setting.

clear qos ipprec-dscp-map

Syntax Description

This command has no arguments or keywords.

Defaults

The default IP precedence-to-DSCP configuration is listed in Table 2-4.

Table 2-4 IP Precedence-to-DSCP Default Mapping

IPPREC	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear the IP precedence-to-DSCP mapping table:

```
Console> (enable) clear qos ipprec-dscp-map
QoS ipprec-dscp-map setting restored to default.
Console> (enable)
```

Related Commands

set qos ipprec-dscp-map
show qos maps

clear qos mac-cos

Use the **clear qos mac-cos** command to clear the values set by the **set qos mac-cos** command.

clear qos mac-cos *dest_mac* [*vlan*]

clear qos mac-cos all

Syntax Description

dest_mac	Number of the destination host MAC address.
vlan	(Optional) Number of the VLAN; valid values are from **1** to **1000** and from **1025** to **4094**.
all	Keyword to clear CoS values for all MAC/VLAN pairs.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If the *vlan* number is not entered, all entries for the MAC address are cleared.

Examples

This example shows how to clear the values set by the **set qos mac-cos** command and return to the default settings for all MAC address and VLAN pairs:

```
Console> (enable) clear qos mac-cos all
All CoS to Mac/Vlan entries are cleared.
Console> (enable)
```

This example shows how to clear the values set by the **set qos mac-cos** command and return to the default settings for a specific MAC address:

```
Console> (enable) clear qos mac-cos 1-2-3-4-5-6 1
CoS to Mac/Vlan entry for mac 01-02-03-04-05-06 vlan 1 is cleared.
Console> (enable)
```

Related Commands

set qos mac-cos
show qos mac-cos

clear qos map

Use the **clear qos map** command to return the values to the default settings.

clear qos map *port_type* **tx** | **rx**

Syntax Description

port_type	Port type; valid values are **2q2t**, **1p3q1t**, and **1p2q2t** for transmit and **1p1q4t** and **1p1q0t** for receive. See the "Usage Guidelines" section for additional information.
tx | **rx**	Keyword to specify the transmit or receive queue.

Defaults

The default mappings for all ports are shown in Table 2-5 and Table 2-6 and applies to all ports.

Table 2-5 Default Transmit Queue and Drop-Threshold Mapping of CoS Values

Port Type	Drop Threshold Type	Low Delay (Queue 2)	High Delay (Queue 1)	Priority Delay (Queue 3)
2q2t	Low drop (Threshold 2)	7, 6	3, 2	N/A
	High drop (Threshold 1)	5, 4	1, 0	N/A
1p2q2t	Low drop (Threshold 2)	7	3, 2	N/A
	High drop (Threshold 1)	5, 4	1, 0	5

Table 2-6 Default Receive Drop-Threshold Mapping of CoS Values

Port Type	Threshold 1 (highest drop)	Threshold 2	Threshold 3	Threshold 4 (lowest drop)	Priority Queue
1p1q0t	0, 1	2, 3	4, 5	7	6
1p1q4t	0, 1	2, 3	4, 5	7	6

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **1p2q1t** and **1p1q8t** port types are not supported.

Examples

This example shows how to return the values to the default settings:

```
Console> (enable) clear qos map 2q2t
This command will take map values back to factory default.
QoS map cleared.
Console> (enable)
```

Related Commands

set qos map
show qos maps

clear qos policed-dscp-map

Use the **clear qos policed-dscp-map** to reset the policer-to-dscp mapping table to the defaults.

clear qos policed-dscp-map

Syntax Description

This command has no arguments or keywords.

Defaults

The default is the identity function; for example, DSCP 63 to policed DSCP 63 and DSCP 62 to policed DSCP 62.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to reset the mapping to the defaults:

```
Console> (enable) clear qos policed-dscp-map
QoS policed-dscp-map setting restored to default.
Console> (enable)
```

Related Commands

set qos policed-dscp-map
show qos maps

clear qos policer

Use the **clear qos policer** command to clear policing rules from NVRAM.

clear qos policer microflow *microflow_name* | **all**

clear qos policer aggregate *aggregate_name* | **all**

Syntax Description

microflow *microflow_name*	Keyword and variable to specify the name of the microflow policing rule.
aggregate *aggregate_name*	Keyword and variable to specify the name of the aggregate policing rule.
all	Keyword to clear all policing rules.

Defaults

This command has no default setting in systems configured with the Supervisor Engine 1 with Layer 3 Switching Engine (PFC); in systems configured with Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2), the default is to apply the given map to the normal rate only.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Policing is the process by which the switch limits the bandwidth consumed by a flow of traffic. Policing can mark or drop traffic.

You cannot clear an entry that is currently being used in an ACE. You must first detach the ACEs from the interface.

You cannot use the **all** keyword if a microflow rate limit is currently being used in an ACE.

The **normal** and **excess** keywords are supported on systems configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) only. With these keywords, you can specify a map for the normal rate and one for the excess rate. Because this selection is optional in the CLI, the default (unspecified) action is to apply the given map to the normal rate only.

This example shows how to clear a specific microflow policing rule:

```
Console> (enable) clear qos policer microflow my_micro
my_micro QoS microflow policer cleared.
Console> (enable)
```

This example shows how to clear all microflow policing rules:

```
Console> (enable) clear qos policer microflow all
All QoS microflow policers cleared.
Console> (enable)
```

This example shows how to clear a specific aggregate policing rule:

```
Console> (enable) clear qos policer aggregate my_micro
my_micro QoS microflow policer cleared.
Console> (enable)
```

This example shows how to clear all aggregate policing rules:

```
Console> (enable) clear qos policer aggregate all
All QoS aggregate policer cleared.
Console> (enable)
```

Related Commands

set qos policer
show qos policer

clear qos statistics

Use the **clear qos statistics** command to clear QoS statistic counters.

clear qos statistics [**aggregate-policer** [*policer_name*]]

Syntax Description

aggregate-policer	(Optional) Keyword to clear QoS aggregate policer statistics.
policer_name	(Optional) Name of the aggregate policer.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you enter the **clear qos statistics** command without the entering the **aggregate-policer** keyword, all QoS statistics are cleared, including all QoS aggregate policer statistics.

If you enter the **aggregate-policer** keyword without specifying a policer name, all aggregate policer statistics are cleared.

Examples

This example shows how to clear the QoS statistic counters:

```
Console> (enable) clear qos statistics
QoS statistical cleared.
Console> (enable)
```

This example shows how to clear all QoS aggregate policer statistics:

```
Console> (enable) clear qos statistics aggregate-policer
QoS aggregate policers statistical counters cleared.
Console> (enable)
```

This example shows how to clear the QoS aggregate policer statistics for aggr_1:

```
Console> (enable) clear qos statistics aggregate-policer aggr_1
Aggregate policer 'aggr_1' statistical counters cleared.
Console> (enable)
```

Related Commands

show qos statistics

clear radius

Use the **clear radius** command to clear one or all of the RADIUS servers from the RADIUS server table or remove a shared key entry.

clear radius server all

clear radius server *ipaddr*

clear radius key

Syntax Description

server	Keyword to specify RADIUS servers.
all	Keyword to specify all RADIUS servers.
ipaddr	Number of the IP address or IP alias.
key	Keyword to specify the RADIUS shared key.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

ipaddr is an IP alias or an IP address in dot notation; for example, 101.102.103.104.

Examples

This example shows how to clear the RADIUS key:

```
Console> (enable) clear radius key
Radius server key cleared.
Console> (enable)
```

This example shows how to clear a specific RADIUS server from the RADIUS server table:

```
Console> (enable) clear radius server 128.56.45.32
128.56.45.32 cleared from radius server table.
Console> (enable)
```

Related Commands

set radius key
set radius server
show radius

clear rcp

Use the **clear rcp** command to clear rcp information for file transfers.

clear rcp

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear rcp information:

```
Console> (enable) clear rcp
Console> (enable)
```

Related Commands

set rcp username
show rcp

clear rgmp statistics

Use the **clear rgmp statistics** command to clear RGMP statistics information for all VLANs.

clear rgmp statistics

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Types Switch command.

Command Modes Privileged.

Examples This example shows how to clear the RGMP statistics on the switch:

```
Console> (enable) clear rgmp statistics
RGMP statistics cleared.
Console> (enable)
```

Related Commands **set rgmp**
show rgmp statistics

clear security acl

Use the **clear security acl** command to remove a specific ACE or all ACEs from a VACL and delete the VACLs from the edit buffer.

clear security acl all

clear security acl *acl_name*

clear security acl capture-ports {**all** | *mod/ports*}

clear security acl log flow

clear security acl *acl_name* [*editbuffer_index*]

clear security acl adjacency *adjacency_name*

clear security acl map {*acl_name* | *vlan* | **all**}

Syntax Description

all	Keyword to remove ACEs for all the VACLs.
acl_name	Name of the VACL whose ACEs are to be removed.
capture-ports	Keyword to remove ports from the capture list.
all	Keyword to remove all ports from the capture list.
mod/ports	Variable to remove specific port from the capture list; *mod/num* is the number of the module and the port on the module.
log flow	Keywords to remove logging table flow entries.
editbuffer_index	(Optional) Index number of the ACE in the VACL.
adjacency	Keyword to remove an adjacency ACE.
adjacency_name	Name of the adjacency ACE.
map	Keyword to clear security ACL to a VLAN mapping.
vlan	Variable to clear ACL mappings for a specific VLAN.
all	Keyword to clear all ACL VLAN mappings.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Changes you make by entering this command are saved to NVRAM and hardware only after you enter the **commit** command.

Use the **show security acl** command to display the VACL list.

The adjacency ACE cannot be cleared before the redirect ACE. The redirect ACE and the adjacency ACE in PBF VACLs should be cleared in the following order:

1. Clear the redirect ACE.
2. Commit the VACL.
3. Clear the adjacency ACE.
4. Commit the adjacency.

Examples

This example shows how to remove ACEs for all the VACLs:

```
Console> (enable) clear security acl all
All editbuffer modified. Use ‘commit’ command to apply changes.
Console> (enable)
```

This example shows how to remove a specific ACE from a specific VACL:

```
Console> (enable) clear security acl IPACL1 2
IPACL1 editbuffer modified. Use ‘commit’ command to apply changes.
Console> (enable)
```

This example shows how to remove an adjacency ACE:

```
Console> (enable) clear security acl adjacency a_1
a_1 editbuffer modified. Use ’commit’ command to apply changes.
Console> (enable)
```

Related Commands

commit
rollback
show security acl

clear security acl capture-ports

Use the **clear security acl capture-ports** command to remove a port from the capture port list.

clear security acl capture-ports {*mod/ports...*}

Syntax Description

mod/ports...	Number of the module and the ports on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Configurations you make by entering this command are saved in NVRAM. This command *does not* require that you enter the **commit** command.

If you have a number of ports and a few are removed, the remaining ports continue to capture the traffic.

Examples

This example shows how to remove entries from the capture port list:

```
Console> (enable) clear security acl capture-ports 1/1,2/1
Successfully cleared the following ports:
1/1,2/1
Console> (enable)
```

Related Commands

set security acl capture-ports
show security acl capture-ports

clear security acl log flow

Use the **clear security acl log flow** command to clear all flows in the security ACL log table.

clear security acl log flow

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is supported on systems configured with Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) only.

Examples

This example shows how to clear all flows in the security ACL log table:

```
Console> (enable) clear security acl log flow
Security acl log table cleared successfully
Console> (enable)
```

Related Commands

set security acl log
show security acl log

clear security acl map

Use the **clear security acl map** command to remove VACL-to-VLAN mapping.

clear security acl map *acl_name vlan*

clear security acl map {*acl_name* | *vlan* | **all**}

Syntax Description

acl_name	Name of the VACL whose VLAN is to be deleted.
vlan	Number of the VLAN whose mapping is to be deleted; valid values are from **1** to **1000** and from **1025** to **4094**.
all	Keyword to remove all VACL-to-VLAN mappings.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Changes you make by entering this command are saved to NVRAM and do not require you to enter the **commit** command.

Use the **show security acl** command to display the ACL list.

Examples

This example shows how to remove a VACL-to-VLAN mapping from a specific VLAN:

```
Console> (enable) clear security acl map ip1 3
Map deletion in progress.

Successfully cleared mapping between ACL ip1 and VLAN 3.
Console> (enable)
```

This example shows how to remove a specific VACL-to-VLAN mapping from all VLANs:

```
Console> (enable) clear security acl map ip1
Map deletion in progress.

Successfully cleared mapping between ACL ip1 and VLAN 5.

Successfully cleared mapping between ACL ip1 and VLAN 8.
Console> (enable)
```

This example shows how to remove all VACL-to-VLAN mappings from a specific VLAN:

```
Console> (enable) clear security acl map 5
Map deletion in progress.

Successfully cleared mapping between ACL ipx1 and VLAN 5.

Successfully cleared mapping between ACL mac2 and VLAN 5.
Console> (enable)
```

This example shows how to remove all VACL-to-VLAN mappings from all VLANs:

```
Console> (enable) clear security acl map all
Map deletion in progress.

Successfully cleared mapping between ACL ip2 and VLAN 12.

Successfully cleared mapping between ACL ipx1 and VLAN 12.

Successfully cleared mapping between ACL ipx1 and VLAN 45.

Successfully cleared mapping between ACL ip2 and VLAN 47.

Successfully cleared mapping between ACL ip3 and VLAN 56.
Console> (enable)
```

Related Commands

commit
rollback
show security acl

clear snmp access

Use the **clear snmp access** command to remove the access rights of an SNMP group.

clear snmp access [**-hex**] {*groupname*} {**security-model** {**v1** | **v2c**}}

clear snmp access {**security-model v3** {**noauthentication** | **authentication** | **privacy**}} [**context** [**-hex**] *contextname*]

Syntax Description

-hex	(Optional) Keyword to display the *groupname* or *contextname* in a hexadecimal format.
groupname	SNMP access table name.
security-model v1 | **v2c**	Keywords to specify the security model v1 or v2c.
security-model v3	Keywords to specify security model v3.
noauthentication	Keyword to specify groups with security model type set to noauthentication.
authentication	Keyword to specify groups with security model type authentication protocol.
privacy	Keyword to specify groups with security model type privacy.
context *contextname*	(Optional) Keyword and variable to specify the name of a context string.

Defaults

The default *contextname* is a NULL string.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use special characters for *groupname* (nonprintable delimiters for this parameter), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

If you do not enter a context name, a NULL context string is used.

Examples

This example shows how to clear SNMP access for a group:

```
Console> (enable) clear snmp access cisco-group security-model v3 authentication
Cleared snmp access cisco-group version v3 level authentication.
Console> (enable)
```

Related Commands

set snmp access
show snmp access
show snmp context

clear snmp community

Use the **clear snmp community** command to remove the mappings between different community strings and security modes.

clear snmp community index [**-hex**] {*index_name*}

Syntax Description

index	Keyword to specify clearing an index.
-hex	(Optional) Keyword to display the *index_name* in a hexadecimal format.
index_name	Name of the SNMP index.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use special characters for *index_name* (nonprintable delimiters for this parameter), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

If you do not enter an *index_name*, a NULL context string is used.

Examples

This example shows how to clear SNMP access for a group:

```
Console> (enable) clear snmp community index ind1
Cleared snmp community ind1.
Console> (enable)
```

Related Commands

set snmp community
show snmp community

clear snmp group

Use the **clear snmp group** command to remove the SNMP user from an SNMP group.

clear snmp group [**-hex**] *groupname* {**user** [**-hex**] *username*} {**security-model** {**v1** | **v2c** | **v3**}}

Syntax Description

-hex	(Optional) Keyword to display the *groupname* and *username* as a hexadecimal format.
groupname	Name of the SNMP group that defines an access control.
user	Keyword to specify the SNMP group username.
username	Name of the SNMP user.
security model v1 | **v2c** | **v3**	Keywords to specify security model v1, v2c, or v3.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use special characters for *groupname* or *username* (nonprintable delimiters for these parameters), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

Examples

This example shows how to remove an SNMP user from a group:

```
Console> (enable) clear snmp group cisco-group user joe security-model v3
Cleared snmp group cisco-group user joe version v3.
Console> (enable)
```

Related Commands

set snmp group
show snmp group

clear snmp notify

Use the **clear snmp notify** command to clear the SNMP notifyname in the snmpNotifyTable.

clear snmp notify [**-hex**] {*notifyname*}

Syntax Description

-hex	(Optional) Keyword to display the *notifyname* as a hexadecimal format.
notifyname	Identifier to index the snmpNotifyTable.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use special characters for *notifyname* (nonprintable delimiters for this parameter), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

Examples

This example shows how to clear an SNMP notifyname from the snmpNotifyTable:

```
Console> (enable) clear snmp notify joe
Cleared SNMP notify table joe.
Console> (enable)
```

Related Commands

set snmp notify
show snmp notify

clear snmp targetaddr

Use the **clear snmp targetaddr** command to clear the SNMP target address entry in the TargetAddressTable.

clear snmp targetaddr [**-hex**] {*addrname*}

Syntax Description

-hex	(Optional) Keyword to display the *addrname* as a hexadecimal format.
addrname	Name of the target agent; the maximum length is 32 bytes.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use special characters for *addrname* (nonprintable delimiters for this parameter), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

Examples

This example shows how to clear an SNMP target address entry in the snmpTargetAddressTable:

```
Console> (enable) clear snmp targetaddr joe
Cleared SNMP targetaddr joe.
Console> (enable)
```

Related Commands

set snmp targetaddr
show snmp targetaddr

clear snmp targetparams

Use the **clear snmp targetparams** command to clear the SNMP target parameters used in the snmpTargetParamsTable.

clear snmp targetparams [**-hex**] {*paramsname*}

Syntax Description

-hex	(Optional) Keyword to display the *paramsname* as a hexadecimal format.
paramsname	Name of the target parameter in the snmpTargetParamsTable; the maximum length is 32 bytes.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use special characters for *paramsname* (nonprintable delimiters for this parameter), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

Examples

This example shows how to remove the SNMP target parameters:

```
Console> (enable) clear snmp targetparams joe
Cleared SNMP targetparams table joe.
Console> (enable)
```

Related Commands

set snmp targetparams
show snmp targetparams

clear snmp trap

Use the **clear snmp trap** command to clear an entry from the SNMP trap receiver table.

clear snmp trap {*rcvr_addr*} [**all**]

Syntax Description

rcvr_addr	IP address or IP alias of the trap receiver (the SNMP management station) to clear.
all	(Optional) Keyword to specify every entry in the SNMP trap receiver table.

Defaults

The default configuration has no entries in the SNMP trap receiver table.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear an entry from the SNMP trap receiver table:

```
Console> (enable) clear snmp trap 192.122.173.82
SNMP trap receiver deleted.
Console> (enable)
```

Related Commands

set snmp trap
show port counters
test snmp trap

clear snmp user

Use the **clear snmp user** command to remove an SNMP user.

clear snmp user [**-hex**] {*username*} [**remote** *engineid*]

Syntax Description

-hex	(Optional) Keyword to display the *username* as a hexadecimal format.
username	Name of the user on the host that connects to the agent.
remote *engineid*	(Optional) Keyword and variable to specify the *username* on a remote SNMP engine.

Defaults

If a remote engine ID is not provided, the default local SNMP engine ID is used.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use special characters for *username* (nonprintable delimiters for this parameter), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

Examples

This example shows how to remove a user from an SNMP group:

```
Console> (enable) clear snmp user joe
Cleared SNMP user joe.
Console> (enable)
```

This example shows how to remove a user on a remote SNMP engine:

```
Console> (enable) clear snmp user joe remote 00:00:00:09:00:d0:00:4c:18:00
Cleared SNMP user.
Console> (enable)
```

Related Commands

set snmp user
show snmp user

clear snmp view

Use the **clear snmp view** command to remove the MIB view entry from the vacmViewTreeFamilyTable.

clear snmp view [**-hex**] {*viewname subtree*}

Syntax Description

-hex	(Optional) Keyword to display the *viewname* as a hexadecimal format.
viewname	Name of a MIB view.
subtree	Name of the subtree.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use special characters for *viewname* (nonprintable delimiters for this parameter), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

A MIB subtree used with a mask defines a view subtree that can be in OID format or a text name mapped to a valid OID.

Examples

This example shows how to clear the SNMP MIB viewname:

```
Console> (enable) clear snmp view myview 1.1.3
Cleared snmp view myview with subtree 1.1.3
Console> (enable)
```

Related Commands

set snmp view
show snmp view

clear spantree mst

Use the **clear spantree mst** command to clear the mapping of VLANs to an MST instance.

clear spantree mst *instance* [**vlan** *vlans*]

Syntax Description

instance	Number of the instance or range of instances; valid values are from **0** to **15**. See the "Usage Guidelines" section for more information.
vlan *vlans*	(Optional) Keyword and variable to specify the VLAN number; valid values are from **1** to **1005** and from **1025** to **4094**.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you enter only one instance number, you also can enter a VLAN number. If you enter a range of instance numbers, you cannot enter a VLAN number.

If you do not specify a VLAN, all VLANs are unmapped from the specified instance and added to MST instance 0 (IST).

Examples

This example shows you how to clear VLAN 2 from MST instance 2:

```
Console> (enable) clear spantree mst 2 vlan 2
Console> (enable)
```

Related Commands

set spantree mst redetect-protocol
show spantree mst

clear spantree portcost

Use the **clear spantree portcost** command to clear the port cost of a port on the switch.

clear spantree portcost *mod/port* [**mst**]

Syntax Description

mod/port	Number of the module and the port on the module.
mst	(Optional) Keyword to restore the default path cost to an MST instance on a port.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to restore the default path cost on a port:

```
Console> (enable) clear spantree portcost 3/1
Port 3/1 is using the cost 0.
Console> (enable)
```

This example shows how to restore the default path cost to all MST instances on a port:

```
Console> (enable) clear spantree portcost 8/1 mst
Port 8/1 MST is using the cost 20000 in MST mode.
Console> (enable)
```

Related Commands

set spantree portcost
show spantree statistics

clear spantree portinstancecost

Use the **clear spantree portinstancecost** command to restore the default path cost to an instance on a port.

clear spantree portinstancecost *mod/port* [**mst**] *instances*

Syntax Description

mod/port	Number of the module and the port on the module.
mst	(Optional) Keyword to restore the default path cost to an MST instance on a port.
instances	Number of the instance; valid values are from **0** to **15**.

Defaults

The default path cost is based on port speed; see Table 2-7 for default settings.

Table 2-7 Default Port Cost—Short Mode

Port Speed	Default Port Cost
4 Mb	250
10 Mb	100
16 Mb	62
100 Mb	19
155 Mb	14
1 Gb	4
10 Gb	2

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is valid in MISTP and MST modes only.

Examples

This example shows how to restore the default path cost to an instance on a port:

```
Console> (enable) clear spantree portinstancecost 5/1 2
Port 5/1 mistp-instance 1-16 have path cost 200000.
Console> (enable)
```

This example shows how to restore the default path cost to all MST instances on a port:

```
Console> (enable) clear spantree portinstancecost 8/1 mst 0-15
Port 8/1 MST Instance 0-15 have path cost 20000.
Console> (enable)
```

Related Commands set spantree portinstancecost
show spantree statistics

clear spantree portinstancepri

Use the **clear spantree portinstancepri** command to reset the spanning tree port instance priority.

clear spantree portinstancepri *mod/port* [**mst**] [*instances*]

Syntax Description

mod/port	Number of the module and the port on the module.
mst	(Optional) Keyword to reset the spanning tree port MST instance priority.
instances	(Optional) Number of the instance; valid values are from **0** to **15**.

Defaults

The default is the port priority is set to 0 with no instances specified.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is valid in MISTP and MST modes only.

Examples

This example shows how to reset the spanning tree port instance priority:

```
Console> (enable) clear spantree portinstancepri 5/1 2
Port 5/1 instances 1-16 using portpri 32.
Console> (enable)
```

This example shows how to reset the spanning tree port priority for all MST instances:

```
Console> (enable) clear spantree portinstancepri 8/1 mst 0-15
Port 8/1 MST Instances 0-15 using portpri 32
Console> (enable)
```

Related Commands

set spantree portinstancepri
show spantree

clear spantree portpri

Use the **clear spantree portpri** command to clear the port priority of a port on the switch.

clear spantree portpri *mod/port* [**mst**]

Syntax Description

mod/port	Number of the module and the port on the module.
mst	(Optional) Keyword to reset the spanning tree MST port priority.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear the spanning tree port priority:

```
Console> (enable) clear spantree portpri 3/1
Port 3/1 is using the cost 32.
Console> (enable)
```

This example shows how to clear the spanning tree MST port priority:

```
Console> (enable) clear spantree portpri 8/1 mst
Port 8/1 is using the priority 32 in MST mode.
Console> (enable)
```

Related Commands

set spantree portpri
show spantree

clear spantree portvlancost

Use the **clear spantree portvlancost** command to restore the default path cost to a VLAN on a port.

clear spantree portvlancost *mod/port* [*vlans*]

Syntax Description

mod/port	Number of the module and the port on the module.
vlans	(Optional) Number of the VLAN; valid values are from **1** to **1000** and from **1025** to **4094**.

Defaults

The default path cost is based on port speed; see Table 2-8 and Table 2-9 for default settings.

Table 2-8 Default Port Cost—Short Mode

Port Speed	Default Port Cost
4 Mb	250
10 Mb	100
16 Mb	62
100 Mb	19
155 Mb	14
1 Gb	4
10 Gb	2

Table 2-9 Default Port Cost—Long Mode

Port Speed	Default Port Cost
100 Kb	200,000,000
1 Mb	20,000,000
10 Mb	2,000,000
100 Mb	200,000
1 Gb	20,000
10 Gb	2,000
100 Gb	200
1 Tb	20
10 Tb	2

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is valid in PVST+ mode only.

If you do not specify a VLAN, all VLANs are cleared.

Examples

These examples show how to restore the default path cost to a VLAN on a port:

```
Console> (enable) clear spantree portvlancost 2/10 1-10
Port 2/10 VLANs 11-21 have path cost 6
Port 2/10 VLANs 1-10,22-1000 have path cost 10.
Console> (enable)

Console> (enable) clear spantree portvlancost 2/10
Port 2/10 VLANs 1-1000 have path cost 10.
Console> (enable)
```

Related Commands

set spantree portvlancost
show spantree statistics

clear spantree portvlanpri

Use the **clear spantree portvlanpri** command to reset the spanning tree port VLAN priority.

clear spantree portvlanpri *mod/port* [*vlans*]

Syntax Description

mod/port	Number of the module and the port on the module.
vlans	(Optional) Number of the VLAN; valid values are from **1** to **1000** and from **1025** to **4094**.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to reset the spanning tree port VLAN priority:

```
Console> (enable) clear spantree portvlanpri 1/2 23-40
Port 1/2 vlans 3,6-20,23-1000 using portpri 32
Port 1/2 vlans 1-2,4-5,21-22 using portpri 30
Console> (enable)
```

Related Commands

set spantree portvlanpri
show spantree

clear spantree root

Use the **clear spantree root** command to restore the spanning tree bridge priority, hello time, maxage, and forward delay on the switch to their default values.

clear spantree root [*vlans*]

clear spantree root mistp-instance *instances*

clear spantree root mst *instances*

Syntax Description

vlans	(Optional) Number of the VLAN; valid values are from **1** to **1000** and from **1025** to **4094**.
mistp-instance *instances*	Keyword and variable to specify the instance number; valid values are from **1** to **16**.
mst *instances*	Keyword and variable to specify the MST instance number; valid values are **0** to **15**.

Defaults

The defaults are as follows:

- switch priority is 32768
- forward delay is 15 seconds
- hello time is 2 seconds
- maxage is 20 seconds

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear the spanning tree root on a range of VLANs:

```
Console> (enable) clear spantree root 1-20
VLANs 1-20 bridge priority set to 32678.
VLANs 1-20 bridge hello time set to 2 seconds.
VLANs 1-20 bridge max aging time set to 20 seconds.
VLANs 1-20 bridge forward delay set to 15 seconds.
```

This example shows how to clear the spanning tree root on two specific VLANs:

```
Console> (enable) clear spantree root 22,24
VLANs 22,24 bridge priority set to 32678.
VLANs 22,24 bridge hello time set to 2 seconds.
VLANs 22,24 bridge max aging time set to 20 seconds.
VLANs 22,24 bridge forward delay set to 15 seconds.
Console> (enable)
```

This example shows how to clear the spanning tree root on an instance:

```
Console> (enable) clear spantree root mistp-instance 1
Instance 1 bridge priority set to 32768.
Instance 1 bridge max aging time set to 20.
Instance 1 bridge hello time set to 2.
Instance 1 bridge forward delay set to 15.
Console> (enable)
```

This example shows how to clear the spanning tree root on an MST instance:

```
Console> (enable) clear spantree root mst 0
MST Instance s 0 bridge priority set to 32768.
Instances 0 bridge max aging time set to 20.
Instances 0 bridge hello time set to 2.
Instances 0 bridge forward delay set to 15.
Console> (enable)
```

Related Commands

set spantree root
show spantree

clear spantree statistics

Use the **clear spantree statistics** command to clear the spanning tree statistics.

clear spantree statistics *mod/port*

clear spantree statistics *vlans*

clear spantree statistics mistp-instance *instances*

clear spantree statistics mst *instances*

Syntax Description

mod/port	Number of the module and the port on the module.
vlans	(Optional) Number of the VLAN; valid values are from **1** to **1000** and from **1025** to **4094**.
mistp-instance *instances*	Keyword and variable to specify the instance number; valid values are from **1** to **16**.
mst *instances*	Keyword and variable to specify the MST instance number; valid values are from **0** to **15**.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear the spanning tree statistics for VLAN 1:

```
Console> (enable) clear spantree statistics 1
Cleared all VLAN counters for VLAN 1
Statistics cleared for vlans 1
Console> (enable)
```

This example shows how to clear the spanning tree statistics for a port:

```
Console> (enable) clear spantree statistics 3/1
Statistics cleared for module 3/1
Console> (enable)
```

This example shows how to clear the spanning tree statistics for an instance:

```
Console> (enable) clear spantree statistics mistp-instance 2
Statistics cleared for instances 2
Console> (enable)
```

This example shows how to clear the spanning tree statistics for an MST instance:

```
Console> (enable) clear spantree statistics mst 0
Statistics cleared for MST instance: 0
Console> (enable)
```

Related Commands show spantree statistics

clear spantree uplinkfast

Use the **clear spantree uplinkfast** command to turn off the UplinkFast feature and to return the switch priority and port costs to the default settings.

clear spantree uplinkfast

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

In some cases, this command could cause load balancing on the switch to be lost.

Examples

This example shows how to turn off the UplinkFast feature and to return the switch priority to the default settings:

```
Console> (enable) clear spantree uplinkfast
This command will cause all portcosts, portvlancosts, and the
bridge priority on all vlans to be set to default.
Do you want to continue (y/n) [n]? y
VLANs 1-1005 bridge priority set to 32768.
The port cost of all bridge ports set to default value.
The portvlancost of all bridge ports set to default value.
uplinkfast disabled for bridge.
Console> (enable)
```

Related Commands

set spantree uplinkfast
show spantree uplinkfast

clear tacacs key

Use the **clear tacacs key** command to remove the key setting used for TACACS+ authentication and encryption.

clear tacacs key

Syntax Description

This command has no arguments or keywords.

Defaults

The default key value is null.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear the key setting used for authentication and encryption:

```
Console> (enable) clear tacacs key
TACACS server key cleared.
Console> (enable)
```

Related Commands

set tacacs key
show tacacs

clear tacacs server

Use the **clear tacacs server** command to remove a host from the list of TACACS+ servers.

clear tacacs server *ip_addr*

Syntax Description

ip_addr	IP address of the server to be removed from the list of TACACS+ servers.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to remove a server from the list of TACACS+ servers:

```
Console> (enable) clear tacacs server 170.1.2.20
170.1.2.20 cleared from TACACS table
Console> (enable)
```

Related Commands

show tacacs

clear timezone

Use the **clear timezone** command to return the time zone to its default, UTC.

clear timezone

Syntax Description

This command has no arguments or keywords.

Defaults

The default time zone is UTC.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **clear timezone** command functions only when NTP is running. If you set the time manually and NTP is disengaged, the **clear timezone** command has no effect.

Examples

This example shows how to clear the time zone:

```
Console> (enable) clear timezone
Timezone name and offset cleared.
Console> (enable)
```

Related Commands

set timezone

clear top

Use the **clear top** command to stop the TopN process.

clear top {**all** | *report_num*}

Syntax Description

all	Keyword to stop all nonpending TopN results.
report_num	TopN report number to kill; valid values are from **1** to **5**.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **clear top all** command will not kill any pending TopN reports. Only the reports with a *done* status are killed.

You can terminate TopN processes without the **background** option (use the **show top background** command to find out if the **background** option is used) by pressing **Ctrl-C** in the same Telnet/console session, or by entering the **clear top** [*report_num*] command from a separate Telnet/console session. The prompt is not printed before the TopN report is completely displayed. Other commands will be blocked until the report has been displayed.

Examples

This example shows how to stop the TopN 1 process from a console session:

```
Console> (enable) clear top 1
10/29/1998,12:05:38:MGMT-5: TopN report 1 killed by Console//.
Console> (enable)
```

This example shows how to stop the TopN 4 process from a Telnet session:

```
Console> (enable) clear top 4
10/29/1998,12:06:00:MGMT-5: TopN report 4 killed by telnet/172.22.34.2/.
Console> (enable)
```

Related Commands

show top
show top report

clear trunk

Use the **clear trunk** command to restore a trunk port to its default trunk type and mode or to clear specific VLANs from the allowed VLAN list for a trunk port.

clear trunk *mod/port* [*vlans*]

Syntax Description

mod/port	Number of the module and the port on the module.
vlans	(Optional) Number of the VLAN to remove from the allowed VLAN list; valid values are from **2** to **1005** and **1025** to **4094**.

Defaults

For all ports except MSM ports, the default is **auto** negotiate. For MSM ports, the default is **off** negotiate mode.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you specify VLANs, those VLANs are removed from the list of VLANs allowed on the trunk. Default VLANs cannot be cleared on the trunk.

Traffic for the removed VLANs are not forwarded over a trunk port. To add VLANs that you have removed, use the **set trunk** *mod/port vlans* command.

If you are trying to clear extended-range VLANs and sufficient space in NVRAM is not available, a warning message displays and the command fails.

Examples

This example shows how to clear VLANs 200 through 500 from the trunk port on port 2 of module 1:

```
Console> (enable) clear trunk 1/2 200-500
Removing Vlan(s) 200-500 from allowed list.
Port 1/2 allowed vlans modified to 1-199,501-1000.
Console> (enable)
```

This example shows the output if you attempt to clear a trunk when not enough NVRAM space is available:

```
Console> (enable) clear trunk 2/18 1030-1999
Failed to clear extended range vlans from allowed list.
Not enough NVRAM space. Use the 'set trunk' command to restore
       some existing entries to the default value.
Console> (enable)
```

Related Commands

set trunk
show trunk

clear vlan

Use the **clear vlan** command to delete an existing VLAN from a management domain.

clear vlan *vlans*

Syntax Description

vlans	Number of the VLAN; valid values are from **1** to **1000** and from **1025** to **4094**.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Follow these guidelines for deleting VLANs:

- When you delete a normal-range Ethernet VLAN in VTP server mode, the VLAN is removed from all switches in the same VTP domain.
- When you delete a normal-range VLAN in VTP transparent mode, the VLAN is deleted only on the current switch.
- You can delete an extended-range VLAN only on the switch where it was created.

Caution When you clear a VLAN, all ports assigned to that VLAN become inactive. However, the VLAN port assignments are retained until you move the ports to another VLAN. If the cleared VLAN is reactivated, all ports still configured on that VLAN are also reactivated. A warning is displayed if you clear a VLAN that exists in the mapping table.

When you clear a private VLAN (primary, isolated, or community), the ports are set to inactive and are not assigned to any VLAN. The private VLAN mappings for the selected VLAN are also cleared. ACL to VLAN mappings are also deleted.

Examples

This example shows how to clear existing VLAN 4000 from a management domain:

```
Console> (enable) clear vlan 4000
This command will de-activate all ports on vlan 4
in the entire management domain
Do you want to continue(y/n) [n]? y
VLAN 4 deleted
Console> (enable)
```

Related Commands

set vlan
show vlan

clear vlan counters

Use the **clear vlan counters** command to return the software-cached counters to 0 for all VLANs.

clear vlan counters

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Types Switch command.

Command Modes Privileged.

Examples This example shows how to clear all counters for all VLANs:

```
Console> (enable) clear vlan counters
vlan counters cleared
Console> (enable)
```

Related Commands **show vlan counters**

clear vlan mapping

Use the **clear vlan mapping** command to delete existing IEEE 802.1Q VLAN-to-ISL VLAN mappings or reserved-to-nonreserved VLAN mapping.

clear vlan mapping dot1q {*dot1q_vlan* | **all**}

clear vlan mapping reserved {*reserved_vlan* | **all**}

Syntax Description

dot1q *dot1q_vlan*	Keyword and variable to clear the IEEE 802.1Q VLAN-to-ISL VLAN mapping.
dot1q all	Keywords to clear all IEEE 802.1Q VLAN-to-ISL VLAN mappings.
reserved *reserved_vlan*	Keyword and variable to clear the specified reserved-to-nonreserved VLAN mapping.
reserved all	Keywords to clear all reserved-to-nonreserved VLAN mappings.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you clear a VLAN, all ports assigned to that VLAN become inactive. However, the VLAN port assignments are retained until you move the ports to another VLAN. If the cleared VLAN is reactivated, all ports still configured on that VLAN are also reactivated.

Examples

This example shows how to clear an existing mapped VLAN from the dot1q mapping table:

```
Console> (enable) clear vlan mapping dot1q 444
Vlan Mapping 444 Deleted.
Console> (enable)
```

This example shows how to clear all mapped VLANs from the mapping table:

```
Console> (enable) clear vlan mapping dot1q all
All Vlan Mapping Deleted.
Console> (enable)
```

This example shows how to clear mapped reserved VLANs from the mapping table:

```
Console> (enable) clear vlan mapping reserved 1007
Vlan Mapping 1007 Deleted.
Console> (enable)
```

Related Commands

set vlan
show vlan

clear vmps rcp

Use the **clear vmps rcp** command to delete the VMPS rcp username from the VMPS server table.

clear vmps rcp *username*

Syntax Description

username	Username up to 14 characters long.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not enter a username, all rcp usernames are deleted.

Examples

This example shows how to clear a specific VMPS rcp username from the VMPS table:

```
Console> (enable) clear vmps rcp jdoe
Console> (enable)
```

Related Commands

set rcp username

clear vmps server

Use the **clear vmps server** command to delete a VMPS server from the VMPS server table.

clear vmps server *ip_addr*

Syntax Description

ip_addr	IP address or host name of the VMPS server to be deleted.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear a VMPS server from the VMPS table:

```
Console> (enable) clear vmps server 192.168.255.255
VMPS domain server 192.168.255.255 cleared from VMPS table.
Console> (enable)
```

This example shows the results of trying to clear a nonexistent VMPS server from the VMPS table:

```
Console> (enable) clear vmps server 192.168.255.255
VMPS domain server 192.168.255.255 not in VMPS table.
Console> (enable)
```

Related Commands

reconfirm vmps
set vmps server

clear vmps statistics

Use the **clear vmps statistics** command to delete existing VMPS statistics.

clear vmps statistics

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to delete existing VMPS statistics:

```
Console> (enable) clear vmps statistics
VMPS and dynamic vlan statistics cleared.
Console> (enable)
```

Related Commands

show vmps statistics

clear vtp pruneeligible

Use the **clear vtp pruneeligible** command to specify which VLANs in the VTP domain are ineligible for pruning.

clear vtp pruneeligible *vlans...*

Syntax Description

vlans...	Number of VLANs to make pruning ineligible; valid values are from **1** to **1000**.

Defaults

The default is VLANs 2 through 1000 are eligible for pruning.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

VTP pruning causes information about each pruning-eligible VLAN to be removed from VTP updates if no stations belong to that VLAN out a particular switch port. Use the **set vtp** command to enable VTP pruning.

By default, VLANs 2 through 1000 are pruning eligible. Use the **clear vtp pruneeligible** command to make VLANs pruning ineligible.

If VLANs are pruning ineligible, use the **set vtp pruneeligible** command to make the VLANs pruning eligible again.

Examples

This example shows how to make VLANs 200 through 500 pruning ineligible:

```
Console> (enable) clear vtp pruneeligible 200-500
Vlans 1,200-500,1001-1005 will not be pruned on this device.
VTP domain Company modified.
Console> (enable)
```

Related Commands

set vtp
set vtp pruneeligible
show vtp domain

clear vtp statistics

Use the **clear vtp statistics** command to delete VTP statistics.

clear vtp statistics

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Types Switch command.

Command Modes Privileged.

Examples This example shows how to clear VTP statistics:

```
Console> (enable) clear vtp statistics
vtp statistics cleared.
Console> (enable)
```

Related Commands **set vtp**
show vtp statistics

commit

Use the **commit** command to commit all or a specific ACE in NVRAM that has not been written to hardware.

commit qos acl {*acl_name* | **all** | **adjacency**}

commit security acl {*acl_name* | **all** | **adjacency**}

Syntax Description

qos acl	Keywords to specify QoS ACEs.
acl_name	Name that identifies the VACL whose ACEs are to be committed.
all	Keyword to commit ACEs for all the ACLs.
adjacency	Keyword to commit adjacency table entries.
security acl	Keywords to specify security ACEs.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **commit** command commits *all* ACEs in NVRAM that have not been written to hardware. Any committed ACL with no ACEs are deleted. We recommend that you enter ACEs in batches and issue the **commit** command to save all of them in hardware and NVRAM.

Examples

This example shows how to commit a specific QoS ACE to NVRAM:

```
Console> (enable) commit qos acl my_acl
Hardware programming in progress...
ACL my_acl is committed to hardware.
Console> (enable)
```

This example shows how to commit a specific security ACE to NVRAM:

```
Console> (enable) commit security acl IPACL2
ACL commit in progress.
ACL IPACL2 is committed to hardware.
Console> (enable)
```

This example shows how to commit an adjacency table entry to NVRAM:

```
Console> (enable) commit security acl adjacency
Commit operation in progress.
Adjacency successfully committed.
```

Related Commands rollback

commit lda

Use the **commit lda** command to commit ASLB configuration that has not been written to hardware to NVRAM.

commit lda

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to commit ASLB configuration to NVRAM:

```
Console> (enable) commit lda
Commit operation in progress...
Successfully committed Local Director Accelerator.
Console> (enable)
```

Related Commands

clear lda
set lda
show lda

configure

Use the **configure** command to download a configuration file from an rcp server or the network and execute each command in that file.

configure {*host file*}[**rcp**]

configure network

Syntax Description

host	IP address or IP alias of the host.
file	Name of the file.
rcp	(Optional) Keyword to specify rcp as the file transfer method.
network	Keyword to specify interactive prompting for the host and the file.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Refer to the *Catalyst 6000 Family Software Configuration Guide* on how to construct a configuration file to download using the **configure** command.

Following is a sample file called system5.cfg in the /tftpboot directory:

```
begin
show time
set ip alias conc7 198.133.219.207
set ip alias montreux 198.133.119.42
set ip alias cres 192.122.174.42
set prompt system5>
set password
# empty string old password

pingpong
pingpong
end
#
```

Each line contains a command, except lines that begin with ! or #.

Examples

This example shows how to download the system5.cfg configuration file from the 192.122.174.42 host:

```
Console> (enable) configure 192.122.174.42 system5.cfg
Configure using system5.cfg from 192.122.174.42 (y/n) [n]? y
/
Done.  Finished Network Download.  (446 bytes)
>> show time
```

```
Wed May 19 1999, 17:42:50
>> set ip alias conc7 198.133.219.207
IP alias added.
>> set ip alias montreux 198.133.219.40
IP alias added.
>> set ip alias cres 192.122.174.42
IP alias added.
>> set prompt system5>
>> set password
Enter old password:
Enter new password: pingpong
Retype new password: pingpong
Password changed.
system5> (enable)
```

Related Commands

copy
show config

confreg

Use the **confreg** command to configure the configuration register utility.

confreg [*num*]

Syntax Description

num	(Optional) Valid values are **0** = ROM monitor, **1** = boot helper image, and **2** to **15** = boot system.

Defaults

This command has no default settings.

Command Types

ROM monitor command.

Command Modes

Normal.

Usage Guidelines

Executed with the **confreg** argument *num*, the VCR changes to match the number specified.

Without the argument, **confreg** dumps the contents of the VCR in English and allows you to alter the contents.

You are prompted to change or keep the information held in each bit of the VCR. In either case, the new VCR value is written into NVRAM and does not take effect until you reset or power cycle the platform.

You must issue a **sync** command to save your change. Otherwise, the change is not saved and a **reset** removes your change.

Examples

This example shows how to use the **confreg** command:

```
rommon 7 > confreg

Configuration Summary
enabled are:
console baud: 9600
boot: the ROM Monitor

do you wish to change the configuration? y/n  [n]:  y
enable  "diagnostic mode"? y/n  [n]: y
enable  "use net in IP bcast address"? y/n  [n]:
enable  "load rom after netboot fails"? y/n  [n]:
enable  "use all zero broadcast"? y/n  [n]:
enable  "break/abort has effect"? y/n  [n]:
enable  "ignore system config info"? y/n  [n]:
change console baud rate? y/n  [n]: y
enter rate: 0 = 9600, 1 = 4800, 2 = 1200, 3 = 2400  [0]:  0
change the boot characteristics? y/n  [n]: y
```

```
enter to boot:
 0 = ROM Monitor
 1 = the boot helper image
 2-15 = boot system
    [0]:  0


Configuration Summary
enabled are:
diagnostic mode
console baud: 9600
boot: the ROM Monitor

do you wish to change the configuration? y/n  [n]:


You must reset or power cycle for new config to take effect
```

Related Commands **show boot**

context

Use the **context** command to display the context of a loaded image.

context

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

ROM monitor command.

Command Modes

Normal.

Usage Guidelines

The context from the kernel mode and process mode of a booted image are displayed, if available.

Examples

This example shows how to display the context of a loaded image:

```
rommon 6 > context
Kernel Level Context:
 Reg       MSW        LSW     | Reg       MSW        LSW
------  ---------- ---------- | -----   ---------- ----------
zero   : 00000000   00000000  | s0     : 00000000   34008301
AT     : 00000000   3e800000  | s1     : 00000000   00000001
v0     : 00000000   00000003  | s2     : 00000000   00000003
v1     : 00000000   00000000  | s3     : 00000000   00000000
a0     : 00000000   0000002b  | s4     : 00000000   60276af8
a1     : 00000000   00000003  | s5     : ffffffff   ffffffff
a2     : 00000000   00000000  | s6     : 00000000   60276c58
a3     : 00000000   60276af8  | s7     : 00000000   0000000a
t0     : 00000000   00000b84  | t8     : 00000000   34008300
t1     : 00000000   3e800004  | t9     : ffffffff   ac000000
t2     : 00000000   00000239  | k0     : 00000000   00000400
t3     : 00000000   34008301  | k1     : 00000000   6024eb5c
t4     : ffffffff   ffff83fd  | gp     : 00000000   60252920
t5     : 00000000   0000003f  | sp     : 00000000   60276a98
t6     : 00000000   00000000  | s8     : 00000000   601fbf33
t7     : ffffffff   ffffffff  | ra     : 00000000   6006d380
HI     : 00000000   00000008  | LO     : 00000000   00000000
EPC    : 00000000   60033054  | ErrPC  : ffffffff   bfc070c8
Stat   : 34408302             | Cause  : 00002020
```

```
Process Level Context:
 Reg       MSW        LSW     | Reg       MSW        LSW
------  ---------- ---------- | -----   ---------- ----------
zero   : 00000000   00000000  | s0     : 00000000   00000074
AT     : 00000000   3e820000  | s1     : 00000000   60276c58
v0     : 00000000   00000081  | s2     : 00000000   601fbac0
v1     : 00000000   00000074  | s3     : 00000000   00000036
a0     : 00000000   00000400  | s4     : 00000000   0000000f
a1     : 00000000   60276c58  | s5     : ffffffff   ffffffff
a2     : 00000000   00000074  | s6     : 00000000   60276c58
a3     : 00000000   00000000  | s7     : 00000000   0000000a
t0     : 00000000   00000400  | t8     : 00000000   34008300
t1     : 00000000   00000400  | t9     : ffffffff   ac000000
t2     : 00000000   00000000  | k0     : 00000000   30408401
t3     : ffffffff   ffff00ff  | k1     : 00000000   30410000
t4     : 00000000   600dcc10  | gp     : 00000000   60252920
t5     : 00000000   0000003f  | sp     : ffffffff   80007ce8
t6     : 00000000   00000000  | s8     : 00000000   601fbf33
t7     : ffffffff   ffffffff  | ra     : 00000000   600dfd20
HI     : 00000000   00000008  | LO     : 00000000   00000000
EPC    : 00000000   600dfd38  | ErrPC  : ffffffff   ffffffff
Stat   : 34008303             | Cause  : ffffffff
```

copy

Use the **copy** command to upload or download a Flash image or a switch configuration to or from a Flash device, rcp server, or TFTP server.

copy *file-id* {**tftp** | **rcp** | **flash** | *file-id* | **config**}

copy tftp {**flash** | *file-id* | **config**}

copy rcp {**flash** | *file-id* | **config**}

copy flash {**tftp** | **rcp** | *file-id* | **config**}

copy config {**flash** | *file-id* | **tftp** | **rcp**} [**all**]

copy acl config {**flash** | *file-id* | **tftp** | **rcp**}

copy cfg1 {**tftp** | **rcp** | **flash** | **config** | **cfg2**} [**all**]

copy cfg2 {**tftp** | **rcp** | **flash** | **config** | **cfg1**} [**all**]

Syntax Description

file-id	Format used to specify the file on the Flash device, where the format is *m/device***:***filename.* *m/* = Option that gives access to different modules, such as the standby supervisor engine or an Ethernet module. *device***:** = Device where the Flash resides. *filename* = Name of the configuration file.
tftp	Keyword to allow you to copy to or from a TFTP server.
rcp	Keyword to specify the file be copied to or from an rcp server.
flash	Keyword to support downloading of multiple modules.
config	Keyword to allow you to copy the configuration to Flash memory, another Flash device, or a file on a TFTP server.
acl config	Keywords to copy the ACL configuration manually to a file. See the "Usage Guidelines" section before using this command.
cfg1	Keyword to specify the first startup configuration file on the supervisor engine.
cfg2	Keyword to specify the second startup configuration file on the supervisor engine.
all	(Optional) Keyword to specify that the entire configuration be copied to the specified destination configuration file.

Defaults

If a source or destination device is not given, the one specified by the **cd** command is used. If a destination filename is omitted, the source filename is used.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Use the **copy** command to perform these tasks:

- Download a system image or configuration file from a TFTP or rcp server to a Flash device.
- Upload a system image or configuration file from a Flash device to a TFTP or rcp server.
- Configure the switch using a configuration file on a Flash device or on a TFTP or rcp server.
- Copy the current configuration to a Flash device or to a TFTP or rcp server.
- Manually copy the ACL configuration to a file.

Caution Manual copying can only be used if **acl config** is set to **flash** and you enable the **auto-config append** option. If you disable the **append** option, the configuration clears before executing the auto-config file; see the **set boot config-register auto-config** command.

If you do not specify the source or destination device, the command uses the ones specified by the **cd** command. If you omit the destination filename, the source filename is used.

The **copy config**, **copy cfg1**, and **copy cfg2** commands copy only nondefault commands to the destination configuration file. Use the keyword **all** to copy both default and nondefault configurations.

If you do not specify a source or destination Flash device, the default Flash device (specified by the **cd** command) is used. Use the **pwd** command to display the current default Flash device. If you omit the destination filename, the system uses the source filename.

The system stores image and configuration files in the *sysname.cfg* file when you define a system name using the **set system name** command; otherwise, it uses the default *myswitch.cfg* file.

A colon (:) is required after the specified device.

If you use the **flash** keyword as the copy source or destination, you are prompted for the Flash device name.

If you are copying a software image to multiple intelligent switching modules of the same type, use the **flash** keyword as the copy destination. The switch automatically determines which modules to copy the image to based on the header in the source image file. If you want to copy a software image to a single intelligent switching module in a switch with multiple modules of the same type, you must specify the destination *file-id* as *m*/**bootflash:** (do not specify a filename).

Examples

This example shows how to use the **copy** command to upload the switch configuration to a file named cat.cfg on the slot0 Flash device:

```
Console> (enable) copy config slot0:cat.cfg
Upload configuration to slot0:cat.cfg
649324 bytes available on device slot0, proceed (y/n) [n]? y
.........
.........
.........
.........
.........
.
/
Configuration has been copied successfully. (10200 bytes)
Console> (enable)
```

This example shows how to use the **copy** command to upload the switch configuration to a file named lab2.cfg on the TFTP server:

```
Console> (enable) copy config tftp:lab2.cfg
IP address or name of remote host [172.20.22.7]? y
Upload configuration to tftp:lab2.cfg (y/n) [n]? y
.........
.........
.........
.
/
Configuration has been copied successfully. (10299 bytes).
Console> (enable)
```

This example shows how to use the **copy** command to upload the switch configuration to the cat.cfg file on the slot0 Flash device:

```
Console> (enable) copy config flash
Flash device [bootflash]? slot0:
Name of file to copy to [test_image]? cat.cfg
Upload configuration to slot0:cat.cfg
749124 bytes available on device slot0, proceed (y/n) [n]? y
.........
.........
.........
.........
.
/
Configuration has been copied successfully. (200345 bytes).
Console> (enable)
```

These examples show how to use the **copy** command to download a configuration from a TFTP server:

```
Console> (enable) copy slot0:cat.cfg config
Configure using slot0:cat.cfg (y/n) [n]? y
/
Finished download. (10900 bytes)
>> set password $1$FMFQ$HfZR5DUszVHIRhrz4h6V70
Password changed.
>> set enablepass $1$FMFQ$HfZR5DUszVHIRhrz4h6V70
Password changed.
>> set prompt Console>
>> set length 24 default
Screen length set to 24.
>> set logout 20
..........
Console> (enable)
```

```
Console> (enable) copy tftp config
IP address or name of remote host? 172.20.22.7
Name of configuration file? cat.cfg
Configure using cat.cfg from 172.20.22.7 (y/n) [n]? y
/
Finished network download. (10900 bytes)
>> set password $1$FMFQ$HfZR5DUszVHIRhrz4h6V70
Password changed.
>> set enablepass $1$FMFQ$HfZR5DUszVHIRhrz4h6V70
Password changed.
>> set prompt Console>
>> set length 24 default
Screen length set to 24.
>> set logout 20
...........
Console> (enable)
Console> (enable) copy flash config
Flash device [bootflash]?
Name of configuration file? test.cfg
Configure using bootflash:test.cfg (y/n) [n]? y
/
Finished download. (10900 bytes)
>> set password $1$FMFQ$HfZR5DUszVHIRhrz4h6V70
Password changed.
>> set enablepass $1$FMFQ$HfZR5DUszVHIRhrz4h6V70
Password changed.
>> set prompt Console>
>> set length 24 default
Screen length set to 24.
>> set logout 20
.....
Console> (enable)
```

This example shows how to copy the running configuration to an rcp server for storage:

```
Console> (enable) copy config rcp
IP address or name of remote host []? 172.20.52.3
Name of file to copy to []? cat6000_config.cfg

Upload configuration to rcp:cat6000_config.cfg, (y/n) [n]? y
.....
..........
.......

..........
...........
..
/
Configuration has been copied successfully.
Console> (enable)
```

This example shows how to configure a Catalyst 6000 family switch using a configuration file downloaded from an rcp server:

```
Console> (enable) copy rcp config
IP address or name of remote host []? 172.20.52.3
Name of file to copy from []? dns-config.cfg

Configure using rcp:dns-config.cfg (y/n) [n]? y
/
Finished network download.  (134 bytes)
>>
>> set ip dns server 172.16.10.70 primary
172.16.10.70 added to DNS server table as primary server.
>> set ip dns server 172.16.10.140
172.16.10.140 added to DNS server table as backup server.
>> set ip dns enable
DNS is enabled
>> set ip dns domain corp.com
Default DNS domain name set to corp.com
Console> (enable)
```

This example shows how to upload an image from a remote host into Flash using an rcp server:

```
Console> (enable) copy rcp flash
IP address or name of remote host []? 172.20.52.3
Name of file to copy from []? cat6000-sup-d.6-1-1.bin
Flash device [bootflash]?
Name of file to copy to [cat6000-sup-d.6-1-1.bin]?

4369664 bytes available on device bootflash, proceed (y/n) [n]? y
CCCC
```

Related Commands

- configure
- set boot config-register
- set boot config-register auto-config
- write

delete

Use the **delete** command to delete a configuration file.

delete [[*m/*]*device***:**]*filename*

Syntax Description

m/	(Optional) Module number of the supervisor engine containing the Flash device.
*device***:**	(Optional) Device where the Flash resides.
filename	Name of the configuration file.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

A colon (:) is required after the specified device.

Examples

This example shows how to delete the cat6000-sup-d.5-5-1.bin configuration file from the Flash device and then verify the deletion by entering the **show flash** command:

```
Console> (enable) delete bootflash:cat6000-sup-d.5-5-1.bin
Console> (enable)
Console> (enable) show flash
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
  1 .D ffffffff 5415406e  3300b8   25  3080247 Jan 12 2000 13:22:46
cat6000-sup-d.6-1-1.bin
  2 .. ffffffff 762950d6  6234d0   25  3093399 Jan 13 2000 12:33:14
cat6000-sup-d.6-1-1.bin

1428272 bytes available (6173904 bytes used)
Console> (enable)
```

Related Commands

dir—switch
show flash
squeeze
undelete

dev

Use the **dev** command to list the device IDs available on a switch.

dev

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

ROM monitor command.

Command Modes

Normal.

Examples

This example shows how to use the **dev** command:

```
rommon 10 > dev
Devices in device table:
        id  name
 bootflash: bootflash
    slot0:  PCMCIA slot 0
    eprom:  eprom
```

dir—ROM monitor

Use the **dir** command to list the files of the named device.

dir *device*

Syntax Description

device	ID of the device.

Defaults

This command has no default settings.

Command Types

ROM monitor command.

Command Modes

Normal.

Examples

This example shows how to use the **dir** command:

```
rommon 11 > dir flash:
         File size           Checksum   File name
        65 bytes (0x41)       0xb49d    clev/oddfile65
   2229799 bytes (0x220627)   0x469e    clev/sierra-k.Z
```

dir—switch

Use the **dir** command to display a list of files on a Flash memory device.

dir [[*m/*]*device***:**][*filename*] [**all** | **deleted** | **long**]

Syntax Description

m/	(Optional) Module number of the supervisor engine containing the Flash device.
*device***:**	(Optional) Device where the Flash resides.
filename	(Optional) Name of the configuration file.
all	(Optional) Keyword to display all files, deleted or not.
deleted	(Optional) Keyword to display only deleted files.
long	(Optional) Keyword to display files that have not been deleted, in long format.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal and privileged.

Usage Guidelines

A colon (:) is required after the specified device.

When you specify the **all** keyword, the file information is displayed in long format.

When you omit all keywords (**all**, **deleted**, or **long**), the system displays file information in short format. Short format is shown in Table 2-10.

Table 2-10 Short Format

Column Heading	Description
#	File index number
length	File length
date/time	Date and time the file was created
name	Filename

When you use one of the keywords (**all**, **deleted**, or **long**), the system displays file information in long format. The long format is shown in Table 2-11.

Table 2-11 Long Format

Column Heading	Description
#	File index number
ED	Letter to indicate whether the file contains an error (E) or is deleted (D)
type	File type (1 = configuration file, 2 = image file); when the file type is unknown, the system displays a zero or FFFFFFFF in this field
crc	File cyclic redundancy check
seek	Offset into the file system of the next file
nlen	Filename length
length	File length
date/time	Date and time the file was created
name	Filename

Examples

This example shows how to display the file information in short format:

```
Console> (enable) dir
-#- -length- -----date/time------ name
  1  6061822 Mar 03 2000 15:42:49 cat6000-sup.6-1-1.bin
  2  6165044 Mar 13 2000 14:40:15 cat6000-sup.5-5-1.bin

3763660 bytes available (12227124 bytes used)
Console> (enable)
```

This example shows how to display the file information in long format:

```
Console> (enable) dir long
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
  1 .. ffffffff f3a3e7c1  607f80   24  6061822 Mar 03 2000 15:42:49 cat6000-sup.
6-1-1.bin
  2 .. ffffffff aa825ac6  be9234   24  6165044 Mar 13 2000 14:40:15 cat6000-sup.
5-5-1.bin

3763660 bytes available (12227124 bytes used)
Console> (enable)
```

Related Commands

show flash

disable

Use the **disable** command to return to normal mode from privileged mode.

disable

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to return to normal mode:

```
Console> (enable) disable
Console>
```

Related Commands

enable

disconnect

Use the **disconnect** command to close an active console port or Telnet session.

disconnect {*ip_addr* | **console**}

Syntax Description

ip_addr	IP address or IP alias.
console	Keyword to denote an active console port.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If multiple sessions from the same IP address exist, the **disconnect** command checks if the current process is also from the same IP address. If it is not, all Telnet sessions from the specified IP address are disconnected. If it is, all sessions, other than the current session, are disconnected. The system prompts whether to disconnect the current Telnet session. You can answer **n** and remain connected or answer **y** and be disconnected.

Examples

This example shows how to close a Telnet session to host 198.134.214.4:

```
Console> (enable) disconnect 198.134.214.4
Telnet session from 198.134.214.4 disconnected. (1)
Console> (enable)
```

This example shows how to close the current console session:

```
Console> (enable) disconnect console
Console session disconnected.
Console> (enable)
```

Related Commands

telnet

download

Use the **download** command to copy a software image from a specified host to the Flash memory of a designated module.

download *host file* [*mod*] [**rcp**]

download serial

download vmps

download boot *flash_device:filename mod_num*

Syntax Description

host	Name or IP address of host.
file	Name of file to be downloaded.
mod	(Optional) Number of the module to receive the downloaded image.
rcp	(Optional) Keyword to specify rcp as the file transfer method.
serial	Keyword to specify download through a serial port.
vmps	Keyword to download VMPS.
boot	Keyword to download an image to the boot ROM of a module.
flash_device:filename	Name of the software image to be downloaded.
mod_num	Number of the module to receive the downloaded image.

Defaults

If a module number is not specified, the image is downloaded to all modules for which the image is valid.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Catalyst 6000 family switches download new code to the processors using Kermit serial download through the EIA/TIA-232 console port.

The **download** command downloads code to the module Flash memory. Catalyst 6000 family switch software rejects an image if it is not a valid image for the module.

The **download serial** command uses Kermit through the serial EIA/TIA-232 console port. The **download serial** command is not allowed from a Telnet session.

Before you can execute the **download vmps** command successfully, you must use the **set vmps downloadserver** command to configure the IP address of the TFTP server and the name of the VMPS configuration file on that server. If the IP address of the TFTP server is not configured, the **download vmps** command reports an error. If the configuration filename is not configured, the **download vmps** command uses the default filename vmps-config-database.1.

After a successful download, the new VMPS information replaces any existing information. If there are not enough resources to build the new configuration database, the VMPS is made inactive.

If you specify the module number, the download goes to the specified module, but the download will fail if the module is of a different type than is indicated by the download header. If you do not specify the module number, the download goes to all modules of that type.

Caution After starting the serial download using Kermit, do not attempt to abort the serial download by pressing **Ctrl-C**. Pressing **Ctrl-C** interrupts the download process and could leave the switch in a problematic state. If this occurs, reboot the switch.

Examples

This example shows how to download the c6000_spv11.bin file from the mercury host to the supervisor engine (by default):

```
Console> (enable) download mercury c6000_spv11.bin
Download image c6000_spv11.bin from mercury to module 1FLASH (y/n) [n]? y
\
Finished network single module download. (2418396 bytes)
FLASH on Catalyst:

Type            Address             Location
Intel 28F008    20000000            NMP (P3) 4MB SIM

Erasing flash sector...done.
Programming flash sector...done.
Erasing flash sector...done.
Programming flash sector...done.
The system needs to be reset to run the new image.
Console> (enable)
```

This example shows how to download the acpflash_1111.bbi file from the mercury host to module 3:

```
Console> (enable) download mercury acpflash_1111.bbi 3
This command will reset Module 3.
Download image acpflash_1111.bbi from mercury to Module 3 FLASH (y/n) [n]? y
/
Done.  Finished network download.  (1964012 bytes)
Console> (enable)
```

This sample session shows how to connect to a remote terminal from a Sun workstation and how to use the **download serial** command to copy a software image to the supervisor engine:

```
[At local Sun workstation]
host% kermit
C-Kermit 5A(172) ALPHA, 30 Jun 95, SUNOS 4.0 (BSD)
Type ? or 'help' for help
C-Kermit> set line /dev/ttyb
C-Kermit> c
Connecting to /dev/ttyb, speed 9600.
The escape character is ^ (ASCII 28).
Type the escape character followed by C to get back,
or followed by ? to see other options.
```

```
Console> enable
Enter Password:
Console> (enable) set system baud 19200
^\C
[Back at local Sun workstation]
C-Kermit> set speed 19200
/dev/ttyb, 19200 bps
C-Kermit> c
Connecting to /dev/ttyb, speed 19200.
The escape character is ^ (ASCII 28).
Type the escape character followed by C to get back,
or followed by ? to see other options.

Console> (enable) download serial
Download Supervisor image via console port (y/n) [n]? y

Concentrator Boot ROM (Ver 1.00)

Waiting for DOWNLOAD!!
Return to your local Machine by typing its escape sequence
Issue Kermit send command from there[ Send 'Filename']

^\C
[Back at Local System]
C-Kermit> send c6000_xx.bin
                          SF
c6000_xx.bin => C6000_XX.BIN, Size: 1233266

X to cancel file,  CR to resend current packet
Z to cancel group, A for status report
E to send Error packet, Ctrl-C to quit immediately: ......................
.........................................................................

...... [OK]
ZB
C-Kermit> quit
host%
```

This example shows the **download vmps** command and typical system responses:

```
Console> (enable) download vmps
Re-initialization of Vlan Membership Policy Server with the downloaded
configuration file is in progress.
6/14/1998,17:37:29:VMPS-2:PARSER: 82 lines parsed, Errors 0
```

This example shows how to download a ROM image to module 9:

```
Console> (enable) download boot bootflash:boot542.ubin 9
Warning!! This command replaces the existing boot code on Module 9.
Please verify with TAC that the file specified is appropriate for WS-X6408-GBIC.
Use this command with caution.
Do you want to continue (y/n) [n]? y
Download boot image start...
Download boot code completed.
Console> (enable)
```

Related Commands

- reset—switch
- show flash
- show rcp
- show vmps

enable

Use the **enable** command to activate privileged mode. In privileged mode, additional commands are available, and certain commands display additional information.

enable

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The (enable) in the prompt indicates that the system is in privileged mode and that commands can be entered.

Examples

This example shows how to enter privileged mode:

```
Console> enable
Enter password:
Console> (enable)
```

Related Commands

disable

format

Use the **format** command to format bootflash or a Flash PC card (a Flash device must be formatted before it can be used).

format [**spare** *spare-num*] [*m/*]*device1***:** [[*device2***:**][*monlib-filename*]]

Syntax Description

spare *spare_num*	(Optional) Number of spare sectors to reserve when other sectors fail.
m/	(Optional) Module number of the supervisor engine containing the Flash device.
*device1***:**	Flash device to be formatted.
*device2***:**	(Optional) Flash device that contains the *monlib* file to be used to format *device1***:**.
monlib-filename	(Optional) Name of the monlib file.

Defaults

The default number of spare sectors is 0.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

A colon (:) is required after the specified device.

You can reserve up to 16 spare sectors for use when other sectors fail. If you do not reserve a spare sector and later some sectors fail, you will have to reformat the entire Flash memory, which will erase all existing data.

The monlib file is the ROM monitor library used by the ROM monitor to access files in the Flash file system. It is also compiled into the system image. In the command syntax, *device1***:** is the device to format and *device2***:** contains the *monlib* file to use.

When you omit the [[*device2***:**][*monlib-filename*]] argument, the system formats *device1***:** using the *monlib* that is bundled with the system software.

When you omit *device2***:** from the [[*device2***:**][*monlib-filename*]] argument, the system formats *device1***:** using the named *monlib* file from the device specified by the **cd** command.

When you omit *monlib-filename* from the [[*device2***:**][*monlib-filename*]] argument, the system formats *device1***:** using the *monlib* file from *device2***:**. When you specify the whole [[*device2***:**][*monlib-filename*]] argument, the system formats *device1***:** using the specified *monlib* file from the specified device.

You can also specify *device1*:*monlib-filename* as the device and filename to be used, as follows:

format device1: [*device1*:] [*monlib-filename*]]

If *monlib-filename* is omitted, the system formats *device1*: using the built-in monlib file on the device.

Note When the system cannot find a monlib file, the system terminates the formatting process.

Note If the Flash device has a volume ID, you must provide the volume ID to format the device. The volume ID is displayed using the **show flash** *m/device:* **filesys** command.

Examples

This example shows how to format a Flash PC card:

```
Console> (enable) format slot0:
All sectors will be erased, proceed (y/n) [n]?y
Enter volume id (up to 31 characters):
Formatting sector 1
Format device slot0 completed.
Console> (enable)
```

frame

Use the **frame** command to display an individual stack frame.

frame [**-d** | **-p**] [*num*]

Syntax Description

-d	(Optional) Keyword to specify a monitor context.
-p	(Optional) Keyword to specify a booted image process level context.
num	(Optional) Number of the frame to display, where **0** = youngest frame.

Defaults

The default is a booted image kernel context—the youngest frame.

Command Types

ROM monitor command.

Command Types

Normal.

Usage Guidelines

The minus sign (-) is required with the **-d** and **-p** options.

Examples

This example shows how to use the **frame** command to specify a booted image process level context, frame 1:

```
rommon 6 > frame -p 1
Stack Frame 1, SP = 0x80007ed8, Size = 32 bytes
[0x80007ed8 : sp + 0x000] = 0x6031de50
[0x80007edc : sp + 0x004] = 0x6031c000
[0x80007ee0 : sp + 0x008] = 0x00000000
[0x80007ee4 : sp + 0x00c] = 0x80007ec4
[0x80007ee8 : sp + 0x010] = 0x00000002
[0x80007eec : sp + 0x014] = 0x00000000
[0x80007ef0 : sp + 0x018] = 0x60008770
[0x80007ef4 : sp + 0x01c] = 0x600087f0
```

history—ROM monitor

Use the **history** command to display the command history (the last 16 commands executed in the ROM monitor environment). This command is aliased to “h” by the ROM monitor for convenience.

history

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

ROM monitor command.

Command Modes

Normal.

Examples

This example shows how to use the **history** command:

```
rommon 13 > history

1   help
2   break -s 0x20090
3   break -s 10090
4   break -s 0xa0001000
5   cont
6   help
7   dev
8   dir
9   dir bootflash:
10  dis
11  dis 0xa0001000
12  dis 0xbe000000
13  history
==========================================================================
```

history—switch

Use the **history** command to show the contents of the command history buffer.

history

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The history buffer size is fixed at 20 commands. See the "Command-Line Interfaces" chapter for detailed information about the command history feature.

Examples

In this example, the **history** command lists the contents of the command history buffer:

```
Console> history
       1 help
       2 history
Console> !2
history
       1 help
       2 history
       3 history
Console>
```

l2trace

Use the **l2trace** command to display the Layer 2 path taken by the packets that start at a specified source address and end at a specified destination address.

l2trace *src_mac_addr dest_mac_addr* [*vlan*] [**detail**]

l2trace *src_ip_addr dest_ip_addr* [**detail**]

Syntax Description

src_mac_addr	Source MAC address.
dest_mac_addr	Destination MAC address.
vlan	(Optional) Number of the VLAN.
src_ip_addr	Source IP address or alias.
dest_ip_addr	Destination IP address or alias.
detail	(Optional) Keyword to specify detailed information.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Types

Privileged.

Usage Guidelines

All the intermediate devices should be Catalyst 5000 or Catalyst 6000 family switches running supervisor engine software release 6.1 or later. Catalyst 4000 family switches must be running supervisor engine software release 6.2 or later.

The **l2trace** command displays 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, **l2trace** aborts with an error message.

You must enable CDP on all the Catalyst 4000, Catalyst 5000, or Catalyst 6000 family switches in the network.

When the switch detects a device (in the Layer 2 path) that does not belong to the Catalyst 4000, Catalyst 5000, or Catalyst 6000 family switch, the switch continues to send Layer 2 trace queries and lets them time out.

This command is rejected if you enter a multicast source or destination MAC address.

If a source or the destination address belongs to multiple VLANs, you must specify the VLAN to be used for determining the Layer 2 path.

The Layer 2 trace feature is not supported when multiple devices are attached to one port via hubs (for example, multiple CDP neighbors detected on a port). When more than one CDP neighbor is detected on the port, l2trace is aborted.

If you specify the IP address of the source and destination systems instead of the MAC addresses, the switch looks at the ARP table to determine the IP address to MAC address mapping of the source and destination systems. If an ARP entry exists for the specified IP address, the corresponding MAC address is used. If no matching ARP entry exists, the system does an ARP query and tries to resolve the IP address. If this is the case, a restriction is imposed that requires the source and destination systems to be in the same subnet as the switch in order for the ARP query to be resolved.

Examples

This example shows how to display the Layer 2 packet path for a specified source and destination MAC address:

```
Console> (enable) l2trace 00-01-22-33-44-55 10-22-33-44-55-66 detail
l2trace vlan number is 10.

00-01-22-33-44-55 found in C5500 named wiring-1 on port 4/1 10Mb half duplex
C5500: wiring-1: 192.168.242.10: 4/1 10Mb half duplex -> 5/2 100MB full duplex
C5000: backup-wiring-1: 192.168.242.20: 1/1 100Mb full duplex -> 3/1-4 FEC attached
C5000: backup-core-1: 192.168.242.30: 4/1-4 FEC attached -> 1/1-2 GEC attached
C6000: core-1: 192.168.242.40: 1/1-2 GEC attached -> 2/1 10MB half duplex.
10-22-33-44-55-66 found in C6000 named core-1 on port 2/1 10MB half duplex.
Console> (enable)
```

This example shows how to display the Layer 2 packet path for a specified source and destination IP alias:

```
Console> (enable) l2trace user-1-pc user-2-pc detail
Mapping IP address to MAC Address
user-1-pc -> 00-01-22-33-44-55
user-2-pc -> 10-22-33-44-55-66
l2trace vlan number is 10

00-01-22-33-44-55 found in C5500 named wiring-1 on port 4/1 10Mb half duplex
C5500: wiring-1: 192.168.242.10: 4/1 10Mb half duplex -> 5/2 100MB full duplex
C5000: backup-wiring-1: 192.168.242.20: 1/1 100Mb full duplex -> 3/1-4 FEC attached
C5000: backup-core-1: 192.168.242.30: 4/1-4 FEC attached -> 1/1-2 GEC attached
C6000: core-1: 192.168.242.40: 1/1-2 GEC attached -> 2/1 10MB half duplex.
10-22-33-44-55-66 found in C6000 named core-1 on port 2/1 10MB half duplex.
Console> (enable)
```

This example shows how to display a summary of Layer 2 packet path information for a specified source and destination IP address:

```
Console> (enable) l2trace 9.7.0.7 9.7.0.6
Starting L2 Trace
sc0 :9.7.0.7 : 3/7
4/16 :9.7.0.2 : 4/10
Console> (enable)
```

This example shows how to display a summary of Layer 2 packet path information for a specified source and destination MAC address:

```
Console> (enable) l2trace 00-01-22-33-44-55 10-22-33-44-55-66
Starting L2 Trace
sc0 :9.7.0.7 : 3/7
4/16 :9.7.0.2 : 4/10
Console> (enable)
```

meminfo

Use the **meminfo** command to display information about the main memory, packet memory, and NVRAM. With the **-l** option, the supported DRAM configurations are displayed.

meminfo [**-l**]

Syntax Description

-l	(Optional) Keyword to specify the long listing, which displays the DRAM configurations.

Defaults

This command has no default settings.

Command Types

ROM monitor command.

Command Modes

Normal.

Usage Guidelines

The minus sign (-) is required with the **-l** option.

Examples

This example shows how to use the **meminfo** command:

```
rommon 9 > meminfo

Main memory size: 16 MB in 32 bit mode.
Available main memory starts at 0xa000e000, size 16328KB
IO (packet) memory size: 25 percent of main memory.
NVRAM size: 32KB
```

ping

Use the **ping** command to send ICMP echo-request packets to another node on the network. You can also use the **ping** command without arguments to configure ping.

ping -s *host*

ping -s *host* [*packet_size*] [*packet_count*]

ping

Syntax Description

-s	Keyword to cause **ping** to send one datagram per second, printing one line of output for every response received.
host	IP address or IP alias of the host.
packet_size	(Optional) Number of bytes in a packet, from **56** to **1472** bytes.
packet_count	(Optional) Number of packets to send; valid values are from **0** to **2,147,483,647**.

Defaults

The defaults for **ping -s** are as follows:

- *packet_size* is 56 bytes
- *packet_count* is 2,147,483,647

The defaults for **ping** with no arguments are as follows:

- *packet_size* is 56 bytes
- *packet_count* is 5
- Wait time is 2 seconds
- Target IP address is none (this is a mandatory field)
- Source address is the host IP address

Command Types

Switch command.

Command Modes

Normal or privileged.

Usage Guidelines

General **ping** command guidelines are as follows:

- Press **Ctrl-C** to stop pinging.
- Continuous ping means that, unless you press **Ctrl-C** to stop pinging, packets are generated continually and dispatched to the host.
- The actual packet size is 8 bytes larger than the size you specify because the switch adds header information.
- Normal response—The normal response occurs in 1 to 10 seconds, depending on network traffic.

The guidelines for the **ping -s** command are as follows:

- The maximum waiting time before timing out is 2 seconds.
- A new ping packet is generated after 1 second of sending the previous packet, regardless of whether an echo-reply is received or not.
- If you do not enter a packet count, continuous ping results.
- Network or host unreachable—The switch found no corresponding entry in the route table.
- Destination does not respond—If the host does not respond, a "no answer from host" appears in 2 seconds.
- Destination unreachable—The gateway for this destination indicates that the destination is unreachable.

The guidelines for the **ping** command without arguments are as follows:

- The **ping** *host* command is accepted in normal mode only. The parameters take the default values automatically.
- The target IP address is a mandatory field to be entered.
- The maximum waiting time is configurable.
- A new ping packet is generated only when an echo-reply is received.
- If you enter a packet count of 0, this results in continuous ping.
- Returns output only when a response is received or you press **Return**.
- Available in privileged mode only.
- When configuring ping, you must either press **Return** or enter a response. Valid responses and appropriate values are as follows:
  - Target IP address: IP address or host name of the destination node you plan to ping.
  - Number of Packets: Number of ping packets to be sent to the destination address; valid values are from 0 to 2,147,483,647 (0 specifies continuous ping).
  - Datagram size: Size of the ping packet; valid values are from 56 to 1472 bytes.
  - Timeout in seconds: Timeout interval; valid values are from 0 to 3600 seconds.
  - Source IP Address [(default)]: IP address or IP alias of the source.

Examples

This example shows how to ping a host with IP alias elvis a single time:

```
Console> ping elvis
!!!!!

-----172.20.52.19 PING Statistics------
5 packets transmitted, 5 packets received, 0% packet loss
round-trip (ms) min/avg/max = 1/1/1
Console>
```

This example shows how to ping a host with IP alias elvis once per second until you press **Ctrl-C** to stop pinging:

```
Console> ping -s elvis
ping elvis: 56 data bytes
64 bytes from elvis: icmp_seq=0. time=11 ms
64 bytes from elvis: icmp_seq=1. time=8 ms
64 bytes from elvis: icmp_seq=2. time=8 ms
64 bytes from elvis: icmp_seq=3. time=7 ms
```

```
64 bytes from elvis: icmp_seq=4. time=11 ms
64 bytes from elvis: icmp_seq=5. time=7 ms
64 bytes from elvis: icmp_seq=6. time=7 ms
^C

----elvis PING Statistics----
7 packets transmitted, 7 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 7/8/11
Console>
```

This example shows how to configure ping:

```
Console> (enable) ping

Target IP Address []: 172.20.52.19
Number of Packets [5]: 6
Datagram Size [56]: 75
Timeout in seconds [2]: 1
Source IP Address [172.20.52.18]:
!!!!!!

----172.20.52.19 PING Statistics----
6 packets transmitted, 6 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 1/1/1
Console> (enable)
```

Related Commands

set interface
set ip route
show interface
show ip route

pwd

Use the **pwd** command to show the current setting of the **cd** command.

pwd [[*m/*]*device***:**]

Syntax Description

m/	(Optional) Module number of the supervisor engine containing the Flash device.
*device***:**	(Optional) Device where the Flash resides.

Defaults

If no module number or device is specified, **pwd** defaults to the first module of the active device.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

A colon (:) is required after the specified device.

Examples

This example shows how to use the **pwd** command to display the current listing of the **cd** command:

```
Console> cd slot0:
Default flash device set to slot0.
Console> pwd
slot0
```

Related Commands

cd

quit

Use the **quit** command to exit a CLI session.

quit

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The **exit** and **logout** commands perform the same function as the **quit** command.

Examples

This example shows how to quit a CLI session:

```
Console> quit
Connection closed by foreign host.
host%
```

reconfirm vmps

Use the **reconfirm vmps** command to reconfirm the current dynamic port VLAN membership assignments with the VMPS server.

reconfirm vmps

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

VMPS database changes are not conveyed automatically to switches participating in VMPS. Therefore, after making a VMPS database change, use this command on VMPS clients and servers to apply the database changes.

Examples

This example shows how to reconfirm the current dynamic port VLAN membership with VMPS:

```
Console> (enable) reconfirm vmps
reconfirm process started
Use 'show dvlan statistics' to see reconfirm status
Console> (enable)
```

Related Commands

show dvlan statistics

reload

Use the **reload** command to force a module to accept a download via SCP. This command resets the module and prompts you to initiate a download when the reset is complete.

reload *module*

Syntax Description

module	Number of the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is used if a module is accidently reset during the downloading of an image. After the reset, a normal download will not work. You must enter the **reload** *module* command followed by the **download** *host file* [*mod*] command.

Examples

This example shows how to reset module 3 and download the acpflash_1111.bbi file from the mercury host to the module:

```
Console> (enable) reload 3
Console> (enable) download mercury acpflash_1111.bbi 3
This command will reset Module 3.
Download image acpflash_1111.bbi from mercury to Module 3 FLASH (y/n) [n]? y
/
Done.  Finished network download.  (1964012 bytes)
Console> (enable)
```

Related Commands

download

repeat

Use the **repeat** command to repeat a command.

repeat [*num* | *string*]

Syntax Description

number	(Optional) Number of the command.
string	(Optional) Command string.

Defaults

If no argument is specified, the last command is repeated.

Command Types

ROM monitor command.

Command Modes

Normal.

Usage Guidelines

The optional command number (from the history buffer list) or match string specifies which command to repeat.

In the match string, the most recent command to begin with the specified string is executed again.

If the string contains white space, you must use quotation marks.

This command is usually aliased to the letter “r.”

Examples

These examples show how to use the **repeat** command. You use the **history** command to display the list of previously entered commands:

```
rommon 22 > history

8   dir
9   dir bootflash:
10   dis
11   dis 0xa0001000
12   dis 0xbe000000
13   history
14   meminfo
15   meminfo -l
16   meminfo
17   meminfo -l
18   meninfo
19   meminfo
20   meminfo -l
21   meminfo -l
22   history
```

```
rommon 23 > repeat dir
dir bootflash:
         File size           Checksum   File name
   1973032 bytes (0x1e1b28)   0xdadf5e24    llue
rommon 24 > repeat
dir bootflash:
         File size           Checksum   File name
   1973032 bytes (0x1e1b28)   0xdadf5e24    llue
rommon 25 > repeat 15
meminfo -l

Main memory size: 16 MB.
Packet memory size: 0 MB
Main memory size: 0x1000000
Available main memory starts at 0xa000e000, size 0xff2000
NVRAM size: 0x20000

Parity Map for the DRAM Banks
Socket 0 in Bank 0 Has No Parity
Socket 1 in Bank 0 Has No Parity
Socket 0 in Bank 1 Has No Parity
Socket 1 in Bank 1 Has No Parity
===========================================================================
```

reset—ROM monitor

Use the **reset** ROM monitor command to perform a soft reset of the switch.

reset [-**s**]

Syntax Description

-s	(Optional) Keyword to reset the entire switch.

Defaults

The default Flash device is slot0.

Command Types

ROM monitor command.

Command Modes

Normal.

Usage Guidelines

This command will not boot the MSFC if the PFC is not present in the Catalyst 6000 family switch.

Examples

This example shows how to use the **reset** command:

```
rommon 26 > reset

System Bootstrap, Version 3.1(1.69)
Copyright (c) 1994-1997 by cisco Systems, Inc.
Supervisor processor with 16384 Kbytes of main memory

rommon 1 >
================================================================================
```

reset—switch

Use the **reset** command to restart the system or an individual module, schedule a system reset, or cancel a scheduled reset.

reset [*mod* | **system** | **mindown**]

reset [**mindown**] **at** {*hh:mm*} [*mm/dd*] [*reason*]

reset [**mindown**] **in** [*hh*:] {*mm*} [*reason*]

reset [**cancel**]

reset {*mod*} [*bootdevice*[,*bootdevice*]]

Syntax Description

mod	(Optional) Number of the module to be restarted.
system	(Optional) Keyword to reset the system.
mindown	(Optional) Keyword to perform a reset as part of a minimal downtime software upgrade in a system with a redundant supervisor engine.
at	Keyword to schedule a system reset at a specific future time.
hh:mm	Hour and minute of the scheduled reset.
mm/dd	(Optional) Month and day of the scheduled reset.
reason	(Optional) Reason for the reset.
in	Keyword to schedule a system reset in a specific time.
hh	(Optional) Number of hours into the future to reset the switch.
mm	Number of minutes into the future to reset the switch.
cancel	(Optional) Keyword to cancel the scheduled reset.
mod	Number of the NAM or IDS.
bootdevice	(Optional) Boot device identification; for format guidelines, see the "Usage Guidelines" section.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not specify a module number (either a switching module or the active supervisor engine module), the command resets the entire system.

You can use the **reset** *mod* command to switch to the standby supervisor engine, where *mod* is the module number of the active supervisor engine.

You can use the **reset mindown** command to reset the switch as part of a minimal downtime software upgrade in a system with a redundant supervisor engine. For complete information on performing a minimal downtime software upgrade, refer to the *Catalyst 6000 Family Software Configuration Guide* for your switch.

Caution If you make configuration changes after entering the **reset mindown** command but before the active supervisor engine resets, the changes are not saved. Input from the CLI is still accepted by the switch while the redundant supervisor engine is reset. Any changes you make to the configuration between the time when you enter the **reset mindown** command and the time when the supervisor engine comes online running the new software image are not saved or synchronized with the redundant supervisor engine.

If you reset an intelligent module (such as the Catalyst 6000 family MSM or MSFC), both the module hardware and software are completely reset.

When entering the *bootdevice*, use the format *device*[:*device_qualifier*] where:

- *device* = **pcmcia**, **hdd**, **network**
- *device_qualifier* **hdd** = number from 1 to 99
- **pcmcia** = slot0 or slot1

Examples

This example shows how to reset the supervisor engine on a Catalyst 6000 family switch with redundant supervisor engines:

```
Console> (enable) reset 1
This command will force a switch-over to the standby supervisor module
and disconnect your telnet session.
Do you want to continue (y/n) [n]? y
Connection closed by foreign host.
host%
```

This example shows how to reset module 4:

```
Console> (enable) reset 4
This command will reset module 4 and may disconnect your telnet session.
Do you want to continue (y/n) [n]? y
Resetting module 4...
Console> (enable)
```

This example shows how to schedule a system reset for a specific future time:

```
Console> (enable) reset at 20:00
Reset scheduled at 20:00:00, Wed Mar 15 2000.
Proceed with scheduled reset? (y/n) [n]? y
Reset scheduled for 20:00:00, Wed Mar 15 2000 (in 0 day 5 hours 40 minutes).
Console> (enable)
```

This example shows how to schedule a reset for a specific future time and include a reason for the reset:

```
Console> (enable) reset at 23:00 3/15 Software upgrade to 6.1(1).
Reset scheduled at 23:00:00, Wed Mar 15 2000.
Reset reason: Software upgrade to 6.1(1).
Proceed with scheduled reset? (y/n) [n]? y
Reset scheduled for 23:00:00, Wed Mar 15 2000 (in 0 day 8 hours 39 minutes).
Console> (enable)
```

This example shows how to schedule a reset with minimum downtime for a specific future time and include a reason for the reset:

```
Console> (enable) reset mindown at 23:00 3/15 Software upgrade to 6.1(1).
Reset scheduled at 23:00:00, Wed Mar 15 2000.
Reset reason: Software upgrade to 6.1(1).
Proceed with scheduled reset? (y/n) [n]? y
Reset mindown scheduled for 23:00:00, Wed Mar 15 2000 (in 0 day 8 hours 39 minutes).
Console> (enable)
```

This example shows how to schedule a reset after a specified time:

```
Console> (enable) reset in 5:20 Configuration update
Reset scheduled in 5 hours 20 minutes.
Reset reason: Configuration update
Proceed with scheduled reset? (y/n) [n]? y
Reset scheduled for 19:56:01, Wed Mar 15 2000 (in 5 hours 20 minutes).
Reset reason: Configuration update
Console> (enable)
```

This example shows how to cancel a scheduled reset:

```
Console> (enable) reset cancel
Reset cancelled.
Console> (enable)
```

Related Commands

commit
show reset

restore counters

Use the **restore counters** command to restore MAC and port counters.

restore counters [**all** | *mod/ports*]

Syntax Description

all	(Optional) Keyword to specify all ports.
mod/ports	(Optional) Number of the module and the ports on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not specify a range of ports to be restored, then all ports on the switch are restored.

Examples

This example shows how to restore MAC and port counters:

```
Console> (enable) restore counters all
This command will restore all counter values reported by the CLI to the hardware counter
values.
Do you want to continue (y/n) [n]? y
MAC and Port counters restored.
Console> (enable)
```

Related Commands

clear counters
show port counters

rollback

Use the **rollback** command to clear changes made to the ACL edit buffer since its last save. The ACL is rolled back to its state at the last **commit** command.

rollback qos acl {*acl_name* | **all**}

rollback security acl {*acl_name* | **all** | **adjacency**}

Syntax Description

qos acl	Keyword to specify QoS ACEs.
acl_name	Name that identifies the VACL whose ACEs are to be affected.
all	Keyword to rollback all ACLs.
security acl	Keywords to specify security ACEs.
adjacency	Keyword to rollback all adjacency tables.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear the edit buffer of a specific QoS ACL:

```
Console> (enable) rollback qos acl ip-8-1
Rollback for QoS ACL ip-8-1 is successful.
Console> (enable)
```

This example shows how to clear the edit buffer of a specific security ACL:

```
Console> (enable) rollback security acl IPACL1
IPACL1 editbuffer modifications cleared.
Console> (enable)
```

Related Commands

commit
show qos acl info

session

Use the **session** command to open a session with a module (for example, the MSM, NAM, or ATM). This command allows you to use the module-specific CLI.

session *mod*

Syntax Description

mod	Number of the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

After you enter this command, the system responds with the Enter Password: prompt, if one is configured on the module.

To end the session, enter the **quit** command.

Use the **session** command to toggle between router and switch sessions.

For information on ATM commands, refer to the *ATM Software Configuration Guide and Command Reference for the Catalyst 5000 Family and 6000 Family Switches*.

For information on NAM commands, refer to the *Catalyst 6000 Network Analysis Module Installation and Configuration Note*.

Examples

This example shows how to open a session with an MSM (module 4):

```
Console> session 4
Trying Router-4...
Connected to Router-4.
Escape character is `^]'.

Router>
```

Related Commands

quit
switch console

set

Use the **set** command to display all of the ROM monitor variable names with their values.

set

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

ROM monitor command.

Command Modes

Normal.

Examples

This example shows how to display all of the ROM monitor variable names with their values:

```
rommon 2 > set
PS1=rommon ! >
BOOT=
?=0
```

Related Commands

varname=

set accounting commands

Use the **set accounting commands** command to enable command event accounting on the switch.

set accounting commands enable {**config** | **enable** | **all**} [**stop-only**] {**tacacs+**}

set accounting commands disable

Syntax Description

enable	Keyword to enable the specified accounting method for commands.
config	Keyword to permit accounting for configuration commands only.
enable	Keyword to permit accounting for enable mode commands only.
all	Keyword to permit accounting for all commands.
stop-only	(Optional) Keyword to apply the accounting method at the command end.
tacacs+	Keyword to specify TACACS+ accounting for commands.
disable	Keyword to disable accounting for commands.

Defaults

The default is accounting is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You must configure the TACACS+ servers before you enable accounting.

Examples

This example shows how to send records at the end of the event only using a TACACS+ server:

```
Console> (enable) set accounting commands enable config stop-only tacacs+
Accounting set to enable for commands-config events in stop-only mode.
Console> (enable)
```

Related Commands

set accounting connect
set accounting exec
set accounting suppress
set accounting system
set accounting update
set tacacs server
show accounting

set accounting connect

Use the **set accounting connect** command to enable accounting of outbound connection events on the switch.

set accounting connect enable {**start-stop** | **stop-only**} {**tacacs+** | **radius**}

set accounting connect disable

Syntax Description

enable	Keyword to enable the specified accounting method for connection events.
start-stop	Keyword to apply the accounting method at the start and stop of the connection event.
stop-only	Keyword to apply the accounting method at the end of the connection event.
tacacs+	Keyword to specify TACACS+ accounting for connection events.
radius	Keyword to specify RADIUS accounting for connection events.
disable	Keyword to disable accounting of connection events.

Defaults

The default is accounting is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You must configure the RADIUS or TACACS+ servers and shared secret keys before you enable accounting.

Examples

This example shows how to enable accounting on Telnet and remote login sessions, generating records at stop only using a TACACS+ server:

```
Console> (enable) set accounting connect enable stop-only tacacs+
Accounting set to enable for connect events in stop-only mode..
Console> (enable)
```

Related Commands

set accounting commands
set accounting exec
set accounting suppress
set accounting system
set accounting update
set radius key
set radius server
set tacacs key
set tacacs server
show accounting

set accounting exec

Use the **set accounting exec** command to enable accounting of normal login sessions on the switch.

set accounting exec enable {**start-stop** | **stop-only**} {**tacacs+** | **radius**}

set accounting exec disable

Syntax Description

enable	Keyword to enable the specified accounting method for normal login sessions.
start-stop	Keyword to specify the accounting method applies at the start and stop of the normal login sessions.
stop-only	Keyword to specify the accounting method applies at the end of the normal login sessions.
tacacs+	Keyword to specify TACACS+ accounting for normal login sessions.
radius	Keyword to specify RADIUS accounting for normal login sessions.
disable	Keyword to disable accounting for normal login sessions.

Defaults

The default is accounting is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You must configure the RADIUS or TACACS+ servers and shared secret keys before you enable accounting.

Examples

This example shows how to enable accounting of normal login sessions, generating records at start and stop using a RADIUS server:

```
Console> (enable) set accounting exec enable start-stop radius
Accounting set to enable for exec events in start-stop mode.
Console> (enable)
```

This example shows how to enable accounting of normal login sessions, generating records at stop using a TACACS+ server:

```
Console> (enable) set accounting exec enable stop-only tacacs+
Accounting set to enable for exec events in stop-only mode.
Console> (enable)
```

Related Commands

- set accounting commands
- set accounting connect
- set accounting suppress
- set accounting system
- set accounting update
- set radius key
- set radius server
- set tacacs key
- set tacacs server
- show accounting

set accounting suppress

Use the **set accounting suppress** command to enable or disable suppression of accounting information for a user who has logged in without a username.

set accounting suppress null-username {**enable** | **disable**}

Syntax Description

null-username	Keyword to specify users must have a user ID.
enable	Keyword to enable suppression for a specified user.
disable	Keyword to disable suppression for a specified user.

Defaults

The default is accounting is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You must configure the TACACS+ servers before you enable accounting.

Examples

This example shows how to suppress accounting information for users without a username:

```
Console> (enable) set accounting suppress null-username enable
Accounting will be suppressed for user with no username.
Console> (enable)
```

This example shows how to include users without the usernames' accounting event information:

```
Console> (enable) set accounting suppress null-username disable
Accounting will be not be suppressed for user with no username.
Console> (enable)
```

Related Commands

set accounting commands
set accounting connect
set accounting exec
set accounting system
set accounting update
set tacacs server
show accounting

set accounting system

Use the **set accounting system** command to enable accounting of system events on the switch.

set accounting system enable {**start-stop** | **stop-only**} {**tacacs+** | **radius**}

set accounting system disable

Syntax Description

enable	Keyword to enable the specified accounting method for system events.
start-stop	Keyword to specify the accounting method applies at the start and stop of the system event.
stop-only	Keyword to specify the accounting method applies at the end of the system event.
tacacs+	Keyword to specify TACACS+ accounting for system events.
radius	Keyword to specify RADIUS accounting for system events.
disable	Keyword to disable accounting for system events.

Defaults

The default is accounting is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You must configure the RADIUS or TACACS+ servers and shared secret keys before you enable accounting.

Examples

This example shows how to enable accounting for system events, sending records only at the end of the event using a RADIUS server:

```
Console> (enable) set accounting system enable stop-only radius
Accounting set to enable for system events in start-stop mode..
Console> (enable)
```

This example shows how to enable accounting for system events, sending records only at the end of the event using a TACACS+ server:

```
Console> (enable) set accounting system enable stop-only tacacs+
Accounting set to enable for system events in start-stop mode..
Console> (enable)
```

Related Commands

- set accounting commands
- set accounting connect
- set accounting exec
- set accounting suppress
- set accounting update
- set radius key
- set radius server
- set tacacs key
- set tacacs server
- show accounting

set accounting update

Use the **set accounting update** command to configure the frequency of accounting updates.

set accounting update {**new-info** | {**periodic** [*interval*]}}

Syntax Description

new-info	Keyword to specify an update when new information is available.
periodic	Keyword to specify an update on a periodic basis.
interval	(Optional) Periodic update interval time; valid values are from **1** to **71582** minutes.

Defaults

The default is accounting is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You must configure the TACACS+ servers before you enable accounting.

Examples

This example shows how to send accounting updates every 200 minutes:

```
Console> (enable) set accounting update periodic 200
Accounting updates will be periodic at 200 minute intervals.
Console> (enable)
```

This example shows how to send accounting updates only when there is new information:

```
Console> (enable) set accounting update new-info
Accounting updates will be sent on new information only.
Console> (enable)
```

Related Commands

set accounting commands
set accounting connect
set accounting exec
set accounting suppress
set accounting system
set tacacs server
show accounting

set aclmerge algo

Use the **set aclmerge algo** command to select the ACL merge algorithm.

set aclmerge algo {**bdd** | **odm**}

Syntax Description

algo	Keyword to set the ACL merge algorithm.
bdd	Keyword to specify the BDD-based ACL merge function.
odm	Keyword to specify the ODM-based ACL merge function.

Defaults

The merge algorithm is ODM.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If BDD is disabled, the merge algorithm can only be ODM. When BDD is enabled, you can choose either the BDD algorithm or the ODM algorithm. Use the **set aclmerge bdd** command to enable or disable BDD.

The ACL merge algorithm that you select is in effect for all new ACL merges. The ACLs already configured are not modified and use the ACL merge algorithm that was enabled when the ACLs were merged.

Examples

This example shows how to select ODM as the ACL merge algorithm:

```
Console> (enable) set aclmerge algo odm
Acl merge algorithm set to odm.
Console> (enable)
```

Related Commands

set aclmerge bdd
show aclmerge

set aclmerge bdd

Use the **set aclmerge bdd** command to enable or disable the binary decision diagram (BDD) ACL merge algorithm.

set aclmerge bdd {**enable** | **disable**}

Syntax Description

enable	Keywords to enable the BDD-based ACL merge function.
disable	Keywords to disable the BDD-based ACL merge function.

Defaults

BDD is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you enable or disable BDD, the change takes effect when your system is restarted.

BDD must be enabled in order to change the ACL merge algorithm.

Enabling BDD on a supervisor engine with 64 MB of RAM could cause memory to run low. To avoid this situation, upgrade the memory or disable BDD.

Examples

This example shows how to disable BDD:

```
Console> (enable) set aclmerge bdd disable
Bdd will be disabled on system restart.
Console> (enable)
```

This example shows how to enable BDD:

```
Console> (enable) set aclmerge bdd enable
Warning:enabling bdd on a supervisor with 64MB RAM
could cause memory to run low, to avoid this situation
please upgrade the memory or disable BDD.

Bdd will be enabled on system restart.
Console> (enable)
```

Related Commands

set aclmerge algo
show aclmerge

set alias

Use the **set alias** command to define aliases (shorthand versions) of commands.

set alias *name command* [*parameter*] [*parameter*]

Syntax Description

name	Alias being created.
command	Command for which the alias is being created.
parameter	(Optional) Parameters that apply to the command for which an alias is being created.

Defaults

The default is no aliases are configured.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The name **all** cannot be defined as an alias. Reserved words cannot be defined as aliases.

For additional information about *parameter*, see the specific command for information about applicable parameters.

Examples

This example shows how to set the alias for the **clear arp** command as arpdel:

```
Console> (enable) set alias arpdel clear arp
Command alias added.
Console> (enable)
```

Related Commands

clear alias
show alias

set arp

Use the **set arp** command to add IP address-to-MAC address mapping entries to the ARP table and to set the ARP aging time for the table.

set arp [**dynamic** | **permanent** | **static**] {*ip_addr hw_addr*}

set arp agingtime *agingtime*

Syntax Description

dynamic	(Optional) Keyword to specify that entries are subject to ARP aging updates.
permanent	(Optional) Keyword to specify that permanent entries are stored in NVRAM until they are removed by the **clear arp** or **clear config** command.
static	(Optional) Keyword to specify that entries are not subject to ARP aging updates.
ip_addr	IP address or IP alias to map to the specified MAC address.
hw_addr	MAC address to map to the specified IP address or IP alias.
agingtime	Keyword to set the period of time after which an ARP entry is removed from the ARP table.
agingtime	Number of seconds that entries will remain in the ARP table before being deleted; valid values are from **0** to **1,000,000** seconds. Setting this value to **0** disables aging.

Defaults

The default is no ARP table entries exist; ARP aging is set to 1200 seconds.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When entering the *hw_addr*, use a 6-hexadecimal byte MAC address in canonical (00-11-22-33-44-55) or noncanonical (00:11:22:33:44:55) format.

Static (nonpermanent) entries remain in the ARP table until you reset the active supervisor engine.

Examples

This example shows how to configure a dynamic ARP entry mapping that will age out after the configured ARP aging time:

```
Console> (enable) set arp dynamic 198.133.219.232 00-00-0c-40-0f-bc
ARP entry added.
Console> (enable)
```

This example shows how to set the aging time for the ARP table to 1800 seconds:

```
Console> (enable) set arp agingtime 1800
ARP aging time set to 1800 seconds.
Console> (enable)
```

This example shows how to configure a permanent ARP entry, which will remain in the ARP cache after a system reset:

```
Console> (enable) set arp permanent 198.146.232.23 00-00-0c-30-0f-bc
Permanent ARP entry added as
198.146.232.23 at 00-00-0c-30-0f-bc on vlan 5
Console> (enable)
```

This example shows how to configure a static ARP entry, which will be removed from the ARP cache after a system reset:

```
Console> (enable) set arp static 198.144.239.22 00-00-0c-50-0f-bc
Static ARP entry added as
198.144.239.22 at 00-00-0c-50-0f-bc on vlan 5
Console> (enable)
```

Related Commands

clear arp
show arp

set authentication enable

Use the **set authentication enable** command to enable authentication using the TACACS+, RADIUS, or Kerberos server to determine if you have privileged access permission.

set authentication enable {**radius** | **tacacs** | **kerberos**} **enable** [**console** | **telnet** | **http** | **all**] [**primary**]

set authentication enable {**enable** | **disable**} [**console** | **telnet** | **http** | **all**] [**primary**]

set authentication enable local {**enable** | **disable**} [**console** | **telnet** | **http** | **all**] [**primary**]

set authentication enable attempt *count* [**console** | **telnet**]

set authentication enable lockout *time* [**console** | **telnet**]

Syntax Description

radius	Keyword to specify RADIUS authentication for login.
tacacs	Keyword to specify TACACS+ authentication for login.
kerberos	Keyword to specify Kerberos authentication for login.
enable	Keyword to enable the specified authentication method for login.
console	(Optional) Keyword to specify the authentication method for console sessions.
telnet	(Optional) Keyword to specify the authentication method for Telnet sessions.
http	(Optional) Keyword to specify the specified authentication method for HTTP sessions.
all	(Optional) Keyword to apply the authentication method to all session types.
primary	(Optional) Keyword to specify the specified authentication method be tried first.
disable	Keyword to disable the specified authentication method for login.
local	Keyword to specify local authentication for login.
attempt *count*	Keyword and variable to specify the number of connection attempts before initiating an error; valid values are **0**, from **3** to **10**, and **0** to disable.
lockout *time*	Keyword and variable to specify the lockout timeout; valid values are from **30** to **600** seconds, and **0** to disable.

Defaults

The default is local authentication is enabled for console and Telnet sessions. RADIUS, TACACS+, and Kerberos are disabled for all session types. If authentication is enabled, the default **attempt** *count* is 3.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Use authentication configuration for both console and Telnet connection attempts unless you use the **console** or **telnet** keywords to specify the authentication methods for each connection type individually.

Examples

This example shows how to use the TACACS+ server to determine if a user has privileged access permission:

```
Console> (enable) set authentication enable tacacs enable
tacacs enable authentication set to enable for console, telnet and http session.
Console> (enable)
```

This example shows how to use the local password to determine if the user has privileged access permission:

```
Console> (enable) set authentication enable local enable
local enable authentication set to enable for console, telnet and http session.
Console> (enable)
```

This example shows how to use the RADIUS server to determine if a user has privileged access permission for all session types:

```
Console> (enable) set authentication enable radius enable
radius enable authentication set to enable for console, telnet and http session.
Console> (enable)
```

This example shows how to use the TACACS+ server to determine if a user has privileged access permission for all session types:

```
Console> (enable) set authentication enable tacacs enable console
tacacs enable authentication set to enable for console session.
Console> (enable)
```

This example shows how to set the Kerberos server to be used first:

```
Console> (enable) set authentication enable kerberos enable primary
kerberos enable authentication set to enable for console, telnet and http session as
primary authentication method.
Console> (enable)
```

This example shows how to limit enable mode login attempts:

```
Console> (enable) set authentication enable attempt 5
Enable mode authentication attempts for console and telnet logins set to 5.
Console> (enable)
```

This example shows how to set the enable mode lockout time for both console and Telnet connections:

```
Console> (enable) set authentication enable lockout 50
Enable mode lockout time for console and telnet logins set to 50.
Console> (enable)
```

Related Commands

set authentication login
show authentication

set authentication login

Use the **set authentication login** command to enable TACACS+, RADIUS, or Kerberos as the authentication method for login.

set authentication login {**radius** | **tacacs** | **kerberos**} **enable** [**console** | **telnet** | **http** | **all**] [**primary**]

set authentication login {**radius** | **tacacs** | **kerberos**} **disable** [**console** | **telnet** | **http** | **all**]

set authentication login {**enable** | **disable**} [**console** | **telnet** | **http** | **all**]

set authentication login local {**enable** | **disable**} [**console** | **telnet** | **http** | **all**]

set authentication login attempt *count* [**console** | **telnet**]

set authentication login lockout *time* [**console** | **telnet**]

Syntax Description

radius	Keyword to specify the use of the RADIUS server password to determine if you have access permission to the switch.
tacacs	Keyword to specify the use of the TACACS+ server password to determine if you have access permission to the switch.
kerberos	Keyword to specify the Kerberos server password to determine if you have access permission to the switch.
enable	Keyword to enable the specified authentication method for login.
console	(Optional) Keyword to specify the authentication method for console sessions.
telnet	(Optional) Keyword to specify the authentication method for Telnet sessions.
http	(Optional) Keyword to specify the authentication method for HTTP sessions.
all	(Optional) Keyword to specify the authentication method for all session types.
primary	(Optional) Keyword to specify that the method specified is the primary authentication method for login.
disable	Keyword to disable the specified authentication method for login.
local	Keyword to specify a local password to determine if you have access permission to the switch.
attempt *count*	Keyword and variable to specify the number of login attempts before initiating an error; valid values are **0**, from **3** to **10**, and **0** to disable.
lockout *time*	Keyword and variable to specify the lockout timeout; valid values are from **30** to **600** seconds, and **0** to disable.

Defaults

The default is local authentication is the primary authentication method for login.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command allows you to choose the authentification method for the web interface. If you configure the authentification method for the HTTP session as RADIUS, then the username or password is validated using the RADIUS protocol, and TACACS+ and Kerberos authentication is set to disable for the HTTP sessions. By default, the HTTP login is validated using the local login password.

You can specify the authentication method for **console**, **telnet**, **http**, or **all** by entering the **console**, **telnet**, **http**, or **all** keywords. If you do not specify **console**, **telnet**, **http**, or **all**, the authentication method default is for **all** sessions.

Examples

This example shows how to disable TACACS+ authentication access for Telnet sessions:

```
Console> (enable) set authentication login tacacs disable telnet
tacacs login authentication set to disable for the telnet sessions.
Console> (enable)
```

This example shows how to disable RADIUS authentication access for console sessions:

```
Console> (enable) set authentication login radius disable console
radius login authentication set to disable for the console sessions.
Console> (enable)
```

This example shows how to disable Kerberos authentication access for Telnet sessions:

```
Console> (enable) set authentication login kerberos disable telnet
kerberos login authentication set to disable for the telnet sessions.
Console> (enable)
```

This example shows how to set TACACS+ authentication access as the primary method for HTTP sessions:

```
Console> (enable) set authentication login tacacs enable http primary
tacacs login authentication set to enable for HTTP sessions as primary authentification
method.
Console> (enable)
```

This example shows how to limit login attempts:

```
Console> (enable) set authentication login attempt 5
Login authentication attempts for console and telnet logins set to 5.
Console> (enable)
```

This example shows how to set the lockout time for both console and Telnet connections:

```
Console> (enable) set authentication login lockout 50
Login lockout time for console and telnet logins set to 50.
Console> (enable)
```

Related Commands

set authentication enable
show authentication

set authorization commands

Use the **set authorizaton commands** command to enable authorization of command events on the switch.

set authorization commands enable {**config** | **enable** | **all**} {*option*} {*fallbackoption*} [**console** | **telnet** | **both**]

set authorization commands disable [**console** | **telnet** | **both**]

Syntax Description

enable	Keyword to enable the specified authorization method for commands.
config	Keyword to permit authorization for configuration commands only.
enable	Keyword to permit authorization for enable mode commands only.
all	Keyword to permit authorization for all commands.
option	Switch response to an authorization request; valid values are **tacacs+**, **if-authenticated**, and **none**. See the "Usage Guidelines" section for valid value definitions.
fallbackoption	Switch fallback response to an authorization request if the TACACS+ server is down or not responding; valid values are **tacacs+**, **deny**, **if-authenticated**, and **none**. See the "Usage Guidelines" section for valid value definitions.
disable	Keyword to disable authorization of command events.
console	(Optional) Keyword to specify the authorization method for console sessions.
telnet	(Optional) Keyword to specify the authorization method for Telnet sessions.
both	(Optional) Keyword to specify the authorization method for both console and Telnet sessions.

Defaults

The default is authorization is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you define the *option* and *fallbackoption* values, the following occurs:

- **tacacs+** specifies the TACACS+ authorization method.
- **deny** does not let you proceed.

- **if-authenticated** allows you to proceed with your action if you have been authenticated.
- **none** allows you to proceed without further authorization in case the TACACS+ server does not respond.

Examples

This example shows how to enable authorization for all commands with the **if-authenticated** *option* and **none** *fallbackoption*:

```
Console> (enable) set authorization commands enable all if-authenticated none
Successfully enabled commands authorization.
Console> (enable)
```

This example shows how to disable command authorization:

```
Console> (enable) set authorization commands disable
Successfully disabled commands authorization.
Console> (enable)
```

Related Commands

set authorization enable
set authorization exec
show authorization

set authorization enable

Use the **set authorization enable** command to enable authorization of privileged mode sessions on the switch.

set authorization enable enable {*option*} {*fallbackoption*} [**console** | **telnet** | **both**]

set authorization enable disable [**console** | **telnet** | **both**]

Syntax Description

enable	Keyword to enable the specified authorization method.
option	Switch response to an authorization request; valid values are **tacacs+**, **if-authenticated**, and **none**. See the "Usage Guidelines" section for valid value definitions.
fallbackoption	Switch fallback response to an authorization request if the TACACS+ server is down or not responding; valid values are **tacacs+**, **deny**, **if-authenticated**, and **none**. See the "Usage Guidelines" section for valid value definitions.
disable	Keyword to disable the authorization method.
console	(Optional) Keyword to specify the authorization method for console sessions.
telnet	(Optional) Keyword to specify the authorization method for Telnet sessions.
both	(Optional) Keyword to specify the authorization method for both console and Telnet sessions.

Defaults

The default is authorization is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you define the *option* and *fallbackoption* values, the following occurs:

- **tacacs+** specifies the TACACS+ authorization method.
- **deny** does not let you proceed.
- **if-authenticated** allows you to proceed with your action if you have authentication.
- **none** allows you to proceed without further authorization in case the TACACS+ server does not respond.

Examples

This example shows how to enable authorization of configuration commands in enable, privileged login mode, sessions:

```
Console> (enable) set authorization enable enable if-authenticated none
Successfully enabled enable authorization.
Console> (enable)
```

This example shows how to disable enable mode authorization:

```
Console> (enable) set authorization enable disable
Successfully disabled enable authorization.
Console> (enable)
```

Related Commands

set authorization commands
set authorization exec
show authorization

set authorization exec

Use the **set authorization exec** command to enable authorization of exec, normal login mode, session events on the switch.

set authorization exec enable {*option*} {*fallbackoption*} [**console** | **telnet** | **both**]

set authorization exec disable [**console** | **telnet** | **both**]

Syntax Description

enable	Keyword to enable the specified authorization method.
option	Switch response to an authorization request; valid values are **tacacs+**, **if-authenticated**, and **none**. See the "Usage Guidelines" section for valid value definitions.
fallbackoption	Switch fallback response to an authorization request if the TACACS+ server is down or not responding; valid values are **tacacs+**, **deny**, **if-authenticated**, and **none**. See the "Usage Guidelines" section for valid value definitions.
disable	Keyword to disable authorization method.
console	(Optional) Keyword to specify the authorization method for console sessions.
telnet	(Optional) Keyword to specify the authorization method for Telnet sessions.
both	(Optional) Keyword to specify the authorization method for both console and Telnet sessions.

Defaults

The default is authorization is denied.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you define the *option* and *fallbackoption* values, the following occurs:

- **tacacs+** specifies the TACACS+ authorization method.
- **deny** fails authorization if the TACACS+ server does not respond.
- **if-authenticated** allows you to proceed with your action if the TACACS+ server does not respond and you have authentication.
- **none** allows you to proceed without further authorization if the TACACS+ server does not respond.

Examples

This example shows how to enable authorization of configuration commands in exec, normal login mode, sessions:

```
Console> (enable) set authorization exec enable if-authenticated none
Successfully enabled exec authorization.
Console> (enable)
```

This example shows how to disable exec mode authorization:

```
Console> (enable) set authorization exec disable
Successfully disabled exec authorization.
Console> (enable)
```

Related Commands

set authorization commands
set authorization enable
show authorization

set banner lcd

Use the **set banner lcd** command to configure the Catalyst 6500 series Switch Fabric Module LCD user banner.

set banner lcd *c* [*text*] *c*

Syntax Description

c	Delimiting character used to begin and end the message.
text	(Optional) Message of the day.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The banner may contain no more than 800 characters, including tabs. Tabs display as eight characters but take only one character of memory.

Once you configure the user banner, it is sent down to all Catalyst 6500 series Switch Fabric Modules in the switch and displayed in the LCD.

Examples

This example shows how to set the Catalyst 6500 series Switch Fabric Module LCD user banner:

```
Console> (enable) set banner lcd &hello
there&
LCD banner set
Console> (enable)
```

Related Commands

show banner

set banner motd

Use the **set banner motd** command to program an MOTD banner to appear before session login.

set banner motd *c* [*text*] *c*

Syntax Description

c	Delimiting character used to begin and end the message.
text	(Optional) Message of the day.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The banner may contain no more than 3,070 characters, including tabs. Tabs display as eight characters but take only one character of memory.

You can use either the **clear banner motd** command or the **set banner motd** *cc* command to clear the message-of-the-day banner.

Examples

This example shows how to set the message of the day using the pound sign (#) as the delimiting character:

```
Console> (enable) set banner motd #
** System upgrade at 6:00am Tuesday.
** Please log out before leaving on Monday. #
MOTD banner set.
Console> (enable)
```

This example shows how to clear the message of the day:

```
Console> (enable) set banner motd ##
MOTD banner cleared.
Console> (enable)
```

Related Commands

clear banner motd
show banner

set boot auto-config

Use the **set boot auto-config** command to specify one or more configuration files to use to configure the switch at bootup. The list of configuration files is stored in the CONFIG_FILE environment variable.

set boot auto-config *device:filename* [**;***device:filename...*] [*mod*]

Syntax Description

*device***:**	Device where the startup configuration file resides.
filename	Name of the startup configuration file.
mod	(Optional) Module number of the supervisor engine containing the Flash device.

Defaults

The default CONFIG_FILE is slot0:switch.cfg.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set boot auto-config** command always overwrites the existing CONFIG_FILE environment variable settings (you cannot prepend or append a file to the variable contents).

If you specify multiple configuration files, you must separate the files with a semicolon (;).

To set the recurrence on other supervisor engines and switches, use the **set boot config-register auto-config** command.

Examples

This example shows how to specify a single configuration file environment variable:

```
Console> (enable) set boot auto-config slot0:cfgfile2
CONFIG_FILE variable = slot0:cfgfile2
WARNING: nvram configuration may be lost during next bootup,
         and re-configured using the file(s) specified.
Console> (enable)
```

This example shows how to specify multiple configuration file environment variables:

```
Console> (enable) set boot auto-config slot0:cfgfile;slot0:cfgfile2
CONFIG_FILE variable = slot0:cfgfile1;slot0:cfgfile2
WARNING: nvram configuration may be lost during next bootup,
         and re-configured using the file(s) specified.
Console> (enable)
```

Related Commands

set boot config-register
set boot system flash
show boot

set boot config-register

Use the **set boot config-register** command to configure the boot configuration register value.

set boot config-register 0x*value* [*mod*]

set boot config-register baud {**1200** | **2400** | **4800** | **9600** | **19200** | **38400**} [*mod*]

set boot config-register ignore-config {**enable** | **disable**} [*mod*]

set boot config-register boot {**rommon** | **bootflash** | **system**} [*mod*]

Syntax Description

0x*value*	Keyword to set the 16-bit configuration register value.
mod	(Optional) Module number of the supervisor engine containing the Flash device.
baud 1200 | **2400** | **4800** | **9600** | **19200** | **38400**	Keywords to specify the console baud rate.
ignore-config	Keywords to set the ignore-config feature.
enable	Keyword to enable the specified feature.
disable	Keyword to disable the specified feature.
boot	Keyword to specify the boot image to use on the next restart.
rommon	Keyword to specify booting from the ROM monitor.
bootflash	Keyword to specify booting from the bootflash.
system	Keyword to specify booting from the system.

Defaults

The defaults are as follows:

- Configuration register value is 0x10F, which causes the switch to boot from what is specified by the BOOT environment variable.
- Baud rate is set to 9600.
- **ignore-config** parameter is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

We recommend that you use only the **rommon** and **system** options with the **set boot config-register boot** command.

Each time you enter one of the **set boot config-register** commands, the system displays all current configuration-register information (the equivalent of entering the **show boot** command).

The baud rate specified in the configuration register is used by the ROM monitor only and is different from the baud rate specified by the **set system baud** command.

When you enable the **ignore-config** feature, the system software ignores the configuration. Enabling the **ignore-config** parameter is the same as entering the **clear config all** command; that is, it clears the entire configuration stored in NVRAM the next time the switch is restarted.

Examples

This example shows how to specify booting from the ROM monitor:

```
Console> (enable) set boot config-register boot rommon
Configuration register is 0x100
ignore-config: disabled
console baud: 9600
boot: the ROM monitor
Console> (enable)
```

This example shows how to specify the default 16-bit configuration register value:

```
Console> (enable) set boot config-register 0x12f
Configuration register is 0x12f
break: disabled
ignore-config: disabled
console baud: 9600
boot: image specified by the boot system commands
Console> (enable)
```

This example shows how to change the ROM monitor baud rate to 4800:

```
Console> (enable) set boot config-register baud 4800
Configuration register is 0x90f
ignore-config: disabled
console baud: 4800
boot: image specified by the boot system commands
Console> (enable)
```

This example shows how to ignore the configuration information stored in NVRAM the next time the switch is restarted:

```
Console> (enable) set boot config-register ignore-config enable
Configuration register is 0x94f
ignore-config: enabled
console baud: 4800
boot: image specified by the boot system commands
Console> (enable)
```

This example shows how to specify rommon as the boot image to use on the next restart:

```
Console> (enable) set boot config-register boot rommon
Configuration register is 0x100
ignore-config: disabled
console baud: 9600
boot: the ROM monitor
Console> (enable)
```

Related Commands

- copy
- set boot auto-config
- set boot system flash
- set config acl nvram
- show boot
- show config

set boot config-register auto-config

Use the **set boot config-register auto-config** command to configure auto-config file dispensation.

set boot config-register auto-config {**recurring** | **non-recurring**} [*mod*]

set boot config-register auto-config {**overwrite** | **append**}

set boot config-register auto-config sync {**enable** | **disable**}

Syntax Description

recurring	Keyword to set auto-config to recurring and specify the switch retains the contents of the CONFIG_FILE environment variable after the switch is reset or power cycled and configured.
non-recurring	Keyword to set auto-config to nonrecurring and cause the switch to clear the contents of the CONFIG_FILE environment variable after the switch is reset or power cycled and before the switch is configured.
mod	(Optional) Module number of the supervisor engine containing the Flash device.
overwrite	Keyword to cause the auto-config file to overwrite the NVRAM configuration.
append	Keyword to cause the auto-config file to append to the file currently in the NVRAM configuration.
sync enable | **disable**	Keywords to enable or disable synchronization of the auto-config file.

Defaults

The defaults are as follows:

- **overwrite**
- **non-recurring**
- **sync is disable**

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **auto-config overwrite** command clears the NVRAM configuration before executing the Flash configuration file. The **auto-config append** command executes the Flash configuration file before clearing the NVRAM configuration.

If you delete the auto-config Flash files on the supervisor engine, the files will also be deleted on the standby supervisor engine.

If you enter the **sync enable** keywords, this enables synchronization to force the configuration files to synchronize automatically to the redundant supervisor engine. The files are kept consistent with what is on the active supervisor engine.

If you use the **set boot auto-config bootflash:switch.cfg** with the overwrite option, you must use the **copy config bootflash:switch.cfg** command to save the switch configuration to the auto-config file.

If you use the **set boot auto-config bootflash:switchapp.cfg** with the append option, you can use the **copy acl config bootflash:switchapp.cfg** command to save the switch configuration to the auto-config file.

If the ACL configuration location is set to Flash memory, the following message is displayed after every commit operation for either security or QoS. Use the **copy** command to save your ACL configuration to Flash memory. If you reset the system and you made one or more commits but did not copy commands to one of the files specified in the CONFIG_FILE variable, the following message displays:

```
Warning: System ACL configuration has been modified but not saved to Flash.
```

The files used with the **recurring** and **non-recurring** options are those specified by the CONFIG_FILE environment variable.

Examples

This example shows how to specify the ACL configuration Flash file at system startup:

```
Console> (enable) set boot auto-config bootflash:switchapp.cfg
Console> (enable) set boot config-register auto-config recurring
Console> (enable)
```

This example shows how to ignore the configuration information stored in NVRAM the next time the switch is restarted:

```
Console> (enable) set boot config-register auto-config non-recurring
Configuration register is 0x2102
ignore-config: disabled
auto-config: non-recurring, overwrite, auto-sync disabled
console baud: 9600
boot: image specified by the boot system commands
Console> (enable)
```

This example shows how to append the auto-config file to the file currently in the NVRAM configuration:

```
Console> (enable) set boot config-register auto-config append
Configuration register is 0x2102
ignore-config: disabled
auto-config: non-recurring, append, auto-sync disabled
console baud: 9600
boot: image specified by the boot system commands
Console> (enable)
```

This example shows how to use the auto-config overwrite option to save the ACL configuration to a bootflash file:

```
Console> (enable) copy config bootflash: switch.cfg
Console> (enable) set boot auto-config bootflash:switch.cfg
Console> (enable) set boot config-register auto-config overwrite
Console> (enable)
```

Caution The following two examples assume that you have saved the ACL configuration to the bootflash:switchapp.cfg file.

This example shows how to enable synchronization of the auto-config file:

```
Console> (enable) set boot config-register auto-config sync enable
Configuration register is 0x2102
ignore-config: disabled
auto-config: non-recurring, append, auto-sync enabled
console baud: 9600
boot: image specified by the boot system commands
Console> (enable)
```

This example shows how to disable synchronization of the auto-config file:

```
Console> (enable) set boot config-register auto-config sync disable
Configuration register is 0x2102
ignore-config: disabled
auto-config: non-recurring, append, auto-sync disabled
console baud: 9600
boot: image specified by the boot system commands
Console> (enable)
```

Related Commands

set boot config-register
set boot system flash
show boot

set boot device

Use the **set boot device** command to set the NAM or IDS boot environment.

set boot device *bootseq*[**,***bootseq*] *mod*

Syntax Description

bootseq	Device where the startup configuration file resides; see the "Usage Guidelines" section for format guidelines. The second *bootseq* is optional.
mod	Number of the module containing the Flash device.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you enter the **set boot device** command, the existing boot string in the supervisor engine NVRAM is always overwritten.

When you enter the *bootseq*, use the following guidelines:

- *bootseq* = *bootdevice*[**:***bootdevice-qualifier*]
- *bootdevice* is the device where the startup configuration file resides; valid values are **pcmcia**, **hdd**, or **network**.
- *bootdevice-qualifier* is the name of the startup configuration file; valid values for **hdd** are from 1 to 99, and for **pcmcia**, valid values are slot0 or slot1.
- The colon between *bootdevice* and *bootdevice-qualifier* is required.
- You can enter multiple *bootseqs* by separating each entry with a comma; 15 is the maximum number of boot sequences you can enter.

The supervisor engine does not validate the boot device you specify, but simply stores the boot device list in NVRAM.

This command is supported by the NAM or IDS only.

Examples

This example shows how to specify the boot environment to boot to the maintenance partition of the NAM on module 2:

```
Console> (enable) set boot device hdd:2 2
Device BOOT variable = hdd:2
Warning: Device list is not verified but still set in the boot string.
Console> (enable)
```

This example shows how to specify multiple boot environments on module 5:

```
Console> (enable) set boot device hdd,hdd:5,pcmcia:slot0,network,hdd:6 5
Device BOOT variable = hdd,hdd:5,pcmcia:slot0,network,hdd:6
Warning:Device list is not verified but still set in the boot string.
Console> (enable)
```

Related Commands

clear boot device
show boot device

set boot sync now

Use the **set boot sync now** command to immediately initiate synchronization of the system image between the active and redundant supervisor engine.

set boot sync now

Syntax Description

This command has no arguments or keywords.

Defaults

The default is synchronization is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set boot sync now** command is similar to the **set boot config-register auto-config** command with the **sync** keyword added. The **set boot sync now** command initiates synchronization to force the configuration files to synchronize automatically to the redundant supervisor engine. The files are kept consistent with what is on the active supervisor engine.

Examples

This example shows how to initiate synchronization of the auto-config file:

```
Console> (enable) set boot sync now
Console> (enable)
```

Related Commands

set boot auto-config
show boot

set boot system flash

Use the **set boot system flash** command to set the BOOT environment variable that specifies a list of images the switch loads at startup.

set boot system flash *device***:**[*filename*] [**prepend**] [*mod*]

Syntax Description

*device***:**	Device where the Flash resides.
filename	(Optional) Name of the configuration file.
prepend	(Optional) Keyword to place the device first in the list of boot devices.
mod	(Optional) Module number of the supervisor engine containing the Flash device.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

A colon (:) is required after the specified device.

You can enter several **boot system** commands to provide a fail-safe method for booting the switch. The system stores and executes the **boot system** commands in the order in which you enter them. Remember to clear the old entry when building a new image with a different filename in order to use the new image.

If the file does not exist (for example, if you entered the wrong filename), then the filename is appended to the bootstring, and this message displays, "Warning: File not found but still added in the bootstring."

If the file does exist, but is not a supervisor engine image, the file is not added to the bootstring, and this message displays, "Warning: file found but it is not a valid boot image."

Examples

This example shows how to append the filename cat6000-sup.5-5-1.bin on device bootflash to the BOOT environment variable:

```
Console> (enable) set boot system flash bootflash:cat6000-sup.5-5-1.bin
BOOT variable = bootflash:cat6000-sup.5-4-1.bin,1;bootflash:cat6000-sup.5-5-1.bin,1;
Console> (enable)
```

This example shows how to prepend cat6000-sup.5-5-1.bin to the beginning of the boot string:

```
Console> (enable) set boot system flash bootflash:cat6000-sup.5-5-1.bin prepend
BOOT variable = bootflash:cat6000-sup.5-5-1.bin,1;bootflash:cat6000-sup.5-4-1.bin,1;
Console> (enable)
```

Related Commands

clear boot system
show boot

set cam

Use the **set cam** command to add entries into the CAM table, set the aging time for the CAM table, and configure traffic filtering from and to a specific host.

set cam {**dynamic** | **static** | **permanent**} {*unicast_mac* | *route_descr*} *mod/port* [*vlan*]

set cam {**static** | **permanent**} {*multicast_mac*} *mod/ports..* [*vlan*]

set cam {**static** | **permanent**} **filter** {*unicast_mac*} *vlan*

set cam agingtime *vlan agingtime*

Syntax Description

dynamic	Keyword to specify entries are subject to aging.
static	Keyword to specify entries are not subject to aging.
permanent	Keyword to specify permanent entries are stored in NVRAM until they are removed by the **clear cam** or **clear config** command.
unicast_mac	MAC address of the destination host used for a unicast.
route_descr	Route descriptor of the "next hop" relative to this switch; valid values are from **0** to **0xffff**.
mod/port	Number of the module and the port on the module.
vlan	(Optional) Number of the VLAN; valid values are from **1** to **1005** and from **1025** to **4094**.
multicast_mac	MAC address of the destination host used for a multicast.
mod/ports..	Number of the module and the ports on the module.
filter	Keyword to specify a traffic filter entry.
agingtime	Keyword to set the period of time after which an entry is removed from the table.
agingtime	Number of seconds (**0** to **1,000,000**) dynamic entries remain in the table before being deleted.

Defaults

The default configuration has a local MAC address, spanning tree address (01-80-c2-00-00-00), and CDP multicast address for destination port 1/3 (the supervisor engine). The default aging time for all configured VLANs is 300 seconds.

The *vlan* variable is required when you configure the traffic filter entry.

Setting the aging time to 0 disables aging.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If the given MAC address is a multicast address (the least significant bit of the most significant byte is set to 1) or broadcast address (ff-ff-ff-ff-ff-ff) and you specify multiple ports, the ports must all be in the same VLAN. If the given address is a unicast address and you specify multiple ports, the ports must be in different VLANs.

The MSM does not support the **set cam** command.

If you enter a route descriptor with no VLAN parameter specified, the default is the VLAN already associated with the port. If you enter a route descriptor, you may only use a single port number (of the associated port).

The MAC address and VLAN for a host can be stored in the NVRAM it is maintained even after a reset.

The *vlan* number is optional unless you are setting CAM entries to dynamic, static, or permanent for a trunk port, or if you are using the **agingtime** keyword.

If port(s) are trunk ports, you must specify the VLAN.

Static (nonpermanent) entries remain in the table until you reset the active supervisor engine.

Enter the *route_descr* variable as two hexadecimal bytes in the following format: 004F. Do not use a "-" to separate the bytes.

Examples

This example shows how to set the CAM table aging time to 300 seconds:

```
Console> (enable) set cam agingtime 1 300
Vlan 1 CAM aging time set to 300 seconds.
Console> (enable)
```

This example shows how to add a unicast entry to the table for module 2, port 9:

```
Console> (enable) set cam static 00-00-0c-a0-03-fa 2/9
Static unicast entry added to CAM table.
Console> (enable)
```

This example shows how to add a permanent multicast entry to the table for module 1, port 1, and module 2, ports 1, 3, and 8 through 12:

```
Console> (enable) set cam permanent 01-40-0b-a0-03-fa 1/1,2/1,2/3,2/8-12
Permanent multicast entry added to CAM table.
Console> (enable)
```

This example shows how to add a traffic filter entry to the table:

```
Console> (enable) set cam static filter 00-02-03-04-05-06 1
Filter entry added to CAM table.
Console> (enable)
```

Related Commands

clear cam
show cam

set cdp

Use the **set cdp** command set to enable, disable, or configure CDP features globally on all ports or on specified ports.

set cdp {**enable** | **disable**} {*mod/ports...*}

set cdp interval *interval*

set cdp holdtime *holdtime*

set cdp version v1 | **v2**

set cdp format device-id {**mac-address** | **other**}

Syntax Description

enable	Keyword to enable the CDP feature.
disable	Keyword to disable the CDP feature.
mod/ports..	Number of the module and the ports on the module.
interval	Keyword to specify the CDP message interval value.
interval	Number of seconds the system waits before sending a message; valid values are from **5** to **900** seconds.
holdtime	Keyword to specify the global Time-To-Live value.
holdtime	Number of seconds for the global Time-To-Live value; valid values are from **10** to **255** seconds.
version v1 | **v2**	Keywords to specify the CDP version number.
format device-id	Keywords to set the device-ID TLV format.
mac-address	Keywords to specify that the device-ID TLV carry the MAC address of the sending device in ASCII, in canonical format.
other	Keyword to specify that the device's hardware serial number concatenated with the device name between parenthesis.

Defaults

The default system configuration has CDP enabled. The message interval is set to 60 seconds for every port; the default Time-To-Live value has the message interval globally set to 180 seconds. The default CDP version is version 2. The default device-id TLV format is **other**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set cdp version** command allows you to globally set the highest version number of CDP packets to send.

If you enter the global **set cdp enable** or **disable** command, CDP is globally configured. If CDP is globally disabled, CDP is automatically disabled on all interfaces, but the per-port **enable** (or **disable**) configuration is not changed. If you globally enable CDP, whether CDP is running on an interface or not depends on its per-port configuration.

If you configure CDP on a per-port basis, you can enter the *mod/port* as a single module and port or a range of ports; for example, 2/1-12,3/5-12.

The Device-Id TLV can carry two different formats of the device identifier for the sending device:

- **mac-address** format—The device-ID TLV is the MAC address of the sending device in ASCII, in canonical format.
- **other** format—The device identifier for the sending device is the device's hardware serial number concatenated with the device name between parenthesis.

Examples

This example shows how to enable the CDP message display for port 1 on module 2:

```
Console> (enable) set cdp enable 2/1
CDP enabled on port 2/1.
Console> (enable)
```

This example shows how to disable the CDP message display for port 1 on module 2:

```
Console> (enable) set cdp disable 2/1
CDP disabled on port 2/1.
Console> (enable)
```

This example shows how to specify the CDP message interval value:

```
Console> (enable) set cdp interval 400
CDP interval set to 400 seconds.
Console> (enable)
```

This example shows how to specify the global Time-To-Live value:

```
Console> (enable) set cdp holdtime 200
CDP holdtime set to 200 seconds.
Console> (enable)
```

This example shows how to set the device ID format to MAC address:

```
Console> (enable) set cdp format device-id mac-address
Device Id format changed to MAC-address
Console> (enable)
```

Related Commands

show cdp
show port cdp

set channelprotocol

Use the **set channelprotocol** command to set the protocol that manages channeling on a module.

set channelprotocol {**pagp** | **lacp**} *mod*

Syntax Description

pagp	Keyword to specify PAgP.
lacp	Keyword to specify LACP.
mod	Number of the module.

Defaults

The default for the channel protocol is PAgP.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

LACP is supported on all Ethernet interfaces.

PAgP and LACP manage channels differently. When all the ports in a channel get disabled, PAgP removes them from its internal channels list; **show** commands do not display the channel. With LACP, when all the ports in a channel get disabled, LACP does not remove the channel; **show** commands continue to display the channel even though all its ports are down. To determine if a channel is actively sending and receiving traffic with LACP, use the **show port** command to see if the link is up or down.

LACP does not support half-duplex links. If a port is in active/passive mode and becomes half duplex, the port is suspended (and a syslog message is generated). The port is shown as "connected" using the **show port** command and as "not connected" using the **show spantree** command. This discrepancy is because the port is physically connected but never joined spanning tree. To get the port to join spanning tree, either set the duplex to full or set the channel mode to off for that port.

For more information about PAgP and LACP, refer to the "Configuring EtherChannel" chapter of the *Catalyst 6000 Family Software Configuration Guide*.

Examples

This example shows how to set PAgP for module 3:

```
Console> (enable) set channelprotocol pagp 3
Channeling protocol set to PAGP for module(s) 3.
Console> (enable)
```

This example shows how to set LACP for modules 2, 4, 5, and 6:

```
Console> (enable) set channelprotocol lacp 2,4-6
Channeling protocol set to LACP for module(s) 2,4,5,6.
Console> (enable)
```

Related Commands

- clear lacp-channel statistics
- set lacp-channel system-priority
- set port lacp-channel
- set spantree channelcost
- set spantree channelvlancost
- show channelprotocol
- show lacp-channel

set channel vlancost

Use the **set channel vlancost** command to set the channel VLAN cost.

set channel vlancost *channel_id cost*

Syntax Description

channel_id	Number of the channel identification; valid values are from **769** to **896**.
cost	Port costs of the ports in the channel.

Defaults

The default is the VLAN cost is updated automatically based on the current port VLAN costs of the channeling ports.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you do not enter the *cost*, the cost is updated based on the current port VLAN costs of the channeling ports.

You can configure only one channel at a time.

Note The **set channel vlancost** command creates a "set spantree portvlancost" entry for each port in the channel. You must then manually reenter the **set spantree portvlancost** command for at least one port in the channel, specifying the VLAN or VLANs that you want associated with the port. When you associate the desired VLAN or VLANs with one port, all ports in the channel are automatically updated. Refer to Chapter 6, "Configuring EtherChannel," in the *Catalyst 6000 Family Software Configuration Guide* for more information.

Note With software releases 6.2(1) and earlier, the 6- and 9-slot Catalyst 6000 family switches support a maximum of 128 EtherChannels.

With software releases 6.2(2) and later, due to the port ID handling by the spanning tree feature, the maximum supported number of EtherChannels is 126 for a 6- or 9-slot chassis and 63 for a 13-slot chassis. Note that the 13-slot chassis was first supported in software release 6.2(2).

Examples

This example shows how to set the channel 769 path cost to 10:

```
Console> (enable) set channel vlancost 769 10
Port(s) 1/1-2 vlan cost are updated to 24.
Channel 769 vlancost is set to 10.
Console> (enable)
```

After you enter this command, you must reenter the **set spantree portvlancost** command so that the desired VLAN or VLANs are associated with all the channel ports.

This example shows how to associate the channel 769 path cost to 10 for VLAN 1 through VLAN 1005:

```
Console> (enable) set spantree portvlancost 1/1 cost 24 1-1005
Port 1/1 VLANs 1025-4094 have path cost 19.
Port 1/1 VLANs 1-1005 have path cost 24.
Port 1/2 VLANs 1-1005 have path cost 24.
Console> (enable)
```

Related Commands

set spantree portvlancost
show channel

set config acl nvram

Use the **set config acl nvram** command to copy the current committed ACL configuration from DRAM back into NVRAM.

set config acl nvram

Syntax Description

This command has no arguments or keywords.

Defaults

The default is NVRAM.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command fails if there is not enough space in NVRAM.

This command copies the current committed configuration to NVRAM; this configuration might be different from the configuration in the auto-config file. After the ACL configuration is copied into NVRAM, you must turn off the auto-config options using the **clear boot auto-config** command.

Examples

This example shows how to copy the ACL configuration to NVRAM:

```
Console> (enable) set config acl nvram
ACL configuration copied to NVRAM.
Console> (enable)
```

Related Commands

clear config
copy
set boot config-register
set boot system flash
show boot

set config mode

Use the **set config mode** command to change the configuration mode from a binary model to a text model.

set config mode binary

set config mode text {**nvram** | *device:file-id*}

Syntax Description

binary	Keyword to set the system configuration mode to a binary model.
text	Keyword to set the system configuration mode to a text model.
nvram	Keyword to specify the saved configuration be stored in NVRAM.
device:file-id	Name of the device and filename where the saved configuration will be stored.

Defaults

The default setting of this command is binary, saving the configuration to NVRAM.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to set the configuration mode to binary:

```
Console> (enable) set config mode binary
System configuration copied to NVRAM. Configuration mode set to binary.
Console> (enable)
```

This example shows how to set the configuration mode to text and designate the location and filename for saving the text configuration file:

```
Console> (enable) set config mode text bootflash:switch.cfg
Binary system configuration has been deleted from NVRAM. Configuration mode set to text.
Use the write memory command to save configuration changes. System configuration file set
to: bootflash:switch.cfg
The file specified will be used for configuration during the next bootup.
Console> (enable)
```

Related Commands

show config mode
write

set cops

Use the **set cops** command to configure COPS functionality.

set cops server *ipaddress* [*port*] [**primary**] [**diff-serv** | **rsvp**]

set cops domain-name *domain_name*

set cops retry-interval *initial incr max*

Syntax Description

server	Keyword to set the name of the COPS server.
ipaddress	IP address or IP alias of the server.
port	(Optional) Number of the TCP port the switch connects to on the server.
primary	(Optional) Keyword to specify the primary server.
diff-serv	(Optional) Keyword to set the COPS server for differentiated services.
rsvp	(Optional) Keyword to set the COPS server for RSVP+.
domain-name *domain_name*	Keyword and variable to specify the domain name of the switch.
retry-interval	Keyword to specify the retry interval in seconds.
initial	Initial timeout value; valid values are from **0** to **65535** seconds.
incr	Incremental value; valid values are from **0** to **65535** seconds.
max	Maximum timeout value; valid values are from **0** to **65535** seconds.

Defaults

The defaults are as follows:

- The retry interval default values are initial = 30 seconds, incr = 30 seconds, max = 5 minutes.
- The default domain-name is a string of length zero.
- No PDP servers are configured.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can configure the names or addresses of up to two PDP servers. One must be the primary, and the optional second server is a secondary, or backup, PDP server.

The COPS domain name can be set globally only; there is no option to set it for each COPS client.

Names such as the server, domain-name, and roles can contain a maximum of 31 characters; longer names are truncated to 31 characters. Valid letters are a-z, A-Z, 0-9, ., - and _. Names cannot start with an underscore (_). The names are not case sensitive for matching, but are case sensitive for display.

When specifying the **retry-interval**, the total of the initial timeout value and the incremental value (increment on each subsequent failure) may not exceed the maximum timeout value.

Examples

This example shows how to configure a server as a primary server:

```
Console> (enable) set cops server 171.21.34.56 primary
171.21.34.56 added to COPS server table as primary server.
Console> (enable)
```

This example shows how to configure a server as a primary RSVP+ server:

```
Console> (enable) set cops server 171.21.34.56 primary rsvp
171.21.34.56 added to COPS server table as primary server for RSVP.
Console> (enable)
```

This example shows how to configure a server as a secondary (or backup) server:

```
Console> (enable) set cops server my_server2
my_server2 added to the COPS server table as backup server.
Console> (enable)
```

This example shows how to set the domain name:

```
Console> (enable) set cops domain-name my_domain
Domain name set to my_domain.
Console> (enable)
```

This example shows how to set the retry interval:

```
Console> (enable) set cops retry-interval 15 1 30
Connection retry intervals set.
Console> (enable)
```

This example shows the display output if the total of the initial timeout value and the incremental value you entered exceeds the maximum timeout value:

```
Console> (enable) set cops retry-interval 15 1 10
The initial timeout plus the increment value may not exceed the max value.
Console> (enable)
```

Related Commands

clear cops
show cops

set crypto key rsa

Use the **set crypto key rsa** command to generate and configure an RSA key pair.

set crypto key rsa *nbits* [**force**]

Syntax Description

nbits	Size of the key; valid values are **512** to **2048** bits.
force	(Optional) Keyword to regenerate the keys and suppress the warning prompt of overwriting existing keys.

Defaults

The command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **crypto** commands are supported on systems that run these image types only:

- supk9 image—for example, cat6000-supk9.6-1-3.bin
- supcvk9 image—for example, cat6000-supcvk9.6-1-3.bin

If you do not enter the **force** keyword, the **set crypto key** command is saved into the config file and you will have to use the **clear config all** command to clear the RSA keys.

The *nbits* value is required.

To support SSH login, you first must generate an RSA key pair.

Examples

This example shows how to create an RSA key:

```
Console> (enable) set crypto key rsa 1024
Generating RSA keys.... [OK]
Console> (enable)
```

Related Commands

clear crypto key rsa
show crypto key

set default portstatus

Use the **set default portstatus** command to set the default port status.

set default portstatus {**enable** | **disable**}

Syntax Description

enable	Keyword to activate default port status.
disable	Keyword to deactivate default port status.

Defaults

The default is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you enter the **clear config all** command or in the event of a configuration loss, all ports collapse into VLAN 1. This might cause a security and network instability problem. Entering the **set default portstatus** command puts all ports into a disable state and blocks the traffic flowing through the ports during a configuration loss. You can then manually configure the ports back to the enable state.

This command is not saved in the configuration file.

After you set the default port status, the default port status does not clear when you enter the **clear config all** command.

Examples

This example shows how to disable the default port status:

```
Console> (enable) set default portstatus disable
 port status set to disable.
Console> (enable)
```

Related Commands

show default

set dot1q-all-tagged

Use the **set dot1q-all-tagged** command to change all existing and new dot1q trunks to the dot1q-only mode.

set dot1q-all-tagged enable | **disable** [**all**]

Syntax Description

enable	Keyword to enable dot1q-tagged-only mode.
disable	Keyword to disable dot1q-tagged-only mode.
all	(Optional) Keyword to specify dot1q tagging for all ports.

Defaults

The 802.1Q tagging feature is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you enable dot1q-tagged-only, all data packets are sent out tagged and all received untagged data packets are dropped on all 802.1Q trunks.

You cannot enable the dot1q tunneling feature on a port until dot1q-tagged-only mode is enabled.

You cannot disable dot1q-tagged-only mode on the switch until dot1q tunneling is disabled on all the ports on the switch.

The optional **all** keyword is not supported.

Note PBF does not work with 802.1Q tunnel traffic. PBF is supported on Layer 3 IP unicast traffic, but it is not applicable to Layer 2 traffic. At the intermediate (PBF) switch, all 802.1Q tunnel traffic appears as Layer 2 traffic.

Examples

This example shows how to enable dot1q tagging:

```
Console> (enable) set dot1q-all-tagged enable
Dot1q tagging is enabled
Console> (enable)
```

This example shows how to disable dot1q tagging:

```
Console> (enable) set dot1q-all-tagged disable
Dot1q tagging is disabled
Console> (enable)
```

Related Commands set port dot1qtunnel
show dot1q-all-tagged

set dot1x

Use the **set dot1x** command to configure dot1x on a system.

set dot1x system-auth-control {**enable** | **disable**}

set dot1x {**quiet-period** | **tx-period** | **re-authperiod**} *seconds*

set dot1x {**supp-timeout** | **server-timeout**} *seconds*

set dot1x max-req *count*

Syntax Description

system-auth-control	Keyword to specify authentication for the system.
enable	Keyword to enable the specified dot1x function.
disable	Keyword to disable the specified dot1x function.
quiet-period *seconds*	Keyword to specify the idle time between authentication attempts; valid values are from **0** to **65535** seconds.
tx-period *seconds*	Keyword to specify the time for the retransmission of EAP-Request/Identity frame; valid values are from **0** to **65535** seconds. See the "Usage Guidelines" section for additional information.
re-authperiod *seconds*	Keyword and variable to specify the time constant for the retransmission reauthentication time; valid values are from **1** to **65535** seconds.
supp-timeout *seconds*	Keyword and variable to specify the time constant for the retransmission of EAP-Request packets; valid values are from **0** to **65535** seconds. See the "Usage Guidelines" section for additional information.
server-timeout *seconds*	Keyword and variable to specify the time constant for the retransmission of packets by the backend authenticator to the authentication server; valid values are from **1** to **65535** seconds. See the "Usage Guidelines" section for additional information.
max-req *count*	Keyword and variable to specify the maximum number of times that the state machine retransmits an EAP-Request frame to the supplicant before it times out the authentication session; valid values are from **1** to **10**.

Defaults

The default settings are as follows:

- **system-auth-control** is enabled
- **quiet-period** is 60 seconds
- **tx-period** is 30 seconds
- **re-authperiod** is 3600 seconds
- **supp-timeout** is 30 seconds
- **server-timeout** is 30 seconds
- **max-req** count is 2

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you set the **system-auth-control**, the following applies:

- The **enable** keyword allows you to control each port's authorization status per the port-control parameter set using the **set port dot1x** command.
- The **disable** keyword allows you to make all ports behave as though the port-control parameter is set to **force-authorized**.

If you do not enable reauthentication, reauthentication does not automatically occur after authentication has occurred.

When the supplicant does not notify the authenticator that it received the EAP-request/identity packet, the authenticator waits a period of time (set by entering the **tx-period** *seconds* parameter), and then retransmits the packet.

When the supplicant does not notify the backend authenticator that it received the EAP-request packet, the backend authenticator waits a period of time (set by entering the **supp-timeout** *seconds* parameter), and then retransmits the packet.

When the authentication server does not notify the backend authenticator that it received specific packets, the backend authenticator waits a period of time (set by entering the **server-timeout** *seconds* parameter), and then retransmits the packets.

Examples

This example shows how to set the system authentication control:

```
Console> (enable) set dot1x system-auth-control enable
dot1x authorization enabled.
Console> (enable)
```

This example shows how to set the idle time between authentication attempts:

```
Console> (enable) set dot1x quiet-period 45
dot1x quiet-period set to 45 seconds.
Console> (enable)
```

This example shows how to set the retransmission time:

```
Console> (enable) set dot1x tx-period 15
dot1x tx-period set to 15 seconds.
Console> (enable)
```

This example shows you how to specify the reauthentication time:

```
Console> (enable) set dot1x re-authperiod 7200
dot1x re-authperiod set to 7200 seconds
Console> (enable)
```

This example shows you how to specify the retransmission of EAP-Request packets by the authenticator to the supplicant:

```
Console> (enable) set dot1x supp-timeout 15
dot1x supp-timeout set to 15 seconds.
Console> (enable)
```

This example shows how to specify the retransmission of packets by the backend authenticator to the authentication server:

```
Console> (enable) set dot1x server-timeout 15
dot1x server-timeout set to 15 seconds.
Console> (enable)
```

This example shows how to specify the maximum number of packet retransmissions:

```
Console> (enable) set dot1x max-req 5
dot1x max-req set to 5.
Console> (enable)
```

Related Commands

clear dot1x config
set port dot1x
show dot1x
show port dot1x

set enablepass

Use the **set enablepass** command to change the password for the privileged level of the CLI.

set enablepass

Syntax Description

This command has no arguments or keywords.

Defaults

The default configuration has no enable password configured.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Passwords are case sensitive and may be 0 to 19 characters in length, including spaces.

The command prompts you for the old password. If the password you enter is valid, you are prompted to enter a new password and to verify the new password.

Examples

This example shows how to establish a new password:

```
Console> (enable) set enablepass
Enter old password: <old_password>
Enter new password: <new_password>
Retype new password: <new_password>
Password changed.
Console> (enable)
```

Related Commands

enable
set password

set errdisable-timeout

Use the **set errdisable-timeout** command to configure a timeout to automatically reenable ports that are in the errdisable state.

set errdisable-timeout {**enable** | **disable**} {*reason*}

set errdisable-timeout interval {*interval*}

Syntax Description

enable	Keyword to enable errdisable timeout.
disable	Keyword to disable errdisable timeout.
reason	Reason for the port being in the errdisable state; valid values are **bpdu-guard**, **channel-misconfig**, **duplex-mismatch**, **udld**, **other**, and **all**.
interval *interval*	Timeout interval; valid values are from **30** to **86400** seconds (30 seconds to 24 hours).

Defaults

By default, all the errdisable state reasons are disabled globally; whenever there are no reasons enabled, the timer is stopped.

The default *interval* is 300 seconds.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The errdisable timeout feature allows you to configure a timeout period for ports in errdisable state. When this feature is enabled, ports are reenabled automatically after the timeout interval has elapsed.

A port enters errdisable state for the following reasons (these reasons appear as configuration options with the set errdisable-timeout enable command):

- Channel misconfiguration
- Duplex mismatch
- BPDU port-guard
- UDLD
- Other (reasons other than the above)
- All (apply errdisable timeout to all reasons)

You can enable or disable errdisable timeout for each of the above listed reasons. The ports in errdisable state for reasons other than the first four reasons are considered "other." If you specify **other**, all ports errdisabled by causes other than the first four reasons are enabled for errdisable timeout. If you specify "all," all ports errdisabled for any reason are enabled for errdisable timeout.

Examples

This example shows how to enable an errdisable timeout for BPDU guard causes:

```
Console> (enable) set errdisable-timeout enable bpdu-guard
Successfully enabled errdisable-timeout for bpdu-guard.
Console> (enable)
```

This example shows how to set an errdisable timeout interval to 450 seconds:

```
Console> (enable) set errdisable-timeout interval 450
Successfully set errdisable timeout to 450 seconds.
Console> (enable)
```

Related Commands

show errdisable-timeout

set errordetection

Use the **set errordetection** command to enable or disable various error detections.

set errordetection inband enable | **disable**

set errordetection memory enable | **disable**

set errordetection portcounters enable | **disable**

Syntax Description

inband	Keyword to detect errors in the inband (sc0) interface.
enable	Keyword to enable the specified error detection.
disable	Keyword to disable the specified error detection.
memory	Keyword to detect memory corruption.
portcounters	Keyword to monitor and poll port counters.

Defaults

The defaults are as follows:

- Inband error detection is disabled.
- Port counter error detection is disabled.
- Memory error detection is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set errordetection** command is useful for monitoring the switch. If an error is detected, a syslog message informs you that a problem exists before noticeable performance degradation occurs. For example:

- **set errordetection inband**—Displays the type of inband failure occurence, such as, inband stuck, resource errors, and inband fail during bootup.
- **set errordetection memory**—Displays the address where the memory corruption occurred.
- **set errordetection portcounters**—Displays the module and port number and the counter that had the problem between two consecutive polls.

Examples

This example shows how to enable memory error detection:

```
Console> (enable) set errordetection memory enable
Memory error detection enabled.
Console> (enable)
```

Related Commands show errordetection

set feature agg-link-partner

Use the **set feature agg-link-partner** command to enable or disable the aggressive link partner feature.

set feature agg-link-partner {**enable** | **disable**}

Syntax Description

enable	Keyword to enable the aggressive link partner feature.
disable	Keyword to disable the aggressive link partner feature.

Defaults

By default, the aggressive link partner feature is disabled globally.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When enabled, this feature reduces the likelihood of aggressive link partners causing excessive collisions, which can lead to excessive alignment errors and runts.

The aggressive link partner feature works only on half duplex 10/100 ports.

Because the **set feature agg-link-partner** command is global, enabling or disabling this feature does so for all related modules in the chassis.

Examples

This example shows how to enable the aggressive link partner feature:

```
Console> (enable) set feature agg-link-partner enable
Aggressive link partner feature enabled.
Console> (enable)
```

This example shows how to disable the aggressive link partner feature:

```
Console> (enable) set feature agg-link-partner disable
Aggressive link partner feature disabled.
Console> (enable)
```

set feature mdg

Use the **set feature mdg** command to enable or disable the multiple default gateway feature.

set feature mdg {**enable** | **disable**}

Syntax Description

enable	Keyword to enable the multiple default gateway.
disable	Keyword to disable the multiple default gateway.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you enable the multiple default gateway feature, the Catalyst 6000 family switch pings the default gateways every 10 seconds to verify the gateways are still available.

Examples

This example shows how to enable the multiple default gateway feature:

```
Console> (enable) set feature mdg enable
Multiple  Gateway feature enabled.
Console> (enable)
```

This example shows how to disable the multiple default gateway feature:

```
Console> (enable) set feature mdg disable
Multiple  Gateway feature disabled.
Console> (enable)
```

set garp timer

Use the **set garp timer** command to adjust the values of the join, leave, and leaveall timers.

set garp timer {*timer_type*} {*timer_value*}

Syntax Description

timer_type	Type of timer; valid values are **join**, **leave,** and **leaveall**.
timer_value	Timer values in milliseconds; valid values are from **1** to **2147483647** milliseconds.

Defaults

The default is the join timer default is 200 ms, the leave timer default is 600 ms, and the leaveall timer default is 10000 ms.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The modified timer values are applied to all GARP applications (for example, GMRP and GVRP) timer values.

You must maintain the following *relationship* for the various timer values:

- Leave time must be greater than or equal to three times the join time.
- Leaveall time must be greater than the leave time.

Caution Set the same GARP application (for example, GMRP and GVRP) timer values on all Layer 2-connected devices. If the GARP timers are set differently on the Layer 2-connected devices, GARP applications will not operate successfully.

Examples

This example shows how to set the join timer value to 100 ms for all the ports on all the VLANs:

```
Console> (enable) set garp timer join 100
GMRP/GARP Join timer value is set to 100 milliseconds.
Console> (enable)
```

This example shows how to set the leave timer value to 300 ms for all the ports on all the VLANs:

```
Console> (enable) set garp timer leave 300
GMRP/GARP Leave timer value is set to 300 milliseconds.
Console> (enable)
```

Related Commands

set gmrp timer
set gvrp timer
show garp timer

set gmrp

Use the **set gmrp** command to enable or disable GMRP on the switch in all VLANs on all ports.

set gmrp {**enable** | **disable**}

Syntax Description

enable	Keyword to enable GMRP on the switch.
disable	Keyword to disable GMRP on the switch.

Defaults

The default is GMRP is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You cannot enable GMRP if IGMP snooping is already enabled.

Examples

This example shows how to enable GMRP on the switch:

```
Console> (enable) set gmrp enable
GMRP is enabled.
Console> (enable)
```

This example shows how to disable GMRP on the switch:

```
Console> (enable) set gmrp disable
GMRP is disabled.
Console> (enable)
```

This example shows the display if you try to enable GMRP on the switch with IGMP enabled:

```
Console> (enable) set gmrp enable
Disable IGMP to enable GMRP snooping feature.
Console> (enable)
```

Related Commands

show gmrp configuration

set gmrp fwdall

Use the **set gmrp fwdall** command to enable or disable the Forward All feature on a specified port or module and port list.

set gmrp fwdall {**enable** | **disable**} *mod/port...*

Syntax Description

enable	Keyword to enable GMRP Forward All on a specified port.
disable	Keyword to disable GMRP Forward All on a specified port.
mod/port...	Number of the module and the ports on the module.

Defaults

The default is the Forward All feature is disabled for all ports.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Forward All indicates that a port is interested in receiving all the traffic for all the multicast groups.

If the port is trunking, then this feature is applied to all the VLANs on that port.

Examples

This example shows how to enable GMRP Forward All on module 5, port 5:

```
Console> (enable) set gmrp fwdall enable 5/5
GMRP Forward All groups option enabled on port(s) 5/5.
Console> (enable)
```

This example shows how to disable the GMRP Forward All on module 3, port 2:

```
Console> (enable) set gmrp service fwdall disable 3/2
GMRP Forward All groups option disabled on port(s) 3/2.
Console> (enable)
```

Related Commands

show gmrp configuration

set gmrp registration

Use the **set gmrp registration** command to specify the GMRP registration type.

set gmrp registration {**normal** | **fixed** | **forbidden**} *mod/port...*

Syntax Description

normal	Keyword to specify dynamic GMRP multicast registration and deregistration on the port.
fixed	Keyword to specify the multicast groups currently registered on the switch are applied to the port, but any subsequent registrations or deregistrations do not affect the port. Any registered multicast groups on the port are not deregistered based on the GARP timers.
forbidden	Keyword to specify that all GMRP multicasts are deregistered and prevent any further GMRP multicast registration on the port.
mod/port...	Number of the module and the ports on the module.

Defaults

The default is administrative control is normal.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You must return the port to **normal** registration mode to deregister multicast groups on the port.

GMRP supports a total of 3072 multicast addresses for the whole switch.

Examples

This example shows how to set the registration type to **fixed** on module 3, port 3:

```
Console> (enable) set gmrp registration fixed 3/3
GMRP Registration is set to Fixed for port(s) 3/3.
Console> (enable)
```

This example shows how to set the registration type to **forbidden** on module 1, port 1:

```
Console> (enable) set gmrp registration forbidden 1/1
GMRP Registration is set to Forbidden for port(s) 1/1.
Console> (enable)
```

Related Commands

show gmrp configuration

set gmrp timer

Use the **set gmrp timer** command to adjust the values of the join, leave, and leaveall timers.

set gmrp timer {*timer_type*} {*timer_value*}

Syntax Description

timer_type	Type of timer; valid values are **join**, **leave,** and **leaveall**.
timer_value	Timer values in milliseconds; valid values are from **1** to **2147483647** milliseconds.

Defaults

The default is the join timer is 200 milliseconds, the leave timer is 600 milliseconds, and the leaveall timer is 10000 milliseconds.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You must maintain the following *relationship* for the various timer values:

- Leave time must be greater than or equal to three times the join time.
- Leaveall time must be greater than the leave time.

Caution Set the same GARP application (for example, GMRP and GVRP) timer values on all Layer 2-connected devices. If the GARP timers are set differently on the Layer 2-connected devices, GARP applications will not operate successfully.

Note The modified timer values are applied to all GARP application (for example, GMRP and GVRP) timer values.

Examples

This example shows how to set the join timer value to 100 milliseconds for all the ports on all the VLANs:

```
Console> (enable) set gmrp timer join 100
GARP Join timer value is set to 100 milliseconds.
Console> (enable)
```

This example shows how to set the leave timer value to 300 milliseconds for all the ports on all the VLANs:

```
Console> (enable) set gmrp timer leave 300
GARP Leave timer value is set to 300 milliseconds.
Console> (enable)
```

This example shows how to set the leaveall timer value to 20000 milliseconds for all the ports on all the VLANs:

```
Console> (enable) set gmrp timer leaveall 20000
GARP LeaveAll timer value is set to 20000 milliseconds.
Console> (enable)
```

Related Commands

set garp timer
set gvrp timer
show gmrp timer

set gvrp

Use the **set gvrp** command to enable or disable GVRP globally in the switch or on a per-port basis.

set gvrp {**enable** | **disable**} [*mod/port*]

Syntax Description

enable	Keyword to enable GVRP on the switch.
disable	Keyword to disable GVRP on the switch.
mod/port	(Optional) Number of the module and port on the module.

Defaults

The default is GVRP is globally set to disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you enable VTP pruning, VTP pruning runs on all the GVRP-disabled trunks.

To run GVRP on a trunk, you need to enable GVRP both globally on the switch and individually on the trunk.

Examples

This example shows how to enable GVRP globally on the switch:

```
Console> (enable) set gvrp enable
GVRP enabled.
Console> (enable)
```

This example shows how to disable GVRP:

```
Console> (enable) set gvrp disable
GVRP disabled.
Console> (enable)
```

This example shows how to enable GVRP on module 2, port 1:

```
Console> (enable) set gvrp enable 2/1
GVRP enabled on port 2/1.
Console> (enable)
```

Related Commands

set garp timer
set gvrp timer
show gmrp timer
show gvrp configuration

set gvrp applicant

Use the **set gvrp applicant** command to specify whether or not a VLAN is declared out of blocking ports.

set gvrp applicant {**normal** | **active**} {*mod/port...*}

Syntax Description

normal	Keyword to disallow the declaration of any VLAN out of blocking ports.
active	Keyword to enforce the declaration of all active VLANs out of blocking ports.
mod/port..	Number of the module and the ports on the module.

Defaults

The default is GVRP applicant set to normal.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

To run GVRP on a trunk, you need to enable GVRP both globally on the switch and individually on the trunk.

On a port connected to a device that does not support the per-VLAN mode of STP, the port state may continuously cycle from blocking to listening to learning, and back to blocking. To prevent this, you must enter the **set gvrp applicant active** *mod/port...* command on the port to send GVRP VLAN declarations when the port is in the STP blocking state.

Examples

This example shows how to enforce the declaration of all active VLANs out of specified blocking ports:

```
Console> (enable) set gvrp applicant active 4/2-3,4/9-10,4/12-24
Applicant was set to active on port(s) 4/2-3,4/9-10,4/12-24.
Console> (enable)
```

This example shows how to disallow the declaration of any VLAN out of specified blocking ports:

```
Console> (enable) set gvrp applicant normal 4/2-3,4/9-10,4/12-24
Applicant was set to normal on port(s) 4/2-3,4/9-10,4/12-24.
Console> (enable)
```

Related Commands

show gvrp configuration

set gvrp dynamic-vlan-creation

Use the **set gvrp dynamic-vlan-creation** command to enable or disable dynamic VLAN creation.

set gvrp dynamic-vlan-creation {**enable** | **disable**}

Syntax Description

enable	Keyword to enable dynamic VLAN creation.
disable	Keyword to disable dynamic VLAN creation.

Defaults

The default is dynamic VLAN creation is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can enable dynamic VLAN creation only when VTP is in transparent mode and no ISL trunks exist in the switch.

This feature is not allowed when there are 802.1Q trunks that are not configured with GVRP.

Examples

This example shows how to enable dynamic VLAN creation:

```
Console> (enable) set gvrp dynamic-vlan-creation enable
Dynamic VLAN creation enabled.
Console> (enable)
```

This example shows what happens if you try to enable dynamic VLAN creation and VTP is not in transparent mode:

```
Console> (enable) set gvrp dynamic-vlan-creation enable
VTP has to be in TRANSPARENT mode to enable this feature.
Console> (enable)
```

This example shows how to disable dynamic VLAN creation:

```
Console> (enable) set gvrp dynamic-vlan-creation disable
Dynamic VLAN creation disabled.
Console> (enable)
```

Related Commands

set vtp
show gvrp configuration

set gvrp registration

Use the **set gvrp registration** command to set the administrative control of an outbound port and apply to all VLANs on the trunk. GVRP registration commands are entered on a per-port basis.

set gvrp registration {**normal** | **fixed** | **forbidden**} *mod/port...*

Syntax Description

normal	Keyword to allow dynamic registering and deregistering each VLAN (except VLAN 1) on the port.
fixed	Keyword to support manual VLAN creation and registration, prevent VLAN deregistration, and register all VLANs known to other ports.
forbidden	Keyword to specify that all the VLANs (except VLAN 1) are statically deregistered from the port.
mod/port...	Number of the module and the ports on the module.

Defaults

The default administrative control is normal.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you set VLAN registration, you are communicating to the switch that the VLAN is interested in the users that are connecting to this port and that the VLAN's broadcast and multicast traffic is allowed to be sent to the port.

For static VLAN configuration, you should set the *mod/port...* control to **fixed** or **forbidden** if the *mod/port...* will not receive or process any GVRP message.

For each dynamically configured VLAN on a port, you should set the *mod/port...* control to **normal** (default), except for VLAN 1; GVRP registration mode for VLAN 1 is always fixed and is not configurable. VLAN 1 is always carried by 802.1Q trunks on which GVRP is enabled.

When GVRP is running, you can create a VLAN through a GVRP trunk port only if you enter the **set gvrp dynamic-vlan-creation enable** and the **set gvrp registration normal** commands.

Examples

This example shows how to set the administrative control to **normal** on module 3, port 7:

```
Console> (enable) set gvrp registration normal 3/7
Registrar Administrative Control set to normal on port 3/7.
Console> (enable)
```

This example shows how to set the administrative control to **fixed** on module 5, port 10:

```
Console> (enable) set gvrp registration fixed 5/10
Registrar Administrative Control set to fixed on Port 5/10.
Console> (enable)
```

This example shows how to set the administrative control to **forbidden** on module 5, port 2:

```
Console> (enable) set gvrp registration forbidden 5/2
Registrar Administrative Control set to forbidden on port 5/2.
Console> (enable)
```

Related Commands **show gvrp configuration**

set gvrp timer

Use the **set gvrp timer** command to adjust the values of the join, leave, and leaveall timers.

set gvrp timer {*timer_type*} {*timer_value*}

Syntax Description

timer_type	Type of timer; valid values are **join**, **leave,** and **leaveall**.
timer_value	Timer values in milliseconds; valid values are from **1** to **2147483647** milliseconds.

Defaults

The default is the join timer is 200 milliseconds, the leave timer is 600 milliseconds, and the leaveall timer is 10000 milliseconds.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You must maintain the following *relationship* for the various timer values:

- Leave time must be greater than or equal to three times the join time.
- Leaveall time must be greater than the leave time.

Caution Set the same GARP application (for example, GMRP and GVRP) timer values on all Layer 2-connected devices. If the GARP timers are set differently on the Layer 2-connected devices, GARP applications will not operate successfully.

Note The modified timer values are applied to all GARP application (for example, GMRP and GVRP) timer values.

Examples

This example shows how to set the join timer value to 100 milliseconds for all the ports on all the VLANs:

```
Console> (enable) set gvrp timer join 100
GVRP/GARP Join timer value is set to 100 milliseconds.
Console> (enable)
```

This example shows how to set the leave timer value to 300 milliseconds for all the ports on all the VLANs:

```
Console> (enable) set gvrp timer leave 300
GVRP/GARP Leave timer value is set to 300 milliseconds.
Console> (enable)
```

This example shows how to set the leaveall timer value to 20000 milliseconds for all the ports on all the VLANs:

```
Console> (enable) set gvrp timer leaveall 20000
GVRP/GARP LeaveAll timer value is set to 20000 milliseconds.
Console> (enable)
```

Related Commands

set garp timer
show gvrp configuration

set igmp

Use the **set igmp** command to enable or disable IGMP snooping on the switch.

set igmp {**enable** | **disable**}

Syntax Description

enable	Keyword to enable IGMP snooping on the switch.
disable	Keyword to disable IGMP snooping on the switch.

Defaults

The default is IGMP snooping is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

IGMP must be disabled to run GMRP.

If your system is configured with a Supervisor Engine 1, you must enable one of the multicast services (IGMP snooping or GMRP) on the switch in order to use IP MMLS.

Examples

This example shows how to enable IGMP snooping on the switch:

```
Console> (enable) set igmp enable
IGMP feature for IP multicast enabled
Console> (enable)
```

This example shows how to disable IGMP snooping on the switch:

```
Console> (enable) set igmp disable
IGMP Snooping is disabled.
Console> (enable)
```

This example shows the display if you try to enable GMRP on the switch with IGMP enabled:

```
Console> (enable) set igmp enable
Disable GMRP to enable IGMP snooping feature.
Console> (enable)
```

Related Commands

clear igmp statistics
set rgmp
show igmp statistics

set igmp fastleave

Use the **set igmp fastleave** command to enable or disable IGMP fastleave processing.

set igmp fastleave {**enable** | **disable**}

Syntax Description

enable	Keyword to enable IGMP fastleave processing.
disable	Keyword to disable IGMP fastleave processing.

Defaults

The default is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This command shows how to enable IGMP fastleave processing:

```
Console> (enable) set igmp fastleave enable
IGMP fastleave set to enable.
Warning: Can cause disconnectivity if there are more than one host joining the same group
per access port.
Console> (enable)
```

This command shows how to disable IGMP fastleave processing:

```
Console> (enable) set igmp fastleave disable
IGMP fastleave set to disable.
Console> (enable)
```

Related Commands

clear igmp statistics
set igmp
show igmp statistics

set igmp mode

Use the **set igmp mode** command to set the IGMP snooping mode.

set igmp mode {**igmp-only** | **igmp-cgmp** | **auto**}

Syntax Description

igmp-only	Keyword to specify IGMP snooping only.
igmp-cgmp	Keyword to specify IGMP and CGMP modes.
auto	Keyword to override the dynamic switching of IGMP snooping modes.

Defaults

The default is IGMP mode is **auto**.

Command Types

Switch.

Command Modes

Privileged.

Usage Guidelines

The switch dynamically chooses either IGMP-only or IGMP-CGMP mode, depending on the traffic present on the network. IGMP-only mode is used in networks with no CGMP devices. IGMP-CGMP mode is used in networks with both IGMP and CGMP devices. Auto mode overrides the dynamic switching of the modes.

Examples

This example shows how to set the IGMP mode to IGMP-only:

```
Console> (enable) set igmp mode igmp-only
IGMP mode set to igmp-only
Console> (enable)
```

This example shows how to set the IGMP mode to auto:

```
Console> (enable) set igmp mode auto
IGMP mode set to auto
Console> (enable)
```

Related Commands

show igmp mode

set igmp querier

Use the **set igmp querier** command to configure the IGMP querier for a specific VLAN.

set igmp querier {**enable** | **disable**} *vlan*

set igmp querier *vlan* {**qi** | **oqi**} *seconds*

Syntax Description

enable	Keyword to enable the IGMP querier for a VLAN.
disable	Keyword to disable the IGMP querier for a VLAN.
vlan	Number of the VLAN.
qi	Keyword to set the querier interval for the VLAN. See the "Usage Guidelines" section for more information about the querier interval.
oqi	Keyword to set the other querier interval for the VLAN. See the "Usage Guidelines" section for more information about the other querier interval.
seconds	Range of the querier interval or the other querier interval in seconds; valid values are from 1 to 1000 seconds.

Defaults

IGMP querier is disabled.

The default value for **qi** is 125 seconds.

The default value for **oqi** is 300 seconds.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You must enable IGMP querier on every VLAN for which switch querier functionality is required.

In the absence of general queries, the **oqi** value is the amount of time a switch waits before electing itself as the querier.

Examples

This example shows how to enable the IGMP querier for VLAN 4001:

```
Console> (enable) set igmp querier enable 4001
Console> (enable)
```

This example shows how to set the querier interval to 130 seconds for VLAN 4001:

```
Console> (enable) set igmp querier 4001 qi 130
Console> (enable)
```

set igmp ratelimit

Use the **set igmp ratelimit** command to enable or disable IGMP rate limiting or to set the rate limit for IGMP snooping packets.

set igmp ratelimit {**enable** | **disable**}

set igmp ratelimit {**dvmrp** | **general-query** | **mospf1** | **mospf2** | **pimv2**} *rate*

Syntax Description

enable	Enables IGMP rate limiting.
disable	Disables IGMP rate limiting.
dvmrp	Sets the IGMP rate limit for Distance Vector Multicast Routing Protocol (DVMRP) packets.
general-query	Sets the IGMP rate limit for general query packets.
mospf1	Sets the IGMP rate limit for Multicast Extensions of OSPF (MOSPF) version 1 packets.
mospf2	Sets the IGMP rate limit for Multicast Extensions of OSPF (MOSPF) version 2 packets.
pimv2	Sets the IGMP rate limit for Protocol Independent Multicast (PIM) version 2 packets.
rate	Rate limit; valid values are from 1 to 65535 packets per 30 seconds.

Defaults

IGMP rate limiting is disabled.

The default rate limits are as follows:

- **dvmrp** is 100 packets.
- **general-query** is 100 packets.
- **mospf1** is 100 packets.
- **mospf2** is 100 packets.
- **pimv2** is 100 packets.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set igmp ratelimit** {**enable** | **disable**} command is supported in both text and binary configuration modes.

If IGMP rate limiting and multicast are enabled, multicast router ports might age out sporadically because the rate of the multicast control packets (such as PIMv2 hellos or IGMP general queries) exceeds the IGMP rate limit watermarks that were configured. The default value for these watermarks is 100. We recommend that you increase the PIMv2 hello ratelimit to 3000 by entering **set igmp ratelimit pimv2 3000**. You can also increase the IGMP general queries rate limit; we recommend that you set the value to 500 by entering **set igmp ratelimit general-query 500**.

Examples

This example shows how to enable IGMP rate limiting:

```
Console> (enable) set igmp ratelimit enable
IGMP Ratelimiting enabled
Console> (enable)
```

This example shows how to set the IGMP rate limit for MOSPF2 to 550 packets per every 30 seconds:

```
Console> (enable) set igmp ratelimit mospf2 550
MOSPF2 Watermark set to allow 550 messages in 30 seconds
Console> (enable)
```

This example shows how to set the IGMP ratel limit for PIMv2 1000 packets per every 30 seconds:

```
Console> (enable) set igmp ratelimit pimv2 1000
PIMV2 Watermark set to allow 1000 messages in 30 seconds
Console> (enable)
```

Related Commands

show igmp ratelimit-info

set inlinepower defaultallocation

Use the **set inlinepower defaultallocation** command to set the default power allocation for a port.

set inlinepower defaultallocation *value*

Syntax Description

value	Default power allocation; valid values are from **2000** to **12500** mW.

Defaults

The default is 10000 mW.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to set the default power allocation to 2000 mW:

```
Console> (enable) set inlinepower defaultallocation 2000
Default inline power allocation set to 9500 mWatt per applicable port.
Console> (enable)
```

Related Commands

set port inlinepower
show environment
show port inlinepower

set interface

Use the **set interface** command to configure the in-band and SLIP interfaces on the switch.

set interface {**sc0** | **sl0**} {**up** | **down**}

set interface sl0 *slip_addr dest_addr*

set interface sc0 [*vlan*] [*ip_addr*[*netmask* [*broadcast*]]]

set interface sc0 [*vlan*] [*ip_addr/netmask* [*broadcast*]]

set interface sc0 dchp {**renew** | **release**}

Syntax Description

sc0	Keyword to specify the in-band interface.
sl0	Keyword to specify the SLIP interface.
up	Keyword to bring the interface into operation.
down	Keyword to bring the interface out of operation.
slip_addr	IP address of the console port.
dest_addr	IP address of the host to which the console port will be connected.
vlan	(Optional) Number of the VLAN to be assigned to the interface; valid values are from **1** to **1005** and from **1025** to **4094**.
ip_addr	(Optional) IP address.
/netmask	(Optional) Subnet mask.
broadcast	(Optional) Broadcast address.
dhcp	Keyword to perform DHCP operations on the sc0 interface.
renew	Keyword to renew the lease on a DHCP-learned IP address.
release	Keyword to release a DHCP-learned IP address back to the DHCP IP address pool.

Defaults

The default configuration is the in-band interface (sc0) in VLAN 1 with the IP address, subnet mask, and broadcast address set to 0.0.0.0. The default configuration for the SLIP interface (sl0) is that the IP address and broadcast address are set to 0.0.0.0.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set interface sc0 dchp** command is valid only when the address is learned from the DHCP server and available in privileged mode only.

Two configurable network interfaces are on a Catalyst 6000 family switch: in-band (sc0) and SLIP (sl0). Configuring the sc0 interface with an IP address and subnet mask allows you to access the switch CLI via Telnet from a remote host. You should assign the sc0 interface to an active VLAN configured on the switch (the default is VLAN 1). Make sure the IP address you assign is in the same subnet as other stations in that VLAN.

Configuring the sl0 interface with an IP address and destination address allows you to make a point-to-point connection to a host through the console port. Use the **slip attach** command to activate SLIP on the console port (you will not be able to access the CLI via a terminal connected to the console port until you use the **slip detach** command to deactivate SLIP on the console port).

When you specify the *netmask*, this indicates the number of bits allocated to subnetting in the hostid section of the given Class A, B, or C address. For example, if you enter an IP address for the sc0 interface as 172.22.20.7, the hostid bits for this Class B address is 16.

If you enter *netmask* in length of bits, for example, 204.20.22.7/24, the range for length is from 0 to 31 bits. If you do not enter the netmask, the number of bits is assumed to be the natural netmask.

Examples

This example shows how to use **set interface sc0** and **set interface sl0** from the console port. It also shows how to bring down **interface sc0** using a terminal connected to the console port:

```
Console> (enable) set interface sc0 192.20.11.44/255.255.255.0
Interface sc0 IP address and netmask set.
Console> (enable) set interface sl0 192.200.10.45 192.200.10.103
Interface sl0 SLIP and destination address set.
Console> (enable) set interface sc0 down
Interface sc0 administratively down.
Console> (enable)
```

This example shows how to set the IP address for sc0 through a Telnet session. Note that the default netmask for that IP address class is used (for example, a Class C address uses 255.255.255.0, and a Class B uses 255.255.0.0):

```
Console> (enable) set interface sc0 192.200.11.40
This command may disconnect active telnet sessions.
Do you want to continue (y/n) [n]? y
Interface sc0 IP address set.
```

This example shows how to take the interface out of operation through a Telnet session:

```
Console> (enable) set interface sc0 down
This command will inactivate telnet sessions.
Do you want to continue (y/n) [n]? y
Interface sc0 administratively down.
```

This example shows how to assign the sc0 interface to a particular VLAN:

```
Console> (enable) set interface sc0 5
Interface sc0 vlan set.
Console> (enable)
```

This example shows what happens when you assign the sc0 interface to a nonactive VLAN:

```
Console> (enable) set interface sc0 200
Vlan is not active, user needs to set vlan 200 active
Interface sc0 vlan set.
Console> (enable)
```

This example shows how to release a DHCP-learned IP address back to the DHCP IP address pool:

```
Console> (enable) set interface sc0 dhcp release
Releasing IP address...Done
Console> (enable)
```

This example shows how to renew a lease on a DHCP-learned IP address:

```
Console> (enable) set interface sc0 dhcp renew
Renewing IP address...Done
Console> (enable)
```

Related Commands

show interface
slip

set ip alias

Use the **set ip alias** command to add aliases of IP addresses.

set ip alias *name ip_addr*

Syntax Description

name	Name of the alias being defined.
ip_addr	IP address of the alias being defined.

Defaults

The default configuration is one IP alias (0.0.0.0) configured as the default.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to define an IP alias of mercury for IP address 192.122.174.234:

```
Console> (enable) set ip alias mercury 192.122.174.234
IP alias added.
Console> (enable)
```

Related Commands

clear ip alias
show ip alias

set ip dns

Use the **set ip dns** command to enable or disable DNS.

set ip dns {**enable** | **disable**}

Syntax Description

enable	Keyword to enable DNS.
disable	Keyword to disable DNS.

Defaults

The default is DNS is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to enable DNS:

```
Console> (enable) set ip dns enable
DNS is enabled.
Console> (enable)
```

This example shows how to disable DNS:

```
Console> (enable) set ip dns disable
DNS is disabled.
Console> (enable)
```

Related Commands

show ip dns

set ip dns domain

Use the **set ip dns domain** command to set the default DNS domain name.

set ip dns domain *name*

Syntax Description

name	DNS domain name.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you specify a domain name on the command line, the system attempts to resolve the host name as entered. If the system cannot resolve the host name as entered, it appends the default DNS domain name as defined with the **set ip dns domain** command. If you specify a domain name with a trailing dot, the program considers this an *absolute* domain name.

Examples

This example shows how to set the default DNS domain name:

```
Console> (enable) set ip dns domain yow.com
 DNS domain name set to yow.com.
Console> (enable)
```

Related Commands

clear ip dns domain
show ip dns

set ip dns server

Use the **set ip dns server** command to set the IP address of a DNS server.

set ip dns server *ip_addr* [**primary**]

Syntax Description

ip_addr	IP address of the DNS server.
primary	(Optional) Keyword to configure a DNS server as the primary server.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can configure up to three DNS name servers as backup. You can also configure any DNS server as the primary server. The primary server is queried first. If the primary server fails, the backup servers are queried.

If DNS is disabled, you must use the IP address with all commands that require explicit IP addresses or manually define an alias for that address. The alias has priority over DNS.

Examples

These examples show how to set the IP address of a DNS server:

```
Console> (enable) set ip dns server 198.92.30.32
198.92.30.32 added to DNS server table as primary server.

Console> (enable) set ip dns server 171.69.2.132 primary
171.69.2.132 added to DNS server table as primary server.

Console> (enable) set ip dns server 171.69.2.143 primary
171.69.2.143 added to DNS server table as primary server.
```

This example shows what happens if you enter more than three DNS name servers as backup:

```
Console> (enable) set ip dns server 161.44.128.70
DNS server table is full. 161.44.128.70 not added to DNS server table.
```

Related Commands

clear ip dns server
show ip dns

set ip fragmentation

Use the **set ip fragmentation** command to enable or disable the fragmentation of IP packets bridged between FDDI and Ethernet networks.

set ip fragmentation {**enable** | **disable**}

Syntax Description

enable	Keyword to permit fragmentation for IP packets bridged between FDDI and Ethernet networks.
disable	Keyword to disable fragmentation for IP packets bridged between FDDI and Ethernet networks.

Defaults

The default value is IP fragmentation is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If IP fragmentation is disabled, packets are dropped.

Note that FDDI and Ethernet networks have different MTUs.

Examples

This example shows how to disable IP fragmentation:

```
Console> (enable) set ip fragmentation disable
Bridge IP fragmentation disabled.
Console> (enable)
```

Related Commands

show ip route

set ip http port

Use the **set ip http port** command to configure the TCP port number for the HTTP server.

set ip http port {**default** | *port-number*}

Syntax Description

default	Keyword to specify the default HTTP server port number (80).
port-number	Number of the TCP port for the HTTP server; valid values are from **1** to **65535**.

Defaults

The default TCP port number is 80.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to set the IP HTTP port default:

```
Console> (enable) set ip http port default
HTTP TCP port number is set to 80.
Console> (enable)
```

This example shows how to set the IP HTTP port number:

```
Console> (enable) set ip http port 2398
HTTP TCP port number is set to 2398.
Console> (enable)
```

Related Commands

set ip http server
show ip http

set ip http server

Use the **set ip http server** command to enable or disable the HTTP server.

set ip http server {**enable** | **disable**}

Syntax Description

enable	Keyword to enable the HTTP server.
disable	Keyword to disable the HTTP server.

Defaults

The default is the HTTP server is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to enable the HTTP server:

```
Console> (enable) set ip http server enable
HTTP server is enabled.
Console> (enable)
```

This example shows the system response when the HTTP server-enabled command is not supported:

```
Console> (enable) set ip http server enable
Feature not supported.
Console> (enable)
```

This example shows how to disable the HTTP server:

```
Console> (enable) set ip http server disable
HTTP server disabled.
Console> (enable)
```

Related Commands

set ip http port
show ip http

set ip permit

Use the **set ip permit** command to enable or disable the IP permit list and to specify IP addresses to be added to the IP permit list.

set ip permit {**enable** | **disable**}

set ip permit {**enable** | **disable**} [**telnet** | **ssh** | **snmp**]

set ip permit *addr* [*mask*] [**telnet** | **ssh** | **snmp** | **all**]

Syntax Description

enable	Keyword to enable the IP permit list.
disable	Keyword to disable the IP permit list.
telnet	(Optional) Keyword to specify the Telnet IP permit list.
ssh	(Optional) Keyword to specify the SSH IP permit list.
snmp	(Optional) Keyword to specify the SNMP IP permit list.
addr	IP address to be added to the IP permit list. An IP alias or host name that can be resolved through DNS can also be used.
mask	(Optional) Subnet mask of the specified IP address.
all	(Optional) Keyword to specify all entries in the IP permit list be removed.

Defaults

The default is IP permit list is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The same functionality of the IP permit list can be achieved by using VACLs. VACLs are handled by hardware (PFC) and the processing is considerably faster. For VACL configuration information, refer to the *Catalyst 6000 Family Software Configuration Guide*.

You can configure up to 100 entries in the permit list. If you enable the IP permit list, but the permit list has no entries configured, a caution displays on the screen.

Make sure you enter the entire **disable** keyword when entering the **set ip permit disable** command. If you abbreviate the keyword, the abbreviation is interpreted as a host name to add to the IP permit list.

If you do not specify the **snmp**, **ssh**, **telnet**, or **all** keyword, the IP address is added to both the SNMP and Telnet permit lists.

You enter the mask in dotted decimal format, for example, 255.255.0.0.

Examples

This example shows how to add an IP address to the IP permit list:

```
Console> (enable) set ip permit 192.168.255.255
192.168.255.255 added to IP permit list.
Console> (enable)
```

This example shows how to add an IP address using an IP alias or host name to both the SNMP and Telnet permit lists:

```
Console> (enable) set ip permit batboy
batboy added to IP permit list.
Console> (enable)
```

This example shows how to add a subnet mask of the IP address to both the SNMP and Telnet permit lists:

```
Console> (enable) set ip permit 192.168.255.255 255.255.192.0
192.168.255.255 with mask 255.255.192.0 added to IP permit list.
Console> (enable)
```

This example shows how to add an IP address to the Telnet IP permit list:

```
Console> (enable) set ip permit 172.16.0.0 255.255.0.0 telnet
172.16.0.0 with mask 255.255.0.0 added to telnet permit list.
Console> (enable)
```

This example shows how to add an IP address to the SNMP IP permit list:

```
Console> (enable) set ip permit 172.20.52.32 255.255.255.224 snmp
172.20.52.32 with mask 255.255.255.224 added to snmp permit list.
Console> (enable)
```

This example shows how to add an IP address to all IP permit lists:

```
Console> (enable) set ip permit 172.20.52.3 all
172.20.52.3 added to IP permit list.
Console> (enable)
```

This example shows how to enable the IP permit list:

```
Console> (enable) set ip permit enable
Telnet, Snmp and Ssh permit list enabled
Console> (enable)
```

This example shows how to disable the IP permit list:

```
Console> (enable) set ip permit disable
Telnet, Snmp and Ssh permit list disabled.
Console> (enable)
```

This example shows how to enable a specific IP permit list type:

```
Console> (enable) set ip permit enable ssh
SSH permit list enabled.
Console> (enable)
```

Related Commands

clear ip permit
show ip permit

set ip redirect

Use the **set ip redirect** command to enable or disable ICMP redirect messages on the Catalyst 6000 family switches.

set ip redirect {**enable** | **disable**}

Syntax Description

enable	Keyword to permit ICMP redirect messages to be returned to the source host.
disable	Keyword to prevent ICMP redirect messages from being returned to the source host.

Defaults

The default configuration is ICMP redirect is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to deactivate ICMP redirect messages:

```
Console> (enable) set ip redirect disable
ICMP redirect messages disabled.
Console> (enable)
```

Related Commands

show ip route
show netstat

set ip route

Use the **set ip route** command to add IP addresses or aliases to the IP routing table.

set ip route {*destination*}[/*netmask*] {*gateway*} [*metric*] [**primary**]

Syntax Description

destination	IP address, IP alias of the network, or specific host to be added. Use **default** as the destination to set the new entry as the default route.
/netmask	(Optional) Number of bits in netmask or dot format (for example, 172.20.22.7/24 or 172.20.22.7/255.255.255.0).
gateway	IP address or IP alias of the router.
metric	(Optional) Value used to indicate the number of hops between the switch and the gateway.
primary	(Optional) Keyword used with the Multiple IP Gateways feature to specify the default IP gateway with the highest priority.

Defaults

The default configuration routes the local network through the sc0 interface with metric 0 as soon as sc0 is configured.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can configure up to three default gateways. The **primary** is the highest priority. If you do not designate a primary gateway, priority is based on the order of input. If you enter two primary definitions, the second definition becomes the primary and the first definition is now the secondary default IP gateway.

You can only specify the **primary** keyword for a default route.

When you enter the *destination* or *gateway*, enter it in dot notation, for example, a.b.c.d.

When you specify the *netmask*, this indicates the number of bits allocated to subnetting in the hostid section of the given Class A, B, or C address. For example, if you enter an IP address for the sc0 interface as 172.22.20.7, the hostid bits for this Class B address is 16. Any number of bits in the hostid bits can be allocated to the netmask field. If you do not enter the *netmask*, the number of bits is assumed to be the natural netmask.

When you enter the netmask, enter it as the number of bits or dot format, for example, **destination/24** or **destination/255.255.255.0**. If you enter the netmask in dot format, you must have contiguous 1s.

Examples

These examples show how to add three default routes to the IP routing table, checking after each addition using the **show ip route** command:

```
Console> (enable) set ip route default 192.122.173.42 1 primary
Route added.
Console> (enable)

Console> (enable) show ip route
Fragmentation   Redirect   Unreachable
-------------   --------   -----------
enabled         enabled    enabled
Destination     Gateway         Flags   Use         Interface
--------------- --------------- ------  ----------  ---------
default         192.122.173.42   UG           59444  sc0
192.22.74.0     192.22.74.223    U                5  sc0
Console> (enable)
Console> (enable) set ip route default 192.122.173.43 1
Route added.
Console> (enable)

Console> (enable) show ip route
Fragmentation   Redirect   Unreachable
-------------   --------   -----------
enabled         enabled    enabled
Destination     Gateway         Flags   Use         Interface
--------------- --------------- ------  ----------  ---------
default         192.122.173.43   UG           59444  sc0
default         192.122.173.42   UG           59444  sc0
192.22.74.0     192.22.74.223    U                5  sc0
Console> (enable)

Console> (enable) set ip route default 192.122.173.44 1
Route added.
Console> (enable)

Console> (enable) show ip route
Fragmentation   Redirect   Unreachable
-------------   --------   -----------
enabled         enabled    enabled
Destination     Gateway         Flags   Use         Interface
--------------- --------------- ------  ----------  ---------
default         192.122.173.44   UG           59444  sc0
default         192.122.173.43   UG           59444  sc0
default         192.122.173.42   UG           59444  sc0
192.22.74.0     192.22.74.223    U                5  sc0
Console> (enable)
```

Related Commands

clear ip route
show ip route

set ip unreachable

Use the **set ip unreachable** command to enable or disable ICMP unreachable messages on the Catalyst 6000 family switch.

set ip unreachable {**enable** | **disable**}

Syntax Description

enable	Keyword to allow IP unreachable messages to be returned to the source host.
disable	Keyword to prevent IP unreachable messages from being returned to the source host.

Defaults

The default is ICMP unreachable messages is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you enable ICMP unreachable messages, the switch returns an ICMP unreachable message to the source host whenever it receives an IP datagram that it cannot deliver. When you disable ICMP unreachable messages, the switch does not notify the source host when it receives an IP datagram that it cannot deliver.

For example, a switch has the ICMP unreachable message function enabled and IP fragmentation disabled. If a FDDI frame is received and needs to transmit to an Ethernet port, the switch cannot fragment the packet. The switch drops the packet and returns an IP unreachable message to the Internet source host.

Examples

This example shows how to disable ICMP unreachable messages:

```
Console> (enable) set ip unreachable disable
ICMP Unreachable message disabled.
Console> (enable)
```

Related Commands

show ip route

set kerberos clients mandatory

Use the **set kerberos clients mandatory** command to make Kerberos authentication mandatory for authenticating to services on the network.

set kerberos clients mandatory

Syntax Description

This command has no arguments or keywords.

Defaults

The default is Kerberos clients are not set to mandatory.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

As an added layer of security, you can optionally configure the switch so that after users authenticate to it, they can authenticate to other services on the network only with Kerberos clients. If you do not make Kerberos authentication mandatory and Kerberos authentication fails, the application attempts to authenticate users using the default method of authentication for that network service. For example, Telnet prompts for a password.

Examples

This example shows how to make Kerberos authentication mandatory:

```
Console> (enable) set kerberos clients mandatory
Kerberos clients set to mandatory
Console> (enable)
```

Related Commands

clear kerberos clients mandatory
set kerberos credentials forward
show kerberos

set kerberos credentials forward

Use the **set kerberos credentials forward** command to configure clients to forward users' credentials as they connect to other hosts in the Kerberos realm.

set kerberos credentials forward

Syntax Description

This command has no arguments or keywords.

Defaults

The default is forwarding is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

A user authenticated to a Kerberized switch has a TGT and can use it to authenticate to a host on the network. However, if forwarding is not enabled and a user tries to list credentials after authenticating to a host, the output will show no Kerberos credentials present.

You can optionally configure the switch to forward user TGTs as they authenticate from the switch to Kerberized remote hosts on the network by using Kerberized Telnet.

Examples

This example shows how to enable Kerberos credentials forwarding:

```
Console> (enable) set kerberos credentials forward
Kerberos credentials forwarding enabled
Console> (enable)
```

Related Commands

set kerberos clients mandatory
set kerberos local-realm
show kerberos

set kerberos local-realm

Use the **set kerberos local-realm** command to configure a switch to authenticate users defined in the Kerberos database.

set kerberos local-realm *kerberos_realm*

Syntax Description

kerberos_realm	IP address or name (in uppercase characters) of the Kerberos realm.

Defaults

The default value is a NULL string.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

To authenticate a user defined in the Kerberos database, you must configure the switch to know the host name or IP address of the host running the KDC and the name of the Kerberos realm.

You must enter the Kerberos realm name in all uppercase characters.

Examples

This example shows how to set a default Kerberos local realm for the switch:

```
Console> (enable) set kerberos local-realm CISCO.COM
Kerberos local realm for this switch set to CISCO.COM.
Console> (enable)
```

Related Commands

clear kerberos realm
set kerberos realm
show kerberos

set kerberos realm

Use the **set kerberos realm** command to map the name of a Kerberos realm to a DNS domain name or a host name.

set kerberos realm {*dns_domain* | *host*} *kerberos_realm*

Syntax Description

dns_domain	DNS domain name to map to Kerberos realm.
host	IP address or name to map to Kerberos host realm.
kerberos_realm	IP address or name of Kerberos realm.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can map the name of the Kerberos realm to a DNS domain name or a host name by entering the **set kerberos realm** command. The information entered with this command is stored in a table with one entry for each Kerberos realm. The maximum number of entries in the table is 100.

You must enter Kerberos realms in uppercase characters.

Examples

This example shows how to map the Kerberos realm to a domain name:

```
Console> (enable) set kerberos realm CISCO CISCO.COM
Kerberos DnsDomain-Realm entry set to CISCO - CISCO.COM
Console> (enable)
```

Related Commands

clear kerberos realm
set kerberos local-realm
show kerberos

set kerberos server

Use the **set kerberos server** command to specify which KDC to use on the switch.

set kerberos server *kerberos_realm* {*hostname* | *ip_address*} [*port*]

Syntax Description

kerberos_realm	Name of the Kerberos realm.
hostname	Name of host running the KDC.
ip_address	IP address of host running the KDC.
port	(Optional) Number of the port.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can specify to the switch which KDC to use in a Kerberos realm. Optionally, you can also specify the port number which the KDC is monitoring. The Kerberos server information you enter is maintained in a table with one entry for each Kerberos realm. The maximum number of entries in the table is 100.

The KDC is a Kerberos server and database program running on a network host that allocates the Kerberos credentials to different users or network services.

Examples

This example shows how to specify the Kerberos server:

```
Console> (enable) set kerberos server CISCO.COM 187.0.2.1 750
Kerberos Realm-Server-Port entry set to:CISCO.COM - 187.0.2.1 - 750
Console> (enable)
```

Related Commands

clear kerberos server
set kerberos server
show kerberos

set kerberos srvtab entry

Use the **set kerberos srvtab entry** command to enter the SRVTAB file directly into the switch from the command line.

set kerberos srvtab entry *kerberos_principal principal_type timestamp key_version number key_type key_length encrypted_keytab*

Syntax Description

kerberos_principal	Service on the switch.
principal_type	Version of the Kerberos SRVTAB.
timestamp	Number representing the date and time the SRVTAB entry was created.
key_version_number	Version of the encrypted key format.
key_type	Type of encryption used.
key_length	Length, in bytes, of the encryption key.
encrypted_keytab	Secret key the switch shares with the KDC.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

To make it possible for remote users to authenticate to the switch using Kerberos credentials, the switch must share a secret key with the KDC. To do this, you must give the switch a copy of the file that is stored in the KDC, which contains the secret key. These files are called SRVTAB files.

When you enter the SRVTAB directly into the switch, create an entry for each Kerberos principal (service) on the switch. The entries are maintained in the SRVTAB table. The maximum table size is 20 entries.

The KDC is a Kerberos server and database program running on a network host that allocates the Kerberos credentials to different users or network services.

The key is encrypted with the private 3DES key when you copy the configuration to a file or enter the **show config** command.

Examples

This example shows how to enter a SRVTAB file directly into the switch:

```
Console> (enable) set kerberos srvtab entry host/niners.cisco.com@CISCO.COM 0 932423923 1
1 8 03;;5>00>50;0=0=0
Kerberos SRVTAB entry set to
Principal:host/niners.cisco.com@CISCO.COM
Principal Type:0
Timestamp:932423923
Key version number:1
Key type:1
Key length:8
Encrypted key tab:03;;5>00>50;0=0=0
```

Related Commands

clear kerberos clients mandatory
show kerberos

set kerberos srvtab remote

Use the **set kerberos srvtab remote** command to provide the switch with a copy of the SRVTAB file from the KDC that contains the secret key.

set kerberos srvtab remote {*hostname* | *ip_address*} *filename*

Syntax Description

hostname	Name of host running the KDC.
ip_address	IP address of host running the KDC.
filename	Name of the SRVTAB file.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

To make it possible for remote users to authenticate to the switch using Kerberos credentials, the switch must share a secret key with the KDC. To do this, you must give the switch a copy of the file that is stored in the KDC, which contains the secret key. These files are called SRVTAB files.

The KDC is a Kerberos server and database program running on a network host that allocates the Kerberos credentials to different users or network services.

The most secure method to copy SRVTAB files to the hosts in your Kerberos realm is to copy them onto physical media and go to each host in turn and manually copy the files onto the system. To copy SRVTAB files to the switch, which does not have a physical media drive, you must transfer them through the network using TFTP.

Examples

This example shows how to copy SRVTAB files to the switch remotely from the KDC:

```
Console> (enable) set kerberos srvtab remote 187.20.32.10 /users/jdoe/krb5/ninerskeytab
Console> (enable)
```

Related Commands

clear kerberos creds
set kerberos srvtab entry
show kerberos

set key config-key

Use the **set key config-key** command to define a private 3DES key.

set key config-key *string*

Syntax Description

string	3DES key name.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can define a private 3DES key for the switch. You can use the private 3DES key to encrypt the secret key that the switch shares with the KDC. If you set the 3DES key, the secret key is not displayed in clear text when you execute the **show kerberos** command. The key length should be eight characters or less.

Examples

This example shows how to define a 3DES key:

```
Console> (enable) set key config-key abcd
Kerberos config key set to abcd
Console> (enable)
```

Related Commands

clear key config-key

set lacp-channel system-priority

Use the **set lacp-channel system-priority** command to set the priority of the system.

set lacp-channel system-priority *value*

Syntax Description

value	Number of the priority; valid values are from **1** to **65535**.

Defaults

The default system priority value is **32768**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

LACP is supported on all Ethernet interfaces.

The **set lacp-channel system-priority** command is a global command; however, the priority value is used only for the modules that are running LACP. The priority value is ignored on the modules that are running PAgP.

Higher value numbers correspond to lower priority levels.

For differences between PAgP and LACP, refer to the "Guidelines for Port Configuration" section of the "Configuring EtherChannel" chapter of the *Catalyst 6000 Family Software Configuration Guide*.

Related Commands

clear lacp-channel statistics
set channelprotocol
set port lacp-channel
set spantree channelcost
set spantree channelvlancost
show lacp-channel
show port lacp-channel

set lcperroraction

Use the **set lcperroraction** command to configure how your system handles LCP errors when a module reports an ASIC problem to the NMP.

set lcperroraction *action*

Syntax Description

action	Action for handling LCP errors. See the "Usage Guidelines" section for more information about valid values for action levels.

Defaults

The default is that the action level is set to **ignore**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Valid values for action levels are as follows:

- **operator**—The system displays a recommended action for you to take. The system also logs the LCP error.
- **system**—The system automatically takes an action to handle the LCP error. The system also logs the LCP error.
- **ignore**—No action is taken. The system only logs the LCP error.

Note Be careful when using the **system** value because the switch automatically takes action, including possibly resetting or power cycling modules.

Examples

This example shows how to set the action that handles an LCP error:

```
Console> (enable) set lcperroraction ignore
Console> (enable)
```

Related Commands

show lcperroraction

set lda

Use the **set lda** command to configure the ASLB information on the Catalyst 6000 family switch.

set lda enable | **disable**

set lda vip {*server_virtual_ip*} {*destination_tcp_port*} [{*server_virtual_ip*} {*destination_tcp_port*}] ...

set lda mac ld {*ld_mac_address*}

set lda mac router {*mac_address*}...

set lda router {*router_vlan*} {*ld_mod/port*} [*backup_ld_mod/port*]

set lda server {*server_vlan*} {*ld_mod/port*} [*backup_ld_mod/port*]

set lda udpage {*udpagetime*}

Syntax Description

enable | **disable**	Keyword to enable or disable the ASLB feature.
vip *server_virtual_ip destination_tcp_port*	Keyword and variables to specify the virtual IP address of the server and the number of the destination TCP port that will be accelerated by the switch (up to 1024).
mac ld *ld_mac_address*	Keyword and variables to specify the LD MAC address.
mac router *mac_address...*	Keyword and variable to specify the router MAC address.
router *router_vlan*	Keyword and variable to specify the router VLAN.
ld_mod/port	Module and port number of the port connected to the LD on the VLAN.
backup_ld_mod/port	(Optional) Module and port number of the port connected to the backup LD.
server *server_vlan*	Keyword and variable to specify the server VLAN.
udpage *udpagetime*	Keyword and variable to specify the UDP aging time for LocalDirector acceleration.

Defaults

The default is the ASLB is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is supported only on switches configured with the Supervisor Engine 1 with Layer 3 Switching Engine WS-F6K-PFC (Policy Feature Card).

You can enter a zero (0) as a wildcard (don't care) digit for the *destination_tcp_port*.

You can enter up to 1024 *server_virtual_ip destination_tcp_port* entries separated by a space.

To cancel a previously entered VIP, use the **clear lda vip** command.

To cancel a previously entered MAC LD or router, use the **clear lda mac** command.

You need to enter the **set lda** commands to provide all the necessary information before using the **commit lda** command to program the setup into hardware.

The information you enter through the **set lda** commands are immediately saved into NVRAM, but you must enter the **commit lda** command for the setting to take effect.

When you disable the ASLB feature, you can enter the **set lda** commands, but the **commit lda** command will fail.

When you enter the **set lda mac router** command, you can enter up to 32 MAC addresses.

You can enter the value zero (0) to disable the **udpage** option. The *udpagingtime* is specified in milliseconds; values are from 0 ms to 2024000 ms.

Examples

This example shows how to enable the ASLB feature:

```
Console> (enable) set lda enable
Successfully enabled Local Director Acceleration.
Console> (enable)
```

This example shows how to disable the ASLB feature:

```
Console> (enable) set lda disable
Disabling Local Director Acceleration.....
Successfully disabled Local Director Acceleration.
Console> (enable)
```

This example shows how to specify the virtual IP address:

```
Console> (enable) set lda vip 10.0.0.8 8
Successfully set server virtual ip and port information.
Use commit lda command to save settings to hardware.
Console> (enable)
```

This example shows how to specify the MAC address for the LocalDirector:

```
Console> (enable) set lda mac ld 1-2-3-4-5-6
Successfully set mac address.
Use commit lda command to save settings to hardware.
Console> (enable)
```

This example shows how to specify multiple router MAC addresses:

```
Console> (enable) set lda mac router 1-2-3-4-5-6 3-4-56-67-4-5
Successfully set mac address.
Use commit lda command to save settings to hardware.
Console> (enable)
```

This example shows how to specify the router VLAN:

```
Console> (enable) set lda router 110 4/26
Successfully set router vlan and ld port.
Use commit lda command to save settings to hardware.
Console> (enable)
```

This example shows how to specify the udpage aging time:

```
Console> (enable) set lda udpage 20
Succesfully set LDA UDP aging time to 20ms.
Console> (enable)
```

This example shows how to specify the server VLAN:

```
Console> (enable) set lda server 105 4/40
Successfully set server vlan and LD port.
Use commit lda command to save settings to hardware.
Console> (enable)
```

Related Commands

clear lda
commit lda
show lda

set length

Use the **set length** command to configure the number of lines in the terminal display screen.

set length *number* [**default**]

Syntax Description

number	Number of lines to display on the screen; valid values are from **0** to **512**.
default	(Optional) Keyword to set the number of lines in the terminal display screen for the current administration session and all other sessions.

Defaults

The default value is 24 lines upon starting a session.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Output from a single command that overflows a single display screen is followed by the --More-- prompt. At the --More-- prompt, you can press **Ctrl-C**, **q**, or **Q** to interrupt the output and return to the prompt, press the **Spacebar** to display an additional screen of output, or press **Return** to display one more line of output.

Setting the screen length to 0 turns off the scrolling feature and causes the entire output to display at once. Unless you use the **default** keyword, a change to the terminal length value applies only to the current session.

When you change the value in a session, it applies only to that session. When you use the **clear config** command, the number of lines in the terminal display screen is reset to the default of 100.

The **default** keyword is available in privileged mode only.

Examples

This example shows how to set the screen length to 60 lines:

```
Console> (enable) set length 60
Screen length for this session set to 60.
Console> (enable)
```

This example shows how to set the default screen length to 40 lines:

```
Console> (enable) set length 40 default
Screen length set to 40.
Console> (enable)
```

set logging buffer

Use the **set logging buffer** command to limit the number of system logging messages buffered.

set logging buffer *buffer_size*

Syntax Description

buffer_size	Number of system logging messages to store in the buffer; valid values are **1** to **500**.

Defaults

The default value is 500.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to limit the syslog message buffer to 400 messages:

```
Console> (enable) set logging buffer 400
System logging buffer size set to <400>.
Console> (enable)
```

Related Commands

clear logging buffer
set logging timestamp
show logging buffer

set logging console

Use the **set logging console** command to enable and disable the sending of system logging messages to the console.

set logging console {**enable** | **disable**}

Syntax Description

enable	Keyword to enable system message logging to the console.
disable	Keyword to disable system message logging to the console.

Defaults

The default is system message logging to the console is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to enable system message logging to the console:

```
Console> (enable) set logging console enable
System logging messages will be sent to the console.
Console> (enable)
```

This example shows how to disable system message logging to the console:

```
Console> (enable) set logging console disable
System logging messages will not be sent to the console.
Console> (enable)
```

Related Commands

set logging level
set logging session
show logging
show logging buffer

set logging history

Use the **set logging history** command to set the size of the syslog history table.

set logging history *syslog_history_table_size*

Syntax Description	*syslog_history_table_size*	Size of the syslog history table; valid values are from **0** to **500**.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The Catalyst 6000 family switch holds syslog messages until the number of messages equals the defined size of the history log, after which the N messages are sent.

Examples

This example shows how to set the size of the syslog history table to 400:

```
Console> (enable) set logging history 400
System logging history table size set to <400>.
Console> (enable)
```

Related Commands

clear logging buffer
show logging

set logging level

Use the **set logging level** command to set the facility and severity level used when logging system messages.

set logging level *facility severity* [**default**]

Syntax Description

facility	Value to specify the type of system messages to capture; facility types are listed in Table 2-12.
severity	Value to specify the severity level of system messages to capture; severity level definitions are listed in Table 2-13.
default	(Optional) Keyword to cause the specified logging level to apply to all sessions.

Table 2-12 Facility Types

Facility Name	Definition
all	All facilities
acl	access control list
cdp	Cisco Discovery Protocol
cops	Common Open Policy Service Protocol
dtp	Dynamic Trunking Protocol
dvlan	Dynamic VLAN
earl	Enhanced Address Recognition Logic
filesys	file system facility
gvrp	GARP VLAN Registration Protocol
ip	Internet Protocol
kernel	Kernel
ld	ASLB facility
mcast	Multicast
mgmt	Management
mls	Multilayer Switching
pagp	Port Aggregation Protocol
protfilt	Protocol Filter
pruning	VTP pruning
privatevlan	Private VLAN facility
qos	Quality of Service
radius	Remote Access Dial-In User Service
rsvp	ReSerVation Protocol
security	Security

Table 2-12 Facility Types (continued)

Facility Name	Definition
snmp	Simple Network Management Protocol
spantree	Spanning Tree Protocol
sys	System
tac	Terminal Access Controller
tcp	Transmission Control Protocol
telnet	Terminal Emulation Protocol
tftp	Trivial File Transfer Protocol
udld	User Datagram Protocol
vmps	VLAN Membership Policy Server
vtp	Virtual Terminal Protocol

Table 2-13 Severity Level Definitions

Severity Level	Description
0—emergencies	System unusable
1—alerts	Immediate action required
2—critical	Critical condition
3—errors	Error conditions
4—warnings	Warning conditions
5—notifications	Normal bug significant condition
6—informational	Informational messages
7—debugging	Debugging messages

Defaults

The default is *facility* is set to **all**, and *level* is set to **0**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can also set the logging level by using the **set logging server** command.

If you do not use the **default** keyword, the specified logging level applies only to the current session.

Examples

This example shows how to set the default facility and severity level for system message logging:

```
Console> (enable) set logging level snmp 2 default
System logging facility <snmp> set to severity 2(critical).
Console> (enable)
```

Related Commands

clear logging level
show logging
show logging buffer

set logging server

Use the **set logging server** command to enable and disable system message logging to configured syslog servers and to add a syslog server to the system logging server table.

set logging server {**enable** | **disable**}

set logging server *ip_addr*

set logging server *facility severity*

set logging server severity *severity*

set logging server *facility*

Syntax Description

enable	Keyword to enable system message logging to configured syslog servers.
disable	Keyword to disable system message logging to configured syslog servers.
ip_addr	IP address of the syslog server to be added to the configuration.
facility	Type of system messages to capture; server facility types are listed in Table 2-14.
severity	Severity level; severity level definitions are listed in Table 2-13.
severity *severity*	Keyword and variable to globally set the syslog maximum severity control for all message types; severity level definitions are listed in Table 2-13.

Table 2-14 Server Facility Types

Severity Level	Description
local 0	Server facility local 0
local 1	Server facility local 1
local 2	Server facility local 2
local 3	Server facility local 3
local 4	Server facility local 4
local 5	Server facility local 5
local 6	Server facility local 6
local 7	Server facility local 7
syslog	syslog facility

Defaults

The default is no syslog servers are configured to receive system messages.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can also set the logging level by using the **set logging level** command. If you do not enter the facility or server keywords, the parameter is applied to all levels.

Severity logging to a configured syslog server depends on the configuration set by the **set logging level** command. The server severity level must be greater than or equal to the default severity level of the message facility that you expect to receive in syslog messages on the syslog server.

Examples

This example shows how to enable system message logging to the server:

```
Console> (enable) set logging server enable
System logging messages will be sent to the configured syslog servers.
Console> (enable)
```

This example shows how to disable system message logging to the server:

```
Console> (enable) set logging server disable
System logging messages will not be sent to the configured syslog servers.
Console> (enable)
```

This example shows how to add a server to the system logging server table using its IP address:

```
Console> (enable) set logging server 171.69.192.205
171.69.192.205 added to the System logging server table.
Console> (enable)
```

This example shows how to globally set the syslog maximum severity control for all message types:

```
Console> (enable) set logging server severity 4
System logging server severity set to 4(warnings).
Console> (enable)
```

Related Commands

clear logging server
show logging

set logging session

Use the **set logging session** command to enable or disable the sending of system logging messages to the current login session.

set logging session {**enable** | **disable**}

Syntax Description

enable	Keyword to enable the sending of system logging messages to the current login session.
disable	Keyword to disable the sending of system logging messages to the current login session.

Defaults

The default is system message logging to the current login session is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to prevent system logging messages from being sent to the current login session:

```
Console> (enable) set logging session disable
System logging messages will not be sent to the current login session.
Console> (enable)
```

This example shows how to cause system logging messages to be sent to the current login session:

```
Console> (enable) set logging session enable
System logging messages will be sent to the current login session.
Console> (enable)
```

Related Commands

set logging console
set logging level
show logging
show logging buffer

set logging telnet

Use the **set logging telnet** command to enable or disable logging on Telnet sessions.

set logging telnet {**enable** | **disable**}

Syntax Description

enable	Keyword to enable logging on Telnet sessions.
disable	Keyword to disable logging on Telnet sessions.

Defaults

The default is system message logging to the Telnet session is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to allow system logging messages to be sent to new Telnet sessions:

```
Console> (enable) set logging telnet enable
System logging messages will be sent to the new telnet sessions.
Console> (enable)
```

This example shows how to prevent system logging messages from being sent to new Telnet sessions:

```
Console> (enable) set logging telnet disable
System logging messages will not be sent to the new telnet sessions.
Console> (enable)
```

Related Commands

set logging console
set logging level
show logging
show logging buffer

set logging timestamp

Use the **set logging timestamp** command to enable or disable the time-stamp display on system logging messages.

set logging timestamp {**enable** | **disable**}

Syntax Description

enable	Keyword to enable the time-stamp display.
disable	Keyword to disable the time-stamp display.

Defaults

By default, system message logging time-stamp is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to enable the time-stamp display:

```
Console> (enable) set logging timestamp enable
System logging messages timestamp will be enabled.
Console> (enable)
```

This example shows how to disable the time-stamp display:

```
Console> (enable) set logging timestamp disable
System logging messages timestamp will be disabled.
Console> (enable)
```

Related Commands

show logging

set logout

Use the **set logout** command to set the number of minutes until the system disconnects an idle session automatically.

set logout *timeout*

Syntax Description

timeout	Number of minutes until the system disconnects an idle session automatically; valid values are from **0** to **10,000** minutes.

Defaults

The default is 20 minutes.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Setting the value to 0 disables the automatic disconnection of idle sessions.

The **show tech-support** command may time out if the configuration file output takes longer to display than the configured session timeout time. If this happens, enter a **set logout** *timeout* value of 0 to disable automatic disconnection of idle sessions or enter a longer *timeout* value.

Examples

This example shows how to set the number of minutes until the system disconnects an idle session automatically:

```
Console> (enable) set logout 20
Sessions will be automatically logged out after 20 minutes of idle time.
Console> (enable)
```

This example shows how to disable the automatic disconnection of idle sessions:

```
Console> (enable) set logout 0
Sessions will not be automatically logged out.
Console> (enable)
```

Related Commands

show tech-support

set mls agingtime

Use the **set mls agingtime** command to specify the MLS aging time of shortcuts to an MLS entry in the Catalyst 6000 family switches.

set mls agingtime [**ip** | **ipx**] {*agingtime*}

set mls agingtime fast {*fastagingtime*} {*pkt_threshold*}

set mls agingtime long-duration {*longagingtime*}

Syntax Description

ip	(Optional) Keyword to specify IP MLS.
ipx	(Optional) Keyword to specify IPX MLS.
agingtime	MLS aging time of shortcuts to an MLS entry; valid values are multiples of 8 to any value in the range of **8** to **2024** seconds.
fast	Keyword to specify the MLS aging time of shortcuts to an MLS entry that has no more than *pkt_threshold* packets switched within *fastagingtime* seconds after it is created.
fastagingtime	MLS aging time of shortcuts to an MLS entry; valid values are multiples of 8 to any value in the range from **0** to **128** seconds.
pkt_threshold	Packet threshold value; valid values are **0**, **1**, **3**, **7**, **15**, **31**, **63**, and **127** packets.
long-duration	Keyword to set the aging time for active flows.
longagingtime	MLS aging time of shortcuts to an MLS entry; valid values are **64** to **1920** seconds in increments of 64.

Defaults

The default *agingtime* is 256 seconds. The default *fastagingtime* is 0, no fast aging. The default *pkt_threshold* is 0. The default *longagingtime* is 1920.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use the **ip** keyword, you are specifying a shortcut for IP MLS. If you use the **ipx** keyword, you are specifying a shortcut for IPX MLS.

If you enter *fastagingtime* **0**, fast aging is disabled.

If you do not specify *fastagingtime* or *pkt_threshold*, the default value is used.

If you enter any of the **set mls** commands on a Catalyst 6000 family switch without MLS, this warning message displays:

```
MLS not supported on feature card.
```

agingtime can be configured as multiples of 8 in the range of 8 to 2024 seconds. The values are picked up in numerical order to achieve efficient aging. Any value for *agingtime* that is not a multiple of 8 seconds is adjusted to the closest one. For example, 65 is adjusted to 64, while 127 is adjusted to 128.

fastagingtime can be configured as multiples of 8 to any value in the range of 0 to 128 seconds.

The default *pkt_threshold* is 0. It can be configured as 0, 1, 3, 7, 15, 31, 63, or 127 (the values picked for efficient aging). If you do not configure *fastagingtime* exactly the same for these values, it adjusts to the closest value. A typical value for *fastagingtime* and *pkt_threshold* is 32 seconds and 0 packet, respectively (it means no packet switched within 32 seconds after the entry was created).

Agingtime applies to an MLS entry that has no more than *pkt_threshold* packets switched within *fastagingtime* seconds after it is created. A typical example is the MLS entry destined to/sourced from a DNS or TFTP server. This entry may never be used again once it is created. For example, only one request goes to a server and one reply returns from the server, and then the connection is closed.

The **agingtime fast** option is used to purge entries associated with very short flows, such as DNS and TFTP.

Keep the number of MLS entries in the MLS cache below 32K. If the number of MLS entries exceed 32K, some flows (less than 1 percent) are sent to the router.

To keep the number of MLS cache entries below 32K, decrease the aging time up to 8 seconds. If your switch has a lot of short flows used by only a few packets, then you can use fast aging.

If cache entries continue to exceed 32K, decrease the normal aging time in 64-second increments from the 256-second default.

You can force an active flow to age out by entering the **set mls agingtime long-duration** command. You can specify the aging time of the active flow in the range of 64 to 1920 seconds in increments of 64.

Examples

These examples show how to set the aging time:

```
Console> (enable) set mls agingtime 512
IP Multilayer switching aging time set to 512 seconds.
Console> (enable)

Console> (enable) set mls agingtime ipx 512
IPX Multilayer switching aging time set to 512
Console> (enable)
```

This example shows how to set the fast aging time:

```
Console> (enable) set mls agingtime fast 32 0
Multilayer switching fast aging time set to 32 seconds for entries with no more than 0
packet switched.
Console> (enable)
```

This example shows how to set the aging time for active flows:

```
Console> (enable) set mls agingtime long-duration 128
Multilayer switching agingtime set to 128 seconds for long duration flows
Console> (enable)
```

Related Commands

clear mls statistics entry
show mls

set mls cef load-balance

Use the **set mls cef load-balance** command to include or exclude Layer 4 ports in a load-balancing hash.

set mls cef load-balance {**full** | **source-destination-ip**}

Syntax Description

full	Keyword to base the hash on Layer 4 ports and source and destination IP addresses.
source-destination-ip	Keyword to base the hash on source and destination IP addresses.

Defaults

By default, the load-balancing hash is based on source and destination IP addresses.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When multiple paths are available to reach a destination, the new hash is applied to pick the path to be used for forwarding.

Examples

This example shows how to base the hash on Layer 4 ports and source and destination IP addresses:

```
Console> (enable) set mls cef load-balance full
Console> (enable)
```

This example shows how to base the hash on source and destination IP addresses:

```
Console> (enable) set mls cef load-balance source-destination-ip
Console> (enable)
```

Related Commands

show mls

set mls exclude protocol

Use the **set mls exclude protocol** command on a switch configured with the Supervisor Engine 1 with Layer 3 Switching Engine WS-F6K-PFC to add a protocol port to be excluded from being shortcut. Use this command on switches configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) to exclude protocols from statistics gathering.

set mls exclude protocol {**tcp** | **udp** | **both**} {*port_number* | *port_name*}

Syntax Description

tcp | **udp** | **both**	Keyword to specify a TCP, UDP port, or that the port be applied to both TCP and UDP traffic.
port_number	Number of the protocol port; valid values are from **1** to **65535**.
port_name	Name of the port; valid values are **dns**, **ftp**, **smtp**, **telnet**, **x**, **www**.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you enter any of the **set mls** commands on a Catalyst 6000 family switch without MLS, this warning message displays:

```
MLS not supported on feature card.
```

You can add a maximum of four protocol ports to the exclude table.

MLS exclusion is supported in full flow mode only.

If you enter **x** for the port name, this specifies the Layer 4 port used by the X-windows application.

Examples

This example shows how to exclude TCP packets on protocol port 6017:

```
Console> (enable) set mls exclude protocol tcp 6017
TCP packets with protocol port 6017 will be switched by RP.
Console> (enable)
```

This example shows how to exclude UDP packets on protocol port 6017:

```
Console> (enable) set mls exclude protocol udp 6017
TCP and UDP packets with protocol port 6017 will be switched by RP.
Console> (enable)
```

Related Commands

show mls

set mls flow

Use the **set mls flow** command to specify the minimum flow mask used for MLS. This command is needed to collect statistics for the supervisor engine.

set mls flow {**destination** | **destination-source** | **full**}

Caution **Use this command carefully.** This command *purges all existing shortcuts* and affects the number of active shortcuts. This command can increase the cache usage and increase the load on the router.

Caution Be extremely careful if you enter this command on a switch that already has a large number of shortcuts (greater than 16K).

Caution Do not place this command in scripts that are frequently executed—changing the MLS flow mask purges all MLS cache entries.

Syntax Description

destination	Keyword to set the minimum flow mask to destination flow.
destination-source	Keyword to set the minimum flow mask to source flow.
full	Keyword to set the minimum flow mask to an extended access list.

Defaults

If there are no access lists on any MLS-RP, the flow mask is set to destination flow.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command specifies the minimum MLS flow mask. Depending on the MLS-RP configuration, the actual flow mask used might be more specific than the specified minimum flow mask. For example, if you configure the minimum flow mask to **destination-source**, but an MLS-RP interface is configured with IP extended access lists, the actual flow mask used will be **full**.

If you configure a more specific flow mask (for example, **destination-source** or **full**), the number of active flow entries increases. To limit the number of active flow entries, you might need to decrease the MLS aging time.

This command is intended to be used for gathering very detailed statistics at the protocol port level; for example, when NetFlow data is exported to an RMON2 probe.

Examples

These examples show how to specify that only expired flows to subnet 171.69.194.0 are exported:

```
Console> (enable) set mls flow destination
Configured flow mask is set to destination flow.
Console> (enable)

Console> (enable) set mls flow destination-source
Configured flow mask is set to destination-source flow.
Console> (enable)

Console> (enable) set mls flow full
Configured flow mask is set to full flow.
Console> (enable)
```

Related Commands

show mls

set mls nde

Use the **set mls nde** command to configure the NDE feature in the Catalyst 6000 family switches to allow command-exporting statistics to be sent to the preconfigured collector.

set mls nde {**enable** | **disable**}

set mls nde {*collector_ip* | *collector_name*} {*udp_port_num*}

set mls nde version {**1** | **7** | **8**}

set mls nde flow [**exclude** | **include**] [**destination** *ip_addr_spec*] [**source** *ip_addr_spec*] [**protocol** *protocol*] [**src-port** *src_port*] [**dst-port** *dst_port*]

Syntax Description

enable	Keyword to enable NDE.
disable	Keyword to disable NDE.
collector_ip	IP address of the collector if DNS is enabled.
collector_name	Name of the collector if DNS is enabled.
udp_port_num	Number of the UDP port to receive the exported statistics.
version	Keyword to specify the version of the NDE; valid versions are **1**, **7**, and **8**.
1 | **7** | **8**	Version of the NDE feature.
flow	Keyword to add filtering to NDE.
exclude	(Optional) Keyword to allow exporting of all flows except the flows matching the given filter.
include	(Optional) Keyword to allow exporting of all flows matching the given filter.
destination	(Optional) Keyword to specify the destination IP address.
ip_addr_spec	(Optional) Full IP address or a subnet address in these formats: *ip_addr*, *ip_addr/netmask*, or *ip_addr/maskbit*.
source	(Optional) Keyword to specify the source IP address.
protocol	(Optional) Keyword to specify the protocol type.
protocol	(Optional) Protocol type; valid values can be a number from **0** to **255** or **ip**, **ipinip**, **icmp**, **igmp**, **tcp**, or **udp**. **0** indicates “do not care.”
src-port *src_port*	(Optional) Keyword and variable to specify the number of the TCP/UDP source port (decimal). Used with **dst-port** to specify the port pair if the **protocol** is **tcp** or **udp**. **0** indicates “do not care.”
dst-port *dst_port*	(Optional) Keyword and variable to specify the number of the TCP/UDP destination port (decimal). Used with **src-port** to specify the port pair if the **protocol** is **tcp** or **udp**. **0** indicates “do not care.”

Defaults

The defaults are Netflow Data Export version 7, and all expired flows are exported until the filter is specified explicitly.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you enter any **set mls nde** commands on a Catalyst 6000 family switch without MLS, this warning message displays:

```
mls not supported on feature card.
```

When you try to enable NDE and there are previously configured filtered flows on the switch, this warning message displays:

```
Console> (enable) set mls nde enable
Netflow export configured for port 80 on host 172.20.25.101
Netflow export enabled.
Warning!! There is a potential statistics mismatch due to existing excluded
protocols.
```

When you try to add a filter to exclude some protocol packets and NDE is currently enabled, this warning message displays:

```
Console> (enable) set mls exclude protocol tcp 80
Netflow tables will not create entries for TCP packets with protocol port
80.
Warning!! There's a potential statistics mismatch due to enabled NDE.
```

Before you use the **set mls nde** command for the first time, you must configure the host to collect MLS statistics. The host name and UDP port number are saved in NVRAM, so you do not need to specify them. If you specify a host name and UDP port, values in NVRAM overwrite the old values. Collector values in NVRAM do not clear when NDE is disabled, because this command configures the collector, but does not enable NDE automatically.

The **set mls nde enable** command enables NDE, exporting statistics to the preconfigured collector.

If the *protocol* is not **tcp** or **udp**, set the **dst-port** *dst_port* and **src-port** *src_port* values to 0; otherwise, no flows are displayed.

If you try to enable NDE without first specifying a collector, you see this display:

```
Console> (enable) set mls nde enable
Please set host name and UDP port number with 'set mls nde <collector_name | collector_ip>
<udp_port_number>'.
Console> (enable)
```

The **set mls nde flow** command adds filtering to the NDE. 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 NDE is disabled.

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.

Use the following syntax to specify an IP subnet address:

- *ip_subnet_addr*—This is the 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.
- *ip_addr/subnet_mask*—This is the 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* is a full host address, such as 172.22.253.1/255.255.252.00.
- *ip_addr/maskbits*—This is the 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* is a full host address, such as 193.22.253.1/22, which has the same subnet address as the *ip_subnet_addr.*

When you use the **set mls nde** {*collector_ip* | *collector_name*} {*udp_port_num*} command, the host name and UDP port number are saved in NVRAM and need not be specified again. If you specify a host name and UDP port, the new values overwrite the values in NVRAM. Collector values in NVRAM do not clear when you disable NDE.

Examples

This example shows how to specify that only expired flows to a specific subnet are exported:

```
Console> (enable) set mls nde flow include destination 171.69.194.140/24
NDE destination filter set to 171.69.194.0/24
Console> (enable)
```

This example shows how to specify that only expired flows to a specific host are exported:

```
Console> (enable) set mls nde flow include destination 171.69.194.140
NDE destination filter set to 171.69.194.140/32.
Console> (enable)
```

This example shows how to specify that only expired flows from a specific subnet to a specific host are exported:

```
Console> (enable) set mls nde flow include destination 171.69.194.140/24 source 171.69.173.5/24
NDE destination filter set to 171.69.194.0/24, source filter set to 171.69.173.0/24
Console> (enable)
```

This example shows how to specify that only flows from a specific port are exported:

```
Console> (enable) set mls nde flow include dst_port 23
NDE source port filter set to 23.
Console> (enable)
```

This example shows how to specify that only expired flows from a specific host that are of a specified protocol are exported:

```
Console> (enable) set mls nde flow include source 171.69.194.140 protocol 51
NDE destination filter set to 171.69.194.140/32, protocol set to 51.
Console> (enable)
```

This example shows how to specify that all expired flows except those from a specific host to a specific destination port are exported:

```
Console> (enable) set mls nde flow exclude source 171.69.194.140 dst_port 23
NDE destination filter set to 171.69.194.140/32, source port filter set to 23.
Flows matching the filter will be excluded.
Console> (enable)
```

Related Commands

clear mls nde flow
show mls

set mls statistics protocol

Use the **set mls statistics protocol** command to add protocols to the protocols statistics list.

set mls statistics protocol *protocol src_port*

Syntax Description

protocol	Name or number of the protocol; valid values are from **1** to **255**, **ip**, **ipinip**, **icmp**, **igmp**, **tcp**, and **udp**.
src_port	Number or type of the source port; valid values are from **1** to **65535**, **dns**, **ftp**, **smtp**, **telnet**, **x**, and **www**.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you enter any **set mls** commands on a Catalyst 6000 family switch without MLS, this warning message displays:

```
MLS not supported on feature card.
```

You can configure a maximum of 64 ports using the **set mls statistics protocol** command.

If you enter **x** for the source port, this specifies the Layer 4 port used by the X-windows application.

Examples

This example shows how to set protocols for statistic collection:

```
Console> (enable) set mls statistics protocol 17 1934
Protocol 17 port 1934 is added to protocol statistics list.
Console> (enable)
```

Related Commands

clear mls statistics entry
show mls statistics

set mls verify

To enable or disable checksum or packet checking based on packet length, use the **set mls verify** command.

set mls verify checksum {**enable** | **disable**}

set mls verify length {**ip** | **ipx** | **both**} {**minimum** | **inconsistant**} {**enable** | **disable**}

Syntax Description

checksum	Specifies IP checksum.
enable	Enables IP checksum.
disable	Disables IP checksum.
length	Specifies checking IP or IPX packets based on packet length.
ip | **ipx** | **both**	Specifies the type of packet.
minimum	Specifies checking minimum packet length.
inconsistant	Specifies checking inconsistent packet length. See the "Usage Guidelines" section for more information.
enable	Enables checking IP or IPX packets based on packet length.
disable	Disables checking IP or IPX packets based on packet length.

Defaults

IP checksum is enabled.

Checking IP and IPX packets based on minimum and inconsistent packet length is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set mls verify** command is available on Supervisor Engine 2 (WS-X6K-SUP2-2GE).

If you enable IP checksum or packet checking based on packet length, the Layer 3 ASIC drops Layer 3 error packets that it encounters. If you disable this feature, the packets are not dropped.

Note We recommend that you do not disable IP checksum or packet checking based on packet length unless you have a specific need to pass non-standard packets.

Checking for inconsistent packet length means that the switch checks for an inconsistency between the physical length of the packet and the length coded in the packet.

Examples

This example shows how to enable IP checksum:

```
Console> (enable) set mls verify checksum enable
Ip checksum verification enabled
Console> (enable)
```

This example shows how to enable checking inconsistent IP and IPX packet length:

```
Console> (enable) set mls verify length both inconsistant enable
Ipx inconsistant length verification enabled
Ip inconsistant length verification enabled
Console> (enable)
```

This example shows how to disable checking minimum IPX packet length:

```
Console> (enable) set mls verify length ipx minimum disable
Ipx minimum length verification disabled
Console> (enable)
```

Related Commands

show mls verify

set module

Use the **set module** command to enable or disable a module.

set module enable | **disable** *mod*

Syntax Description

enable	Keyword to enable a module.
disable	Keyword to disable a module.
mod	Number of the module.

Defaults

The default is all modules are enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Avoid disabling a module when you are connected via a Telnet session; if you disable your session, you will disconnect your Telnet session.

If there are no other network connections to a Catalyst 6000 family switch (for example, on another module), you have to reenable the module from the console.

You can specify a series of modules by entering a comma between each module number (for example, 2,3,5). You can specify a range of modules by entering a dash between module numbers (for example, 2-5).

The **set module disable** command does not cut off the power to a module, it only disables the module. To turn off power to a module, refer to the **set module power** command.

If an individual port on a module was previously disabled, enabling the module does not enable the disabled port.

Examples

This example shows how to enable module 2:

```
Console> (enable) set module enable 2
Module 2 enabled.
Console> (enable)
```

This example shows how to disable module 3 when connected via the console port:

```
Console> (enable) set module disable 3
Module 3 disabled.
Console> (enable)
```

This example shows how to disable module 2 when connected via a Telnet session:

```
Console> (enable) set module disable 2
This command may disconnect your telnet session.
Do you want to continue (y/n) [n]? y
Module 2 disabled.
Console> (enable)
```

Related Commands **show module**

set module name

Use the **set module name** command to set the name for a module.

set module name *mod* [*mod_name*]

Syntax Description

mod	Number of the module.
mod_name	(Optional) Name created for the module.

Defaults

The default is no module names are configured for any modules.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If no module name is specified, any previously specified name is cleared.

Use the **set module name** command to set the module for the MSM. Additional **set module** commands are not supported by the MSM.

Examples

This example shows how to set the name for module 1 to Supervisor:

```
Console> (enable) set module name 1 Supervisor
Module name set.
Console> (enable)
```

Related Commands

show module

set module power

Use the **set module power** command to turn on or shut off the power to a module.

set module power up | **down** *mod*

Syntax Description

up	Keyword to turn on the power to a module.
down	Keyword to turn off the power to a module.
mod	Number of the module.

Defaults

The default is power is on to a module.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set module power up** command allows you to check if adequate power is available in the system to turn the power on. If not enough power is available, the module status changes from power-down to power-deny, and this message displays:

```
Module 4 could not be powered up due to insufficient power.
```

Examples

This example shows how to power up module 4:

```
Console> (enable) set module power up 4
Module 4 powered up.
Console> (enable)
```

This example shows how to power down module 4:

```
Console> (enable) set module power down 4
Module 4 powered down.
Console> (enable)
```

Related Commands

show environment

set module shutdown

Use the **set module shutdown** command to shut down the NAM and IDSM.

set module shutdown all | *mod*

Syntax Description

all	Keyword to shut down NAM and IDSMs.
mod	Number of the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use the **set module shutdown** command, the configuration is not saved in NVRAM. The next time when the module boots up, it will come online. You can either reinsert or reset the module to bring it online.

If there are no other network connections to a Catalyst 6000 family switch (for example, on another module), you have to reenable the module from the console.

You can specify a series of modules by entering a comma between each module number (for example, 2,3,5).

Examples

This example shows how to shutdown the NAM or IDSM:

```
Console> (enable) set module shutdown 2


Console> (enable)
```

set msfcautostate

Use the **set msfcautostate** command to enable or disable the line protocol state determination of the MSFCs due to port state changes.

set msfcautostate {**enable** | **disable**}

Syntax Description

enable	Keyword to activate the line protocol state determination.
disable	Keyword to deactivate the line protocol state determination.

Defaults

The default is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This feature is used to accurately reflect the Layer 3 interface status based on the underlying Layer 2 interface status so that routing and other protocols converge faster. Faster protocol convergence prevents traffic from being discarded without notice.

When you enable the MSFC auto state feature, VLAN interfaces on the MSFC are active only when there is at least one other active interface in the spanning tree forwarding state on the Catalyst 6000 family switch. This interface could be a physical end-user port, a trunk connection for which the VLAN is active, or even another MSFC with an equivalent VLAN interface.

If you enable and then disable or disable and then enable the **set msfcautostate** command, you might have to use the **shutdown** and **no shutdown** commands to disable and then restart the VLAN and WAN interfaces on the MSFC.

If your FXS module ports are in an auxiliary VLAN and there are no switching module ports active in the VLAN, the FXS module will not initialize because the MSFC auto state feature shuts down all MSFC interfaces and subinterfaces. We recommend that you add a physical Ethernet port to the VLAN.

Caution You should not disable the MSFC auto state feature because the Layer 3 interface status might not accurately reflect the Layer 2 interface status. If you disable this feature, traffic might be discarded without notice even though other valid traffic paths might exist.

Examples

This example shows how to enable the line protocol state determination of the MSFC:

```
Console> (enable) set msfcautostate enable
Console> (enable)
```

This example shows how to disable the line protocol state determination of the MSFC:

```
Console> (enable) set msfcautostate disable
Console> (enable)
```

Related Commands show msfcautostate

set msmautostate

Use the **set msmautostate** command to enable or disable the line protocol state determination of the MSMs due to port state changes.

set msmautostate {**enable** | **disable**}

Syntax Description

enable	Keyword to activate the line protocol state determination.
disable	Keyword to deactivate the line protocol state determination.

Defaults

The default configuration has line protocol state determination disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This feature is useful for discontinuing the advertisement of routing paths when access to them is severed (either through fault or administrative disabling).

When you enable **msmautostate**, VLAN interfaces on the MSM are active only when there is at least one other active interface within the Catalyst 6000 family switch. This could be a physical end-user port, a trunk connection for which the VLAN is active, or even another MSM with an equivalent VLAN interface.

If you disable msmautostate, you might have to use the **shutdown** and **no shutdown** commands to disable and then restart the VLAN interface to bring the MSM back up.

Examples

This example shows how to enable the line protocol state determination of the MSM:

```
Console> (enable) set msmautostate enable
MSM port auto state enabled.
Console> (enable)
```

This example shows how to disable the line protocol state determination of the MSM:

```
Console> (enable) set msmautostate disable
MSM port auto state disabled.
Console> (enable)
```

Related Commands

show msmautostate

set multicast router

Use the **set multicast router** command to configure a port manually as a multicast router port.

set multicast router *mod/port*

Syntax Description

mod/port	Number of the module and port on the module.

Defaults

The default is no ports are configured as multicast router ports.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you enable IGMP snooping, the ports to which a multicast-capable router is attached are identified automatically. The **set multicast router** command allows you to configure multicast router ports statically.

Examples

This example shows how to configure a multicast router port:

```
Console> (enable) set multicast router 3/1
Port 3/1 added to multicast router port list.
Console> (enable)
```

Related Commands

clear multicast router
set igmp
show multicast group count
show multicast router

set ntp broadcastclient

Use the **set ntp broadcastclient** command to enable or disable NTP in broadcast-client mode.

set ntp broadcastclient {**enable** | **disable**}

Syntax Description

enable	Keyword to enable NTP in broadcast-client mode.
disable	Keyword to disable NTP in broadcast-client mode.

Defaults

The default is broadcast-client mode is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The broadcast-client mode assumes that a broadcast server, such as a router, sends time-of-day information regularly to a Catalyst 6000 family switch.

Examples

This example shows how to enable an NTP broadcast client:

```
Console> (enable) set ntp broadcastclient enable
NTP Broadcast Client mode enabled.
Console> (enable)
```

This example shows how to disable an NTP broadcast client:

```
Console> (enable) set ntp broadcastclient disable
NTP Broadcast Client mode disabled.
Console> (enable)
```

Related Commands

show ntp

set ntp broadcastdelay

Use the **set ntp broadcastdelay** command to configure a time-adjustment factor so the Catalyst 6000 family switch can receive broadcast packets.

set ntp broadcastdelay *microseconds*

Syntax Description

microseconds	Estimated round-trip time, in microseconds, for NTP broadcasts; valid values are from **1** to **999999**.

Defaults

The default is the NTP broadcast delay is set to 3000 milliseconds.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to set the NTP broadcast delay to 4000 milliseconds:

```
Console> (enable) set ntp broadcastdelay 4000
NTP broadcast delay set to 4000 microseconds.
Console> (enable)
```

Related Commands

show ntp

set ntp client

Use the **set ntp client** command to enable or disable a Catalyst 6000 family switch as an NTP client.

set ntp client {**enable** | **disable**}

Syntax Description

enable	Keyword to enable a Catalyst 6000 family switch as an NTP client.
disable	Keyword to disable a Catalyst 6000 family switch as an NTP client.

Defaults

The default is NTP client mode is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can configure NTP in either broadcast-client mode or client mode. The broadcast-client mode assumes that a broadcast server, such as a router, sends time-of-day information regularly to a Catalyst 6000 family switch. The client mode assumes that the client (a Catalyst 6000 family switch) regularly sends time-of-day requests to the NTP server.

Examples

This example shows how to enable NTP client mode:

```
Console> (enable) set ntp client enable
NTP client mode enabled.
Console> (enable)
```

Related Commands

show ntp

set ntp server

Use the **set ntp server** command to specify the NTP server address and configure an NTP server authentication key.

set ntp server *ip_addr* [**key** *public_keynum*]

Syntax Description

ip_addr	IP address of the NTP server.
key *public_keynum*	(Optional) Keyword to specify the key number; valid values are **1** to **4292945295**.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The client mode assumes that the client (a Catalyst 6000 family switch) sends time-of-day requests regularly to the NTP server. A maximum of ten servers per client is allowed.

Examples

This example shows how to configure an NTP server:

```
Console> (enable) set ntp server 172.20.22.191
NTP server 172.20.22.191 added.
Console> (enable)
```

Related Commands

clear ntp server
show ntp

set ntp summertime

Use the **set ntp summertime** command to specify whether the system should set the clock ahead one hour during daylight saving time.

set ntp summertime {**enable** | **disable**} [*zone*]

set ntp summertime recurring [{*week*} {*day*} {*month*} {*hh*:*mm*} {*week* | *day* | *month* | *hh*:*mm*} [*offset*]]

set ntp summertime date {*month*} {*date*} {*year*} {*hh*:*mm*}{*month* | *date* | *year* | *hh*:*mm*} [*offset*]

Syntax Description

enable	Keyword to cause the system to set the clock ahead one hour during daylight saving time.
disable	Keyword to prevent the system from setting the clock ahead one hour during daylight saving time.
zone	(Optional) Time zone used by the **set summertime** command.
recurring	Keyword to specify the summertime dates that recur every year.
week	Week of the month (**first**, **second**, **third**, **fourth**, **last**, **1**...**5**).
day	Day of the week (**Sunday**, **Monday**, **Tuesday**, and so forth).
month	Month of the year (**January**, **February**, **March**, and so forth).
hh:mm	Hours and minutes.
offset	(Optional) Amount of offset in minutes (**1** to **1440** minutes).
date	Day of the month (**1** to **31**).
year	Number of the year (**1993** to **2035**).

Defaults

By default, the **set ntp summertime** command is disabled. Once enabled, the default for *offset* is 60 minutes, following U.S. standards.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

After you enter the **clear config** command, the dates and times are set to default.

Unless you configure it otherwise, this command advances the clock one hour at 2:00 a.m. on the first Sunday in April and moves back the clock one hour at 2:00 a.m. on the last Sunday in October.

Examples

This example shows how to cause the system to set the clock ahead one hour during daylight saving time:

```
Console> (enable) set ntp summertime enable PDT
Summertime is enabled and set to “PDT”.
Console> (enable)
```

This example shows how to prevent the system from setting the clock ahead one hour during daylight saving time:

```
Console> (enable) set ntp summertime disable
Summertime disabled.
Console> (enable)
```

This example shows how to set daylight saving time to the zonename AUS and repeat every year, starting from the third Monday of February at noon and ending at the second Saturday of August at 3:00 p.m. with an offset of 30 minutes:

```
Console> (enable) set ntp summertime AUS recurring 3 Mon Feb 12:00 2 Saturday Aug 15:00 30
Summer time is disabled and set to 'AUS' with offset 30 minutes.
   start: 12:00:00 Sun Feb 13 2000
   end:   14:00:00 Sat Aug 26 2000
   Recurring, starting at 12:00:00 on Sunday of the third week of February and ending
   on Saturday of the fourth week of August.
Console> (enable)
```

This example shows how to set the daylight saving time to start on January 29, 1999 at 2:00 a.m. and end on August 19, 2004 at 3:00 p.m. with an offset of 30 minutes:

```
Console> (enable) set ntp summertime date jan 29 1999 02:00 aug 19 2004 15:00 30
Summertime is disabled and set to ''
Start : Fri Jan 29 1999, 02:00:00
End   : Thu Aug 19 2004, 15:00:00
Offset: 30 minutes
Recurring: no
Console> (enable)
```

This example shows how to set recurring to reset default to US summertime:

```
Console> (enable) set ntp summertime recurring 3 mon feb 4 thurs oct 8:00 500
Command authorization none.
Summertime is enabled and set to ''
Start : Mon Feb 21 2000, 03:00:00
End   : Fri Oct 20 2000, 08:00:00
Offset: 500 minutes (8 hours 20 minutes)
Recurring: yes, starting at 03:00am of third Monday of February and ending on 08:00am of
fourth Thursday of October.
Console> (enable)
```

Related Commands **show ntp**

set ntp timezone

Use the **set ntp timezone** command to configure the time offset from Greenwich Mean Time.

set timezone [*zone_name*] [*hours* [*minutes*]]

Syntax Description

zone_name	Name of the time zone.
hours	(Optional) Time offset (hours) from Greenwich Mean Time; valid values are from **–12** to **12** hours.
munutes	(Optional) Time offset (minutes) from Greenwich Mean Time; valid values are **0** to **59** munutes.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set ntp timezone** command is effective only when NTP is running. If you set the time explicitly and NTP is disengaged, the **set ntp timezone** command has no effect. If you have enabled NTP and have not entered the **set timezone** command, the Catalyst 6000 family switch displays UTC by default.

Examples

This example shows how to set the time zone to Pacific Standard Time with an offset of minus 8 hours from UTC:

```
Console> (enable) set ntp timezone PST -8
Timezone set to “PST”, offset from UTC is -8 hours.
Console> (enable)
```

Related Commands

clear ntp timezone
show ntp

set password

Use the **set password** command to change the login password on the CLI.

set password

Syntax Description

This command has no arguments or keywords.

Defaults

The default is no password is configured.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Passwords are case sensitive and may be from 0 to 19 characters in length, including spaces.

The command prompts you for the old password. If the password you enter is valid, you are prompted to enter a new password and to verify the new password. A zero-length password is allowed by pressing **Return**.

Examples

This example shows how to set an initial password:

```
Console> (enable) set password
Enter old password: <old_password>
Enter new password: <new_password>
Retype new password: <new_password>
Password changed.
Console> (enable)
```

set pbf

Use the **set pbf** command to enable PBF and to set a MAC address for the PFC2.

set pbf [**mac** *mac_address*]

Syntax Description

mac *mac_address*	(Optional) Keyword and variable to specify MAC address for the PFC2.

Defaults

You can use the default MAC address, or you can specify a MAC address. See the "Usage Guidelines" section for more information.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You must set a MAC address for the PFC2. We recommend that you use the default MAC address provided by the MAC PROM. When you specify your own MAC address using the **set pbf mac** command, if the MAC address is a duplicate of a MAC address already in use, packets might be dropped.

PBF is not supported with an operating (booted) MSFC2 in the Catalyst 6000 family switch that is being used for PBF. If an MSFC2 is present but not booted, you can configure PBF.

PBF may require some configuration on attached hosts. When a router is not present in the network, ARP table entries have to be statically added on each host participating in PBF. Refer to the "Configuring Policy-Based Forwarding" section of Chapter 16, "Configuring Access Control," in the *Catalyst 6000 Family Software Configuration Guide* for detailed information on configuring hosts.

Note PBF does not work with 802.1Q tunnel traffic. PBF is supported on Layer 3 IP unicast traffic, but it is not applicable to Layer 2 traffic. At the intermediate (PBF) switch, all 802.1Q tunnel traffic appears as Layer 2 traffic.

Examples

This example shows how to set the default MAC address for the PFC2:

```
Console> (enable) set pbf
Console> (enable) Operation successful.
Console> (enable)
```

This example shows how to set a specific MAC address for the PFC2:

```
Console> (enable) set pbf mac 00-01-64-61-39-c2
Console> (enable) Operation successful.
Console> (enable)
```

Related Commands clear pbf
show pbf

set port auxiliaryvlan

Use the **set port auxiliaryvlan** command to configure the auxiliary VLAN ports.

set port auxiliaryvlan *mod*[*/port*] {*vlan* | **untagged** | **dot1p** | **none**}

Syntax Description

mod[*/port*]	Number of the module and (optional) port or multiple ports.
vlan	Number of the VLAN; valid values are from **1** to **4096**.
untagged	Keyword to specify the connected device send and receive untagged packets without 802.1p priority.
dot1p	Keyword to specify the connected device send and receive packets with 802.1p priority.
none	Keyword to specify that the switch does not send any auxiliary VLAN information in the CDP packets from that port.

Defaults

The default setting is **none**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not specify a port, all ports are selected.

This command is not supported by the NAM.

The *vlan* option specifies that the connected device send packets tagged with a specific VLAN.

If you enter the **none** option, voice information will not be sent or received.

Dynamic VLAN support for VVID includes these restrictions to the following MVAP configuration on the switch port:

- You can configure any VVID on a dynamic port including dot1p and untagged, except when the VVID is equal to **dot1p** or **untagged**. If this is the case, you must configure VMPS with the MAC address of the IP phone. When you configure the VVID as **dot1p** or **untagged** on a dynamic port, this warning message displays:

  ```
  VMPS should be configured with the IP phone mac's.
  ```

- For dynamic ports, the auxiliary VLAN ID cannot be the same as the native VLAN ID assigned by VMPS for the dynamic port.
- You cannot configure trunk ports as dynamic ports, but an MVAP can be configured as a dynamic port.

Examples

This example shows how to set the auxiliary VLAN port to **untagged**:

```
Console> (enable) set port auxiliaryvlan 5/7 untagged
Port 5/7 allows the connected device send and receive untagged packets and
without 802.1p priority.
Console> (enable)
```

This example shows how to set the auxiliary VLAN port to **dot1p**:

```
Console> (enable) set port auxiliaryvlan 5/9 dot1p
Port 5/9 allows the connected device send and receive packets with 802.1p priority.
Console> (enable)
```

This example shows how to set the auxiliary VLAN port to **none**:

```
Console> (enable) set port auxiliaryvlan 5/12 none
Port 5/12 will not allow sending CDP packets with AuxiliaryVLAN information.
Console> (enable)
```

This example shows how to set the auxiliary VLAN port to a specific module, port, and VLAN:

```
Console> (enable) set port auxiliaryvlan 2/1-3 222
Auxiliaryvlan 222 configuration successful.
AuxiliaryVlan AuxVlanStatus Mod/Ports
------------ ------------ ------------------------
222          active       1/2,2/1-3
Console> (enable)
```

Related Commands

show port auxiliaryvlan

set port broadcast

Use the **set port broadcast** command to set the broadcast, multicast, or unicast suppression for one or more ports. The threshold limits the backplane traffic received from the module.

set port broadcast *mod/port threshold***%** [**multicast** {**enable** | **disable**}] [**unicast** {**enable** | **disable**}]

Syntax Description

mod/port	Number of the module and the port on the module.
*threshold***%**	Percentage of total available bandwidth that can be used by traffic; valid values are decimal numbers from **0.00%** to **100%** or whole numbers from **0%** to **100%**.
multicast	(Optional) Keyword to specify multicast suppression.
enable | **disable**	(Optional) Keywords to enable or disable the suppression type.
unicast	(Optional) Keyword to specify unicast suppression.

Defaults

The default is 100% (no broadcast limit).

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

You can enter the threshold value in two ways:

- A decimal number followed by a percent sign (for example 0.33%)
- A whole number followed by a percent sign (for example 33%)

The percent sign (%) is required when entering the threshold value.

The **multicast** and **unicast** keywords are supported on Gigabit Ethernet modules only.

If you enter the command without using the **multicast** or **unicast** keyword, only broadcast traffic is suppressed. If you enter the **multicast** or **unicast** keyword, both broadcast and the selected traffic type are suppressed.

Examples

This example shows how to limit broadcast traffic to 20 percent to a specific port on module 4:

```
Console> (enable) set port broadcast 4/3 20%
Port 4/3 broadcast traffic limited to 20.00%.
Console> (enable)
```

This example shows how to allow a specific amount of multicast traffic to a range of ports on module 4:

```
Console> (enable) set port broadcast 4/1-24 80% multicast enable
Port 4/1-24 multicast traffic limited to 80%.
Console> (enable)
```

Related Commands

clear pbf
show port broadcast

set port channel

Use the **set port channel** command to configure EtherChannel on Ethernet module ports.

set port channel *mod/port* [*admin_group*]

set port channel *mod/port* **mode** {**on** | **off** | **desirable** | **auto**} [**silent** | **non-silent**]

set port channel all mode off

set port channel all distribution {**ip** | **mac**} [**source** | **destination** | **both**]

set port channel all distribution {**session**} [**source** | **destination** | **both**]

Syntax Description

mod/port	Number of the module and the port on the module.
admin_group	(Optional) Number of the administrative group; valid values are from **1** to **1024**.
mode	Keyword to specify the EtherChannel mode.
on	Keyword to enable and force specified ports to channel without PAgP.
off	Keyword to prevent ports from channeling.
desirable	Keyword to set a PAgP mode that places a port into an active negotiating state, in which the port initiates negotiations with other ports by sending PAgP packets.
auto	Keyword to set a PAgP mode that places a port into a passive negotiating state, in which the port responds to PAgP packets it receives, but does not initiate PAgP packet negotiation.
silent	(Optional) Keyword to use with **auto** or **desirable** when no traffic is expected from the other device to prevent the link from being reported to STP as down.
non-silent	(Optional) Keyword to use with **auto** or **desirable** when traffic is expected from the other device.
all mode off	Keywords to globaly turn off channeling on all ports.
all distribution	Keywords to apply frame distribution to all ports in the Catalyst 6000 family switch.
ip	Keyword to specify the frame distribution method using IP address values.
mac	Keyword to specify the frame distribution method using MAC address values.
source	(Optional) Keyword to specify the frame distribution method using source address values.
destination	(Optional) Keyword to specify the frame distribution method using destination address values.
both	(Optional) Keyword to specify the frame distribution method using source and destination address values.
session	Keyword to allow frame distribution of Layer 4 traffic.
both	(Optional) Keyword to specify the frame distribution method using source and destination Layer 4 port number.

Defaults

The default is EtherChannel is set to **auto** and **silent** on all module ports. The defaults for frame distribution are **ip** and **both**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

This command is not supported by non-EtherChannel-capable modules.

The **set port channel all distribution session** command is supported on systems configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) only.

Make sure that all ports in the channel are configured with the same port speed, duplex mode, and so forth. For more information on EtherChannel, refer to the *Catalyst 6000 Family Software Configuration Guide*.

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 are running QoS, make sure that bundled ports are all of the same trust types and have similar queueing and drop capabilities.

Disable the port security feature on the channeled ports (see the **set port security** command). If you enable port security for a channeled port, the port shuts down when it receives packets with source addresses that do not match the secure address of the port.

You can configure up to eight ports on the same switch in each administrative group.

When you assign ports to an existing admin group, the original ports associated with the admin group will move to an automatically picked new admin group. You cannot add ports to the same admin group.

If you do not enter an *admin_group*, it means that you want to create a new administrative group with *admin_group* selected automatically. The next available *admin_group* is automatically selected.

If you do not enter the channel mode, the channel mode of the ports addressed are not modified.

The **silent** | **non-silent** parameters only apply if **desirable** or **auto** modes are entered.

If you do not specify **silent** or **non-silent**, the current setting is not affected.

Note With software releases 6.2(1) and earlier, the 6- and 9-slot Catalyst 6000 family switches support a maximum of 128 EtherChannels.

With software releases 6.2(2) and later, due to the port ID handling by the spanning tree feature, the maximum supported number of EtherChannels is 126 for a 6- or 9-slot chassis and 63 for a 13-slot chassis. Note that the 13-slot chassis was first supported in software release 6.2(2).

Examples

This example shows how to set the channel mode to **desirable**:

```
Console> (enable) set port channel 2/2-8 mode desirable
Ports 2/2-8 channel mode set to desirable.
Console> (enable)
```

This example shows how to set the channel mode to **auto**:

```
Console> (enable) set port channel 2/7-8,3/1 mode auto
Ports 2/7-8,3/1 channel mode set to auto.
Console> (enable)
```

This example shows how to group ports 4/1 through 4 in an admin group:

```
Console> (enable) set port channel 4/1-4 96
Port(s) 4/1-4 are assigned to admin group 96.
Console> (enable)
```

This example shows the display when the port list is exceeded:

```
Console> (enable) set port channel 2/1-9 1
No more than 8 ports can be assigned to an admin group.
Console> (enable)
```

This example shows how to disable EtherChannel on module 4, ports 4 through 6:

```
Console> (enable) set port channel 4/4-6 mode off
Port(s) 4/4-6 channel mode set to off.
Console> (enable)
```

This example shows the display output when you assign ports to an existing admin group. This example moves ports in admin group 96 to another admin group and assigns ports 4/4 through 6 to admin group 96:

```
Console> (enable) set port channel 4/4-6 96
Port(s) 4/1-3 are moved to admin group 97.
Port(s) 4/4-6 are assigned to admin group 96.
Console> (enable)
```

This example shows how to set the channel mode to **off** for ports 4/4 through 6 and assign ports 4/4 through 6 to an automatically selected admin group:

```
Console> (enable) set port channel 4/4-6 off
Port(s) 4/4-6 channel mode set to off.
Port(s) 4/4-6 are assigned to admin group 23.
Console> (enable)
```

This example shows how to configure the EtherChannel load-balancing feature:

```
Console> (enable) set port channel all distribution ip destination
Channel distribution is set to ip destination.
Console> (enable)
```

Related Commands

show channel
show channel group
show port channel

set port cops

Use the **set port cops** command to create port roles.

set port cops *mod*/*port* **roles** *role1* [*role2*]...

Syntax Description

mod/port	Number of the module and the port on the module.
roles *role#*	Keyword and variable to specify the roles.

Defaults

The default is all ports have a default role of null string, for example, the string of length 0.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

A port may have multiple roles. You can configure a maximum of 64 total roles per switch. You can specify multiple roles in a single command.

Examples

This example shows how to create roles on a port:

```
Console> (enable) set port cops 3/1 roles backbone_port main_port
New role 'backbone_port' created.
New role 'main_port' created.
Roles added for port 3/1-4.
Console> (enable)
```

This example shows the display if you attempt to create a roll and exceed the maximum allowable number of roles:

```
Console> (enable) set port cops 3/1 roles access_port
Unable to add new role. Maximum number of roles is 64.
Console> (enable)
```

Related Commands

clear port cops
show port cops

set port debounce

Use the **set port debounce** command to enable or disable the debounce timer or configure the timer setting on a per-port basis.

set port debounce *mod/port* {**enable** | **disable**}

Syntax Description

mod/port	Number of the module and the port on the module.
enable | **disable**	Keywords to enable or disable the debounce timer.

Defaults

By default, the debounce timer is disabled on all ports.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The debounce timer is the time the firmware waits before notifying the supervisor engine of a link change at the physical layer.

When the debounce timer is disabled, the debounce timer values are as follows:

- 10/100 ports—300 milliseconds
- 100BASE-FX ports—300 milliseconds
- 10/100/1000BASE-T and gigabit TX ports—300 milliseconds
- 10-gigabit and gigabit fiber ports—10 milliseconds

When the debounce timer is enabled, the debounce timer values are as follows:

- 10/100 ports—3100 milliseconds
- 100BASE-FX ports—3100 milliseconds
- 10/100/1000BASE-T and gigabit TX ports—3100 milliseconds
- 10-gigabit and gigabit fiber ports—100 milliseconds

For 10/100 ports and 100BASE-FX ports in the disabled state, the firmware may take up to 600 milliseconds to notify the supervisor engine of a link change because the firmware polling time is every 300 milliseconds.

For 10/100 ports and 100BASE-FX ports in the enabled state, the firmware may take up to 3400 milliseconds to notify the supervisor engine of a link change because the firmware polling time is every 300 milliseconds.

Examples

This example shows how to enable the debounce timer for a specific port on a specific module:

```
Console> (enable) set port debounce 1/1 enable
Debounce is enabled on port 1/1.
Warning:Enabling port debounce causes Link Up/Down detections to be delayed.
It results in loss of data traffic during debouncing period, which might
affect the convergence/reconvergence of various Layer 2 and Layer 3
protocols.
Use with caution.
Console> (enable)
```

Related Commands

show port debounce

set port disable

Use the **set port disable** command to disable a port or a range of ports.

set port disable *mod/port*

Syntax Description		
	mod/port	Number of the module and the port on the module.

Defaults

The default system configuration has all ports enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

It takes approximately 30 seconds for this command to take effect.

Examples

This example shows how to disable a port using the **set port disable** command:

```
Console> (enable) set port disable 5/10
Port 5/10 disabled.
Console> (enable)
```

Related Commands

set port enable
show port

set port dot1qtunnel

Use the **set port dot1qtunnel** command to configure the dot1q tunnel mode for the port.

set port dot1qtunnel *mod/port* {**access** | **disable**}

Syntax Description

mod/port	Number of the module and the port on the module.
access	Keyword to turn off the port's trunking mode.
disable	Keyword to disable dot1q tunneling.

Defaults

The default is dot1qtunnel is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You cannot enable the dot1q tunneling feature on a port until dot1q-tagged-only mode is enabled.

You cannot disable dot1q-tagged-only mode on the switch until dot1q tunneling is disabled on all the ports on the switch.

You cannot set the dot1q tunnel mode to access if port security is enabled.

You cannot set the dot1q tunnel mode to access on a port with an auxiliary VLAN configured.

An interconnected network can have redundant paths to the same edge switch of ISP, but it cannot have redundant paths to two different edge switches of ISP.

Note PBF does not work with 802.1Q tunnel traffic. PBF is supported on Layer 3 IP unicast traffic, but it is not applicable to Layer 2 traffic. At the intermediate (PBF) switch, all 802.1Q tunnel traffic appears as Layer 2 traffic.

Examples

This example shows how to set dot1q tunneling on the port to access:

```
Console> (enable) set port dot1qtunnel 4/1 access
Dot1q tunnel feature set to access mode on port 4/1.
Port 4/2 trunk mode set to off.
Console> (enable)
```

This example shows the output if you try to turn on trunking on a port that has dot1q tunneling mode set:

```
Console> (enable) set trunk 4/1 on
Failed to set port 4/1 to trunk mode on.
The dot1q tunnel mode for the port is currently set to access.
Console> (enable)
```

Related Commands show port dot1qtunnel

set port dot1x

Use the **set port dot1x** command to configure dot1x on a port.

set port dot1x *mod/port* **multiple-host** {**enable** | **disable**}

set port dot1x *mod/port* {**port-control** *port_control_value*}

set port dot1x *mod/port* {**initialize** | **re-authenticate**}

set port dot1x *mod/port* **re-authentication** {**enable** | **disable**}

Syntax Description

mod/port	Number of the module and port on the module.
multiple-host	Keyword to specify multiple-user access; see the "Usage Guidelines" section for additional information.
enable	Keyword to enable multiple-user access.
disable	Keyword to disable multiple-user access.
port-control *port_control_value*	Keyword and variable to specify the port control type; valid values are **force-authorized**, **force-unauthorized**, and **auto**.
initialize	Keyword to initialize dot1x on the port.
re-authenticate	Keyword to manually initiate a reauthentication of the entity connected to the port.
re-authentication	Keyword to automatically initiate reauthentication of the entity connected to the port within the reauthentication time period; see the "Usage Guidelines" section for more information.
enable	Keyword to enable automatic reauthentication.
disable	Keyword to disable automatic reauthentication.

Defaults

The default settings are as follows:

- The default *port_control_value* is **force-authorized**.
- The multiple host feature is disabled.
- The reauthentication feature is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The dot1x port will not be allowed to become a trunk port, MVAP, channel port, dynamic port, or a secure port.

When setting the port control type, the following applies:

- **force-authorized** forces the controlled port to transition to the authorized state unconditionally and is equivalent to disabling 802.1x restriction in the port.
- **force-unauthorized** forces the controlled port to transit to the unauthorized state unconditionally and prevents the authorized services of the authenticator to the supplicant.
- **auto** enables 802.1x control on the port.

If you disable the multiple host feature, once a dot1x port is authorized through a successful authentication of a supplicant, only that particular host (MAC address) is allowed on that port. When the system detects another host (different MAC address) on the authorized port, it shuts down the port and displays a syslog message. This is the default system behavior.

If you enable the multiple host feature, once a dot1x port is authorized through a successful authentication of a supplicant, any host (any MAC address) is allowed to send or receive traffic on that port.

If you enable reauthentication, you can set the reauthentication time period in seconds by entering the **set dot1x re-authperiod** *seconds* command. The default for the reauthentication time period is 3600 seconds.

Examples

This example shows how to set the port control type automatically:

```
Console> (enable) set port dot1x 4/1 port-control auto
Port 4/1 dot1x port-control is set to auto.
Console> (enable)
```

This example shows how to initialize dot1x on a port:

```
Console> (enable) set port dot1x 4/1 initialize
dot1x port 4/1 initializing...
dot1x initialized on port 4/1.
Console> (enable)
```

This example shows how to manually reauthenticate a port:

```
Console> (enable) set port dot1x 4/1 re-authenticate
dot1x port 4/1 re-authenticating...
dot1x re-authentication successful...
dot1x port 4/1 authorized.
Console> (enable)
```

This example shows how to enable multiple-user access on a specific port:

```
Console> (enable) set port dot1x 4/1 multiple-host enable
Multiple hosts allowed on port 4/1.
Console> (enable)
```

This example shows how to enable automatic reauthentication on a port:

```
Console> (enable) set port dot1x 4/1 re-authentication enable
Port 4/1 re-authentication enabled.
Console> (enable)
```

Related Commands

set dot1x
show dot1x
show port dot1x

set port duplex

Use the **set port duplex** command to configure the duplex type of an Ethernet port or a range of ports.

set port duplex *mod/port* {**full** | **half**}

Syntax Description

mod/port	Number of the module and the port on the module.
full	Keyword to specify full-duplex transmission.
half	Keyword to specify half-duplex transmission.

Defaults

The default configuration for 10-Mbps and 100-Mbps modules has all Ethernet ports set to half duplex.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can configure Ethernet and Fast Ethernet interfaces to either full duplex or half duplex.

The **set port duplex** command is not supported on Gigabit Ethernet ports. Gigabit Ethernet ports support full-duplex mode only.

If the transmission speed on a 16-port RJ-45 Gigabit Ethernet port is set to 1000, duplex mode is set to full. If the transmission speed is changed to 10 or 100, the duplex mode stays at full. You must configure the correct duplex mode when transmission speed is changed to 10 or 100 from 1000.

Examples

This example shows how to set port 1 on module 2 to full duplex:

```
Console> (enable) set port duplex 2/1 full
Port 2/1 set to full-duplex.
Console> (enable)
```

Related Commands

show port

set port enable

Use the **set port enable** command to enable a port or a range of ports.

set port enable *mod/port*

Syntax Description

mod/port	Number of the module and the port on the module.

Defaults

The default is all ports are enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

It takes approximately 30 seconds for this command to take effect.

Examples

This example shows how to enable port 3 on module 2:

```
Console> (enable) set port enable 2/3
Port 2/3 enabled.
Console> (enable)
```

Related Commands

set port disable
show port

set port flowcontrol

Use the **set port flowcontrol** command to configure a port to send or receive pause frames. Pause frames are special packets that signal a source to stop sending frames for a specific period of time because the buffers are full.

set port flowcontrol *mod/port* {**receive** | **send**} {**off** | **on** | **desired**}

Syntax Description

mod/port	Number of the module and the port on the module.
receive	Keyword to specify a port processes pause frames.
send	Keyword to specify a port sends pause frames.
off	Keyword to prevent a local port from receiving and processing pause frames from remote ports or from sending pause frames to remote ports.
on	Keyword to enable a local port to receive and process pause frames from remote ports or send pause frames to remote ports.
desired	Keyword to obtain predictable results regardless of whether a remote port is set to **on**, **off**, or **desired**.

Defaults

Flow-control defaults vary depending upon port speed:

- Gigabit Ethernet ports default to **off** for receive (Rx) and **desired** for transmit (Tx)
- Fast Ethernet ports default to **off** for receive and **on** for transmit

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.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

When you configure the 24-port 100BASE-FX and 48-port 10/100 BASE-TX RJ-45 modules, you can set the receive flow control to **on** or **off** and the send flow control to **off**.

All Catalyst Gigabit Ethernet ports can receive and process pause frames from remote devices.

To obtain predictable results, use 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**.

Table 2-15 describes guidelines for different configurations of the **send** and **receive** keywords.

Table 2-15 send and receive Keyword Configurations

Configuration	Description
send on	Enables a local port to send pause frames to remote ports.
send off	Prevents a local port from sending pause frames to remote ports.
send desired	Obtains predictable results whether a remote port is set to **receive on**, **receive off**, or **receive desired**.
receive on	Enables a local port to process pause frames that a remote port sends.
receive off	Prevents a local port from sending pause frames to remote ports.
receive desired	Obtains predictable results whether a remote port is set to **send on**, **send off**, or **send desired**.

Examples

This example shows how to configure port 1 of module 5 to receive and process pause frames:

```
Console> (enable) set port flowcontrol receive 5/1 on
Port 5/1 flow control receive administration status set to on
(port will require far end to send flowcontrol)
Console> (enable)
```

This example shows how to configure port 1 of module 5 to receive and process pause frames if the remote port is configured to send pause frames:

```
Console> (enable) set port flowcontrol receive 5/1 desired
Port 5/1 flow control receive administration status set to desired
(port will allow far end to send flowcontrol if far end supports it)
Console> (enable)
```

This example shows how to configure port 1 of module 5 to receive but NOT process pause frames on port 1 of module 5:

```
Console> (enable) set port flowcontrol receive 5/1 off
Port 5/1 flow control receive administration status set to off
(port will not allow far end to send flowcontrol)
Console> (enable)
```

This example shows how to configure port 1 of module 5 to send pause frames:

```
Console> (enable) set port flowcontrol send 5/1 on
Port 5/1 flow control send administration status set to on
(port will send flowcontrol to far end)
Console> (enable)
```

This example shows how to configure port 1 of module 5 to send pause frames and yield predictable results even if the remote port is set to **receive off**:

```
Console> (enable) set port flowcontrol send 5/1 desired
Port 5/1 flow control send administration status set to desired
(port will send flowcontrol to far end if far end supports it)
Console> (enable)
```

Related Commands **show port flowcontrol**

set port gmrp

Use the **set port gmrp** command to enable or disable GMRP on the specified ports in all VLANs.

set port gmrp *mod/port* {**enable** | **disable**}

Syntax Description

mod/port	Number of the module and the port on the module.
enable	Keyword to enable GVRP on a specified port.
disable	Keyword to disable GVRP on a specified port.

Defaults

The default is GMRP is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

You can enter this command even when GMRP is not enabled, but the values come into effect only when you enable GMRP using the **set gmrp enable** command.

Examples

This example shows how to enable GMRP on module 3, port 1:

```
Console> (enable) set port gmrp 3/1 enable
GMRP enabled on port(s) 3/1.
GMRP feature is currently disabled on the switch.
Console> (enable)
```

This example shows how to disable GMRP on module 3, ports 1 through 5:

```
Console> (enable) set port gmrp 3/1-5 disable
GMRP disabled on port(s) 3/1-5.
Console> (enable)
```

Related Commands

show gmrp configuration

set port gvrp

Use the **set port gvrp** command to enable or disable GVRP on the specified ports in all VLANs.

set port gvrp *mod/port* {**enable** | **disable**}

Syntax Description

mod/port	Number of the module and the port on the module.
enable	Keyword to enable GVRP on a specified port.
disable	Keyword to disable GVRP on a specified port.

Defaults

The default is GVRP is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

When you enable VTP pruning, it runs on all the GVRP-disabled trunks.

To run GVRP on a trunk, you need to enable GVRP both globally on the switch and individually on the trunk.

You can configure GVRP on a port even when you globally enable GVRP. However, the port will not become a GVRP participant until you globally enable GVRP.

You can enable GVRP on an 802.1Q trunk only.

If you enter the **set port gvrp** command without specifying the port number, GVRP is affected globally in the switch.

Examples

This example shows how to enable GVRP on module 3, port 2:

```
Console> (enable) set port gvrp 3/2 enable
GVRP enabled on 3/2.
Console> (enable)
```

This example shows how to disable GVRP on module 3, port 2:

```
Console> (enable) set port gvrp 3/2 disable
GVRP disabled on 3/2.
Console> (enable)
```

This example shows what happens if you try to enable GVRP on a port that is not an 802.1Q trunk:

```
Console> (enable) set port gvrp 4/1 enable
Failed to set port 4/1 to GVRP enable. Port not allow GVRP.
Console> (enable)
```

This example shows what happens if you try to enable GVRP on a specific port when GVRP has not first been enabled using the **set gvrp** command:

```
Console> (enable) set port gvrp 5/1 enable
GVRP enabled on port(s) 5/1.
GVRP feature is currently disabled on the switch.
Console> (enable)
```

Related Commands

clear gvrp statistics
set gvrp
show gvrp configuration

set port host

Use the **set port host** command to optimize the port configuration for a host connection.

set port host *mod/port*

Syntax Description

mod/port	Number of the module and the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

To optimize the port configuration, the **set port host** command sets channel mode to off, enables spanning tree PortFast, sets the trunk mode to off, and disables the dot1q tunnel feature. Only an end station can accept this configuration.

Because spanning tree PortFast is enabled, you should enter the **set port host** command only on ports connected to a single host. Connecting hubs, concentrators, switches, and bridges to a fast-start port can cause temporary spanning tree loops.

Enable the **set port host** command to decrease the time it takes to start up packet forwarding.

Examples

This example shows how to optimize the port configuration for end station/host connections on ports 2/1 and 3/1:

```
Console> (enable) set port host 2/1,3/1

Warning: Span tree port fast start should only be enabled on ports connected to a single
host.  Connecting hubs, concentrators, switches, bridges, etc. to a fast start port can
cause temporary spanning tree loops.  Use with caution.

Spantree ports 2/1,3/1 fast start enabled.
Dot1q tunnel feature disabled on port(s)  4/1.
Port(s) 2/1,3/1 trunk mode set to off.
Port(s) 2/1 channel mode set to off.

Console> (enable)
```

Related Commands

clear port host

set port inlinepower

Use the **set port inlinepower** command to set the inline power mode of a port or group of ports.

set port inlinepower *mod/port* {**off** | **auto**}

Syntax Description

mod/port	Number of the module and the port on the module.
off	Keyword to not power up the port even if an unpowered phone is connected.
auto	Keyword to power up the port only if the switching module has discovered the phone.

Defaults

The default is **auto**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

If you enter this command on a port that does not support the IP phone power feature, an error message is displayed.

You can enter a single port or a range of ports, but you cannot enter the module number only.

An inline power-capable device can still be detected even if the inlinepower mode is set to off.

Caution Damage can occur to equipment connected to the port if you are not using a phone that can be configured for the IP phone phantom power feature.

Examples

This example shows how to set the inlinepower to off:

```
Console> (enable) set port inlinepower 2/5 off
Inline power for port 2/5 set to off.
Console> (enable)
```

This example shows the output if the inlinepower feature is not supported:

```
Console> (enable) set port inlinepower 2/3-9 auto
Feature not supported on module 2.
Console> (enable)
```

Related Commands

set inlinepower defaultallocation
show environment
show port inlinepower

set port jumbo

Use the **set port jumbo** command to enable or disable the jumbo frame feature on a per-port basis.

set port jumbo *mod/port* {**enable** | **disable**}

Syntax Description

mod/port	Number of the module and the port on the module.
enable	Keyword to enable jumbo frames on a specified port.
disable	Keyword to disable jumbo frames on a specified port.

Defaults

If you enable the jumbo frame feature, the MTU size for packet acceptance is 9216 bytes for nontrunking ports.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

You can use the jumbo frame feature to transfer large frames or jumbo frames through Catalyst 6000 family switches to optimize server-to-server performance.

The MSFC and MSM do not support the routing of jumbo frames; if jumbo frames are sent to these routers, router performance is significantly degraded.

The MSFC2 supports routing of jumbo frames. The GSR supports jumbo frames.

The jumbo frame feature is supported on any Ethernet port.

For information on how to set the jumbo frame MTU size, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com.

Examples

This example shows how to enable the jumbo frames feature on module 3, port 2:

```
Console> (enable) set port jumbo 3/2 enable
Jumbo frames enabled on port 5/3.
Console> (enable)
```

This example shows how to disable the jumbo frames feature on module 3, port 2:

```
Console> (enable) set port jumbo 3/2 disable
Jumbo frames disabled on port 3/2.
Console> (enable)
```

Related Commands

set trunk
show port jumbo

set port lacp-channel

Use the **set port lacp-channel** command to set the priority value for physical ports, to assign an administrative key to a particular set of ports, or to change the channel mode for a set of ports that were previously assigned to the same administrative key.

set port lacp-channel *mod/ports* **port-priority** *value*

set port lacp-channel *mod/ports* [*admin-key*]

set port lacp-channel *mod/ports* **mode** {**on** | **off** | **active** | **passive**}

Syntax Description

mod/ports	Number of the module and the ports on the module.
port-priority	Keyword to specify the priority for physical ports.
value	Number of the port priority; valid values are from **1** to **255**. See the "Usage Guidelines" section for more information about the priority value.
admin-key	(Optional) Number of the administrative key; valid values are from **1** to **1024**. See the "Usage Guidelines" section for more information about the administrative key.
mode	Keyword to specify the channel mode for a set or ports.
on | **off** | **active** | **passive**	Keyword to specify the status of the channel mode.

Defaults

LACP is supported on all Ethernet interfaces.

The default port priority value is **128**.

The default mode for all ports that are assigned the administrative key is **passive**.

For differences between PAgP and LACP, refer to the "Guidelines for Port Configuration" section of the "Configuring EtherChannel" chapter of the *Catalyst 6000 Family Software Configuration Guide*.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command can only be used for ports belonging to LACP modules. This command cannot be used on ports running in PAgP mode.

Higher priority values correspond to lower priority levels.

The following usage guidelines apply when you assign an administrative key to ports:

- If you do not enter a value for the administrative key, the switch chooses a value automatically.
- If you choose a value for the administrative key, but this value is already used in your switch, all the ports associated with this value are moved to a new administrative key that is assigned automatically. The previously used value is now associated with new ports.

- You can assign a maximum of 8 ports to an administrative key.
- If you assign an administrative key to a channel that was previously assigned a particular mode, the channel will maintain that mode after you enter the administrative key value.

Examples

This example shows how to set the priority of ports 1/1 to 1/4 and 2/6 to 2/8 to 10:

```
Console> (enable) set port lacp-channel 4/1-4
Ports 4/1-4 being assigned admin key 96.
Console> (enable)
```

This example shows how to assign ports 4/1 to 4/4 to an administrative key that the switch automatically chooses:

```
Console> (enable) set port lacp-channel 4/1-4
Ports 4/1-4 being assigned admin key 96.
Console> (enable)
```

This example shows how to assign ports 4/4 to 4/6 to administrative key 96 when that key was previously assigned to ports 4/1 to 4/3:

```
Console> (enable) set port lacp-channel 4/4-6 96
admin key 96 already assigned to port 4/1-3.
Port(s) 4/1-3 being assigned to admin key 97.
Port(s) 4/4-6 being assigned to admin key 96.
Console> (enable)
```

Related Commands

clear lacp-channel statistics
set channelprotocol
set lacp-channel system-priority
set spantree channelcost
set spantree channelvlancost
show lacp-channel
show port lacp-channel

set port membership

Use the **set port membership** command to set the VLAN membership assignment to a port.

set port membership *mod/port* {**dynamic** | **static**}

Syntax Description

mod/port	Number of the module and the port on the module.
dynamic	Keyword to specify the port become a member of dynamic VLANs.
static	Keyword to specify the port become a member of static VLANs.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Dynamic VLAN support for VVID includes these restrictions to the following configuration of MVAP on the switch port:

- You can configure any VVID on a dynamic port including dot1p and untagged, except when the VVID is equal to dot1p or untagged. If this is the case, then you must configure VMPS with the MAC address of the IP phone. When you configure the VVID as dot1p or untagged on a dynamic port, this warning message displays:

  ```
  VMPS should be configured with the IP phone mac's.
  ```

- You cannot change the VVID of the port equal to PVID assigned by the VMPS for the dynamic port.
- You cannot configure trunk ports as dynamic ports, but you can configure MVAP as a dynamic port.

Examples

This example shows how to set the port membership VLAN assignment to **dynamic**:

```
Console> (enable) set port membership 5/5 dynamic
Port 5/5 vlan assignment set to dynamic.
Spantree port fast start option enabled for ports 5/5.
Console> (enable)
```

This example shows how to set the port membership VLAN assignment to **static**:

```
Console> (enable) set port membership 5/5 static
Port 5/5 vlan assignment set to static.
Console> (enable)
```

Related Commands

set pvlan
set pvlan mapping
set vlan
set vlan mapping

set port name

Use the **set port name** command to configure a name for a port.

set port name *mod/port* [*port_name*]

Syntax Description

mod/port	Number of the module and the port on the module.
port_name	(Optional) Name of the module.

Defaults

The default is no port name is configured for any port.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

If you do not specify the name string, the port name is cleared.

Examples

This example shows how to set port 1 on module 4 to Snowy:

```
Console> (enable) set port name 4/1 Snowy
Port 4/1 name set.
Console> (enable)
```

Related Commands

show port

set port negotiation

Use the **set port negotiation** command to enable or disable the link negotiation protocol on the specified port.

set port negotiation *mod/port* {**enable** | **disable**}

Syntax Description

mod/port	Number of the module and the port on the module.
enable	Keyword to enable the link negotiation protocol.
disable	Keyword to disable the link negotiation protocol.

Defaults

The default is link negotiation protocol is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set port negotiation** command is supported on Gigabit Ethernet ports only, except on WS-X6316-GE-TX and on WS-X6516-GE-TX

If the port does not support this command, this message appears:

```
Feature not supported on Port N/N.
```

where N/N is the module and port number.

In most cases, when you enable link negotiation, the system autonegotiates flow control, duplex mode, and remote fault information. The exception applies to 16-port 10/100/1000BASE-T Ethernet modules; when you enable link negotiation on these Ethernet modules, the system autonegotiates flow control only.

You must either enable or disable link negotiation on both ends of the link. Both ends of the link must be set to the same value or the link cannot connect.

Examples

This example shows how to disable link negotiation protocol on port 1, module 4:

```
Console> (enable) set port negotiation 4/1 disable
Link negotiation protocol disabled on port 4/1.
Console> (enable)
```

Related Commands

show port negotiation

set port protocol

Use the **set port protocol** command to enable or disable protocol membership of ports.

set port protocol *mod/port* {**ip** | **ipx** | **group**} {**on** | **off** | **auto**}

Syntax Description

mod/port	Number of the module and the port on the module.
ip	Keyword to specify IP.
ipx	Keyword to specify IPX.
group	Keyword to specify VINES, AppleTalk, and DECnet protocols.
on	Keyword to indicate the port will receive all the flood traffic for that protocol.
off	Keyword to indicate the port will not receive any flood traffic for that protocol.
auto	Keyword to specify that the port is added to the group only after packets of the specific protocol are received on that port.

Defaults

The default is that the ports are configured to **on** for the IP protocol groups and **auto** for IPX and group protocols.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

Protocol filtering is supported only on nontrunking EtherChannel ports. Trunking ports are always members of all the protocol groups.

If the port configuration is set to **auto**, the port initially does not receive any flood packets for that protocol. When the corresponding protocol packets are received on that port, the supervisor engine detects this and adds the port to the protocol group.

Ports configured as **auto** are removed from the protocol group if no packets are received for that protocol within a certain period of time. This aging time is set to 60 minutes. They are also removed from the protocol group on detection of a link down.

Examples

This example shows how to disable IPX protocol membership of port 1 on module 2:

```
Console> (enable) set port protocol 2/1 ipx off
IPX protocol disabled on port 2/1.
Console> (enable)
```

This example shows how to enable automatic IP membership of port 1 on module 5:

```
Console> (enable) set port protocol 5/1 ip auto
IP protocol set to auto mode on module 5/1.
Console> (enable)
```

Related Commands

show port protocol

set port qos

Use the **set port qos** command to specify whether an interface is interpreted as a physical port or as a VLAN.

set port qos *mod/ports...* **port-based** | **vlan-based**

Syntax Description

mod/ports...	Number of the module and the ports on the module.
port-based	Keyword to interpret the interface as a physical port.
vlan-based	Keyword to interpret the interface as part of a VLAN.

Defaults

The default is ports are port-based if QoS is enabled and VLAN-based if QoS is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

Changing a port from port-based QoS-to-VLAN-based QoS detaches all ACLs from the port. Any ACLs attached to the VLAN apply to the port immediately.

When you set a port to VLAN-based QoS using the **set port qos** command with RSVP or COPS QoS enabled on that port, the QoS policy-source is COPS or DSBM-election is enabled. The VLAN-based setting has been saved in NVRAM only.

Examples

This example shows how to specify an interface as a physical port:

```
Console> (enable) set port qos 1/1-2 port-based
Updating configuration ...
QoS interface is set to port-based for ports 1/1-2.
Console> (enable)
```

This example shows how to specify an interface as a VLAN:

```
Console> (enable) set port qos 3/1-48 vlan-based
Updating configuration ...
QoS interface is set to VLAN-based for ports 3/1-48.
Console> (enable)
```

This example shows the output if you change from port-based QoS-to-VLAN-based QoS with either RSVP or COPS enabled on the port:

```
Console> (enable) set port qos 3/1-48 vlan
Qos interface is set to vlan-based for ports 3/1-48
Port(s) 3/1-48 - QoS policy-source is Cops or DSBM-election is enabled.
Vlan-based setting has been saved in NVRAM only.
Console> (enable)
```

Related Commands

set port qos cos
set port qos trust
show port qos
show qos info

set port qos cos

Use the **set port qos cos** command to set the default value for all packets that have arrived through an untrusted port.

set port qos *mod/ports* **cos** *cos_value*

set port qos *mod/ports* **cos-ext** *cos_value*

Syntax Description

mod/ports	Number of the module and ports.
cos *cos_value*	Keyword and variable to specify the CoS value for a port; valid values are from **0** to **7**.
cos-ext *cos_value*	Keyword and variable to specify the CoS extension for a phone port; valid values are from **0** to **8**.

Defaults

The default is CoS 3.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

If the default is enforced when you disable QoS, CoS is enforced when you enable QoS.

Examples

This example shows how to set the CoS default value on a port:

```
Console> (enable) set port qos 2/1 cos 3
Port 2/1 qos cos set to 3.
Console> (enable)
```

This example shows how to set the CoS-ext default value on a port:

```
Console> (enable) set port qos 2/1 cos-ext 3
Port 2/1 qos cos-ext set to 3.
Console> (enable)
```

Related Commands

clear port qos cos
set port qos
set port qos trust
show port qos
show qos info

set port qos policy-source

Use the **set port qos policy-source** command to set the QoS policy source for all ports in the specified module.

set port qos policy-source *mod/ports...* **local** | **cops**

Syntax Description

mod/ports...	Number of the module and the ports on the module.
local	Keyword to set the policy source to local NVRAM configuration.
cops	Keyword to set the policy source to COPS configuration.

Defaults

The default is all ports are set to local.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you set the policy source to **local**, the QoS policy is taken from local configuration stored in NVRAM. If you set the policy source to local after it was set to COPS, the QoS policy reverts back to the local configuration stored in NVRAM.

Examples

This example shows how to set the policy source to local NVRAM:

```
Console> (enable) set port qos 5/5 policy-source local
QoS policy source set to local on port(s) 5/1-48.
Console> (enable)
```

This example shows the output if you attempt to set the policy source to COPS and no COPS servers are available:

```
Console> (enable) set port qos 5/5 policy-source cops
QoS policy source for the switch set to COPS.
Warning: No COPS servers configured. Use the 'set cops server' command
to configure COPS servers.
Console> (enable)
```

This example shows the output if you set the policy source to COPS and the switch is set to local configuation (using the **set qos policy-source** command):

```
Console> (enable) set port qos 5/5 policy-source cops
QoS policy source set to COPS on port(s) 5/1-48.
Warning: QoS policy source for the switch set to use local configuration.
Console> (enable)
```

Related Commands

clear qos config
show port qos

set port qos trust

Use the **set port qos trust** command to set the trusted state of a port; for example, whether the packets arriving at a port are trusted to carry the correct classification.

set port qos *mod/ports...* **trust** {**untrusted** | **trust-cos** | **trust-ipprec** | **trust-dscp**}

Syntax Description

mod/ports...	Number of the module and the ports on the module.
untrusted	Keyword to specify that packets need to be reclassified from the matching ACE.
trust-cos	Keyword to specify that although the CoS bits in the incoming packets are trusted, the ToS is invalid and a valid value needs to be derived from the CoS bits.
trust-ipprec	Keyword to specify that although the ToS/CoS bits in the incoming packets are trusted, the ToS is invalid and the ToS is set as IP precedence.
trust-dscp	Keyword to specify that the ToS/CoS bits in the incoming packets can be accepted as is with no change.

Defaults

The default is **untrusted**; when you disable QoS, the default is **trust-cos** on Layer 2 switches and **trust-dscp** on Layer 3 switches.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you disable QoS, the default is **trust-cos** on Layer 2 switches and **trust-dscp** on Layer 3 switches.

This command is not supported by the NAM.

On 10/100 ports, you can use only the **set port qos trust** command to activate the receive-drop thresholds. To configure a trusted state, you have to convert the port to port-based QoS, define an ACL that defines all (or the desired subset) of ACEs to be trusted, and attach the ACL to that port.

Examples

This example shows how to set the port to a trusted state:

```
Console> (enable) set port qos 3/7 trust trust-cos
Port 3/7 qos set to trust-cos.
Console> (enable)
```

This example shows the output if you try to set the trust state on a 10/100 port:

```
Console> (enable) set port qos 3/28 trust trust-cos
Trust type trust-cos not supported on this port.
Receive thresholds are enabled on port 3/28.
Port  3/28 qos set to untrusted.
Console> (enable)
```

Related Commands

- set port qos
- set port qos cos
- show port qos
- show qos info

set port qos trust-ext

Use the **set port qos trust-ext** command to configure the access port on a Cisco IP phone connected to the switch port.

set port qos *mod/ports...* **trust-ext** {**trusted** | **untrusted**}

Syntax Description

mod/ports...	Number of the module and the ports on the module.
trusted	Keyword to specify that all traffic received through the access port passes through the phone switch unchanged.
untrusted	Keyword to specify that all traffic in 802.1Q or 802.1p frames received through the access port is marked with a configured Layer 2 CoS value.

Defaults

The default when the phone is connected to a Cisco LAN switch is untrusted mode; trusted mode is the default when the phone is not connected to a Cisco LAN switch.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

Traffic in frame types other than 802.1Q or 802.1p passes through the phone switch unchanged, regardless of the access port trust state.

Examples

This example shows how to set the trust extension on ports on the connected phone to a trusted state:

```
Console> (enable) set port qos 3/7 trust-ext trusted
Port in the phone device connected to port 3/7 is configured to be trusted.
Console> (enable)
```

Related Commands

set port qos
set port qos cos
show qos info
show port qos

set port rsvp dsbm-election

Use the **set port rsvp dsbm-election** command to specify whether or not the switch participates in the DSBM election on that particular segment.

set port rsvp *mod/port* **dsbm-election enable** | **disable** [*dsbm_priority*]

Syntax Description

mod/port	Number of the module and the port.
enable	Keyword to enable participation in the DSBM election.
disable	Keyword to disable participation in the DSBM election.
dsbm_priority	(Optional) DSBM priority; valid values are from **128** to **255**.

Defaults

The default is DSBM is disabled; the default *dsbm_priority* is 128.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

Examples

This example shows how to enable participation in the DSBM election:

```
Console> (enable) set port rsvp 2/1,3/2 dsbm-election enable 232
DSBM election enabled for ports 2/1,3/2.
DSBM priority set to 232 for ports 2/1,3/2.
This DSBM priority will be used during the next election process.
Console> (enable)
```

This example shows how to disable participation in the DSBM election:

```
Console> (enable) set port rsvp 2/1 dsbm-election disable
DSBM election disabled for ports(s)  2/1.
Console> (enable)
```

This example shows the output when you enable participation in the DSBM election on a port that is not forwarding:

```
Console> (enable) set port rsvp 2/1,3/2 dsbm-election enable 232
DSBM enabled and priority set to 232 for ports 2/1,3/2.
Warning: Port 2/1 not forwarding. DSBM negotiation will start after port starts forwarding
on the native vlan.
Console> (enable)
```

Related Commands

show port rsvp

set port security

Use the **set port security** command to configure port security on a port or range of ports.

set port security *mod/port...* [**enable** | **disable**] [*mac_addr*] [**age** {*age_time*}] [**maximum** {*num_ of_mac*}] [**shutdown** {*shutdown_time*}] [**violation** {**shutdown** | **restrict**}]

Syntax Description

mod/port...	Number of the module and the port on the module.
enable	(Optional) Keyword to enable port security.
disable	(Optional) Keyword to disable port security.
mac_addr	(Optional) Secure MAC address of the enabled port.
age *age_time*	(Optional) Keyword and variable to specify the duration for which addresses on the port will be secured; valid values are **0** (to disable) and from **1** to **1440** (minutes).
maximum *num_of_mac*	(Optional) Keyword and variable to specify the maximum number of MAC addresses to secure on the port; valid values are from **1** to **1025**.
shutdown *shutdown_time*	(Optional) Keyword and variable to specify the duration for which a port will remain disabled in case of a security violation; valid values are **0** (to disable) and from **1** to **1440** (minutes).
violation	(Optional) Keyword to specify the action to be taken in the event of a security violation.
shutdown	Keyword to shut down the port in the event of a security violation.
restrict	Keyword to restrict packets from unsecure hosts.

Defaults

The default port security configuration is as follows:

- Port security is disabled.
- Number of secure addresses per port is one.
- Violation action is shutdown.
- Age is permanent (addresses are not aged out).
- Shutdown time is indefinite.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

If you enter the **set port security enable** command but do not specify a MAC address, the first MAC address seen on the port becomes the secure MAC address.

You can specify the number of MAC addresses to secure on a port. You can add MAC addresses to this list of secure addresses. The maximum number is 1024.

The **set port security violation** command allows you to specify whether you want the port to shut down or to restrict access to insecure MAC addresses only. The shutdown time allows you to specify the duration of shutdown in the event of a security violation.

We recommend that you configure the age timer and the shutdown timer if you want to move a host from one port to another when port security is enabled on those ports. If the *age_time* value is less than or equal to the *shutdown_time* value, the moved host will function again in an amount of time equal to the *shutdown_time* value. The age timer begins upon learning the first MAC address, and the disable timer begins when there is a security violation.

Examples

This example shows how to set port security with a learned MAC address:

```
Console> (enable) set port security 3/1 enable
Port 3/1 port security enabled with the learned mac address.
Console> (enable)
```

This example shows how to set port security with a specific MAC address:

```
Console> (enable) set port security 3/1 enable 01-02-03-04-05-06
Port 3/1 port security enabled with 01-02-03-04-05-06 as the secure mac address.
Console> (enable)
```

This example sets the shutdown time to 600 minutes on port 7/7:

```
Console> (enable) set port security 7/7 shutdown 600
Secure address shutdown time set to 600 minutes for port 7/7.
Console> (enable)
```

This example sets the port to drop all packets that are coming in on the port from insecure hosts:

```
Console> (enable) set port security 7/7 violation restrict
Port security violation on port 7/7 will cause insecure packets to be dropped.
Console> (enable)
```

Related Commands

clear port security
show port security

set port speed

Use the **set port speed** command set to configure the speed of a port interface.

set port speed *mod/port* {**10** | **100** | **1000** | **auto**}

Syntax Description

mod/port	Number of the module and the port on the module.
10 | **100** | **1000**	Keyword to set a port speed for 10BASE-T, 100BASE-T, or 1000BASE-T ports.
auto	Keyword to specify autonegotiation for transmission speed and duplex mode on 10/100 Fast Ethernet ports.

Defaults

The default is **auto**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

In most cases, autonegotiation manages transmission speed, duplex mode, the master link, and the slave link. The exception applies to 16-port 10/100/1000BASE-T Ethernet modules, where autonegotiation manages transmission speed only.

You can configure Fast Ethernet interfaces on the 10/100-Mbps Fast Ethernet switching module to either 10, 100, or 1000 Mbps, or to autosensing mode, allowing the interfaces to sense and distinguish between 10- and 100-Mbps port transmission speeds and full-duplex or half-duplex port transmission types at a remote port connection. If you set the interfaces to autosensing, they configure themselves automatically to operate at the proper speed and transmission type.

Examples

This example shows how to configure port 1, module 2 to **auto**:

```
Console> (enable) set port speed 2/1 auto
Port 2/1 speed set to auto-sensing mode.
Console> (enable)
```

This example shows how to configure the port speed on port 2, module 2 to **10 Mbps**:

```
Console> (enable) set port speed 2/2 10
Port 2/2 speed set to 10 Mbps.
Console> (enable)
```

Related Commands

show port

set port sync-restart-delay

Use the **set port sync-restart-delay** command to specify a port's synchronization restart delay.

set port sync-restart-delay *mod/port delay*

Syntax Description

mod/port	Number of the module and the port on the module.
delay	Delay time in milliseconds; the delay range is **200** to **60000** ms (60 seconds).

Defaults

The default delay time is 210 ms.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Generally, the more DWDM equipment you have in the network, the longer the synchronization delay should be.

The **set port sync-restart-delay** and **show port sync-restart-delay** commands are available in both binary mode and text configuration mode.

Use the **clear config** command to reset the synchronization delay to 210 ms.

Related Commands

clear config
show port sync-restart-delay

set port trap

Use the **set port trap** command to enable or disable the operation of the standard SNMP link trap (up or down) for a port or range of ports.

set port trap *mod/port* {**enable** | **disable**}

Syntax Description

mod/port	Number of the module and the port on the module.
enable	Keyword to activate the SNMP link trap.
disable	Keyword to deactivate the SNMP link trap.

Defaults

The default is all port traps are disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

To set SNMP traps, enter the **set snmp trap** command.

Examples

This example shows how to enable the SNMP link trap for module 1, port 2:

```
Console> (enable) set port trap 1/2 enable
Port 1/2 up/down trap enabled.
Console> (enable)
```

Related Commands

show port trap

set port voice interface dhcp

Use the **set port voice interface dhcp** command to set the port voice interface for the DHCP, TFTP, and DNS servers.

set port voice interface *mod/port* **dhcp enable** [**vlan** *vlan*]

set port voice interface *mod/port* **dhcp disable** {*ipaddrspec*} {**tftp** *ipaddr*} [**vlan** *vlan*] [**gateway** *ipaddr*] [**dns** [*ipaddr*] [*domain_name*]]

Syntax Description

mod/port	Number of the module and the port on the module.
enable	Keyword to activate the SNMP link trap.
vlan *vlan*	(Optional) Keyword and variable to specify a VLAN interface; valid values are from **1** to **1005** and from **1025** to **4094**.
disable	Keyword to deactivate the SNMP link trap.
ipaddrspec	IP address and mask; see the "Usage Guidelines" section for format instructions.
tftp *ipaddr*	Keyword and variable to specify the number of the TFTP server IP address or IP alias in dot notation a.b.c.d.
gateway *ipaddr*	(Optional) Keyword and variable to specify the number of the gateway server IP address or IP alias in dot notation a.b.c.d.
dns	(Optional) Keyword to specify the DNS server.
ipaddr	(Optional) Number of the DNS IP address or IP alias in dot notation a.b.c.d.
domain_name	(Optional) Name of the domain.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The *ipaddrspec* format is {*ipaddr*} {*mask*} or {*ipaddr*}/{*mask*} {*mask*}. The *mask* is a dotted format (255.255.255.0) or number of bits (0 to 31).

You can specify a single port only when setting the IP address.

If you enable DHCP on a port, the port obtains all other configuration information from the TFTP server. When you disable DHCP on a port, the following mandatory parameters must be specified:

- If you do not specify DNS parameters, the software uses the system DNS configuration on the supervisor engine to configure the port.
- You cannot specify more than one port at a time because a unique IP address must be set for each port.

Examples

This example shows how to enable the port voice interface for the DHCP server:

```
Console> (enable) set port voice interface 7/4-8 dhcp enable
Port 7/4 DHCP enabled.
Console> (enable)
```

This example shows how to disable the set port voice interface DHCP server:

```
Console> (enable) set port voice interface 7/3 dhcp disable 171.68.111.41/24 tftp
173.32.43.11 dns 172.20.34.204 cisco.com
Port 7/3 dhcp disabled.
System DNS configurations applied.
Console> (enable)
```

This example shows how to enable the port voice interface for the DHCP server with a specified VLAN:

```
Console> (enable) set port voice interface 7/4-6 dhcp enable vlan 3
Vlan 3 configuration successful
Ports 7/4-6 DHCP enabled.
Console> (enable)
```

This example shows how to enable the port voice interface for the TFTP, DHCP, and DNS servers:

```
Console> (enable) set port voice interface dhcp enable 4/2 171.68.111.41 tftp 173.32.43.11
dhcp 198.98.4.1 dns 189.69.24.192
Port 4/2 interface set.
IP address: 171.68.111.41 netmask 255.255.0.0
TFTP server: 173.32.43.11
DHCP server: 198.98.4.1
DNS server: 189.69.24.192
Console> (enable)
```

This example shows how to enable a single port voice interface:

```
Console> (enable) set port voice interface 4/2-9 123.23.32.1/24
Single port must be used when setting the IP address.
Console> (enable)
```

Related Commands

show port voice interface

set power redundancy

Use the **set power redundancy** command to turn redundancy between the power supplies on or off.

set power redundancy {**enable** | **disable**}

Syntax Description

enable	Keyword to activate redundancy between the power supplies.
disable	Keyword to deactivate redundancy between the power supplies.

Defaults

The default is power redundancy is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

In a system with dual power supplies, this command turns redundancy between the power supplies on or off. In a redundant configuration, the power available to the system is the maximum power capability of the weakest supply.

In a nonredundant configuration, the power available to the system is the sum of the power capability of both supplies.

Examples

This example shows how to activate redundancy between power supplies:

```
Console> (enable) set power redundancy enable
Power supply redundancy enabled.
Console> (enable)
```

This example shows how to deactivate redundancy between power supplies:

```
Console> (enable) set power redundancy disable
Power supply redundancy disabled.
Console> (enable)
```

Related Commands

show environment
show system

set prompt

Use the **set prompt** command to change the prompt for the CLI.

set prompt *prompt_string*

Syntax Description

prompt_string	String to use as the command prompt.

Defaults

The default is the prompt is set to Console>.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use the **set system name** command to assign a name to the switch, the switch name is used as the prompt string. However, if you specify a different prompt string using the **set prompt** command, that string is used for the prompt.

Examples

This example shows how to set the prompt to system100>:

```
Console> (enable) set prompt system100>
system100> (enable)
```

Related Commands

set system name

set protocolfilter

Use the **set protocolfilter** command to activate or deactivate protocol filtering on Ethernet VLANs and on nontrunking Ethernet, Fast Ethernet, and Gigabit Ethernet ports.

set protocolfilter {**enable** | **disable**}

Syntax Description

enable	Keyword to activate protocol filtering.
disable	Keyword to deactivate protocol filtering.

Defaults

The default is protocol filtering is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

Protocol filtering is supported only on Ethernet VLANs and on nontrunking EtherChannel ports.

Examples

This example shows how to activate protocol filtering:

```
Console> (enable) set protocolfilter enable
Protocol filtering enabled on this switch.
Console> (enable)
```

This example shows how to deactivate protocol filtering:

```
Console> (enable) set protocolfilter disable
Protocol filtering disabled on this switch.
Console> (enable)
```

Related Commands

show protocolfilter

set pvlan

Use the **set pvlan** command to bind the isolated or community VLAN to the primary VLAN and assign the isolated or community ports to the private VLAN.

set pvlan *primary_vlan* {*isolated_vlan* | *community_vlan* | *twoway_community_vlan*} [*mod/port* | **sc0**]

Caution We recommend that you read and understand the "Configuring VLANs" chapter in the *Catalyst 6000 Family Software Configuration Guide* before using this command.

Syntax Description

primary_vlan	Number of the primary VLAN.
isolated_vlan	Number of the isolated VLAN.
community_vlan	Number of the community VLAN.
twoway_community_vlan	Number of the two-way community VLAN.
mod/port	(Optional) Module and port numbers of the isolated or community ports.
sc0	(Optional) Keyword to specify the inband port sc0.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You must set the primary VLAN, isolated VLAN, and community VLANs using the **set vlan pvlan-type** *pvlan_type* command before making the association with the **set pvlan** command.

Each isolated or community VLAN can have only one primary VLAN associated with it. A primary VLAN may have one isolated and/or multiple community VLANs associated to it.

Although you can configure sc0 as a private port, you cannot configure sc0 as a promiscuous port.

Examples

This example shows how to map VLANs 901, 902, and 903 (isolated or community VLANs) to VLAN 7 (the primary VLAN):

```
Console> (enable) set pvlan 7 901 4/3
Port 4/3 is successfully assigned to vlan 7, 901 and is made an isolated port.
Console> (enable) set pvlan 7 902 4/4-5
Ports 4/4-5 are successfully assigned to vlan 7, 902 and are made community ports.
Console> (enable) set pvlan 7 903 4/6-7
Ports 4/6-7 are successfully assigned to vlan 7, 903 and are made community ports.
Console> (enable) set pvlan 300 301 sc0
Successfully set the following ports to Private Vlan 300, 301:
sc0
Console> (enable)
```

Related Commands

clear config pvlan
clear pvlan mapping
clear vlan
set pvlan mapping
set vlan
show pvlan
show pvlan capability
show pvlan mapping
show vlan

set pvlan mapping

Use the **set pvlan mapping** command to map isolated or community VLANs to the primary VLAN on the promiscuous port.

set pvlan mapping *primary_vlan* {*isolated_vlan* | *community_vlan* | *twoway_community_vlan*} *mod/port*

Syntax Description

primary_vlan	Number of the primary VLAN.
isolated_vlan	Number of the isolated VLAN.
community_vlan	Number of the community VLAN.
twoway_community_vlan	Number of the two-way community VLAN.
mod/port	Module and port number of the promiscuous port.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You must set the primary VLAN, isolated VLANs, and community VLANs using the **set vlan pvlan-type** command bound with the **set pvlan** command, before you can apply the VLANs on any of the promiscuous ports with the **set pvlan mapping** command.

You should connect the promiscuous port to an external device for the ports in the private VLAN to communicate with any other device outside the private VLAN.

You should apply this command for each primary or isolated (community) association in the private VLAN.

Examples

This example shows how to remap community VLAN 903 to the primary VLAN 901 on ports 3 through 5 on module 8:

```
Console> (enable) set pvlan mapping 901 903 8/3-5
Successfully set mapping between 901 and 903 on 8/3-5.
Console> (enable)
```

Related Commands

clear pvlan mapping
clear vlan
set pvlan
set vlan
show pvlan
show pvlan mapping
show vlan

set qos

Use the **set qos** command to turn on or turn off QoS functionality on the switch.

set qos enable | **disable**

Syntax Description

enable	Keyword to activate QoS functionality.
disable	Keyword to deactivate QoS functionality.

Defaults

The default is QoS functionality is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Refer to the *Catalyst 6000 Family Software Configuration Guide* for information on how to change the QoS default configurations.

When you enable and disable QoS in quick succession, a bus timeout might occur.

If you enable or disable QoS on channel ports with different port types, channels might break or form.

Examples

This example shows how to enable QoS:

```
Console> (enable) set qos enable
QoS is enabled.
Console> (enable)Console> (enable)
```

This example shows how to disable QoS:

```
Console> (enable) set qos disable
QoS is disabled.
Console> (enable)
```

Related Commands

show qos info

set qos acl default-action

Use the **set qos acl default-action** command to set the ACL default actions.

set qos acl default-action ip {{**dscp** *dscp*} | **trust-cos** | **trust-ipprec** | **trust-dscp**} [{**microflow** *microflow_name*}] [{**aggregate** *aggregate_name*}]

set qos acl default-action ipx {{**dscp** *dscp*} | **trust-cos**} [{**microflow** *microflow_name*}] [{**aggregate** *aggregate_name*}]

set qos acl default-action {ipx | **mac}** {{**dscp** *dscp*} | **trust-cos**} [{**aggregate** *aggregate_name*}]

Syntax Description

ip	Keyword to specify the IP ACL default actions.
dscp *dscp*	Keyword and variable to set the DSCP to be associated with packets matching this stream.
trust-cos	Keyword to specify DSCP is derived from the packet CoS.
trust-ipprec	Keyword to specify DSCP is derived from the packet's IP precedence.
trust-dscp	Keyword to specify DSCP is contained in the packet already.
microflow *microflow_name*	(Optional) Keyword and variable to specify the name of the microflow policing rule to be applied to packets matching the ACE.
aggregate *aggregate_name*	(Optional) Keyword and variable to specify the name of the aggregate policing rule to be applied to packets matching the ACE.
ipx	Keyword to specify the IPX ACL default actions.
mac	Keyword to specify the MAC ACL default actions.

Defaults

The default is no ACL is set up. When you enable QoS, the default-action is to classify everything to best effort and to do no policing. When you disable QoS, the default-action is **trust-dscp** on all packets and no policing.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Configurations you make by entering this command are saved to NVRAM and the switch and do not require that you enter the **commit** command.

Examples

This example shows how to set up the IP ACL default actions:

```
Console> (enable) set qos acl default-action ip dscp 5 microflow micro aggregate agg
QoS default-action for IP ACL is set successfully.
Console> (enable)
```

This example shows how to set up the IPX ACL default actions:

```
Console> (enable) set qos acl default-action ipx dscp 5 microflow micro aggregate agg
QoS default-action for IPX ACL is set successfully.
Console> (enable)
```

This example shows how to set up the MAC ACL default actions:

```
Console> (enable) set qos acl default-action mac dscp 5 microflow micro aggregate agg
QoS default-action for MAC ACL is set successfully.
Console> (enable)
```

Related Commands

clear qos acl
show qos acl info

set qos acl ip

Use the **set qos acl ip** command to create or add IP access lists.

set qos acl ip {*acl_name*} {{**dscp** *dscp*} | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*] {*src_ip_spec*} [**precedence** *precedence* | **dscp-field** *dscp*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

set qos acl ip {*acl_name*} {{**dscp** *dscp*} | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*] {*protocol*} {*src_ip_spec*} {*dest_ip_spec*} [**precedence** *precedence* | **dscp-field** *dscp*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

set qos acl ip {*acl_name*} {{**dscp** *dscp*} | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*] **icmp** {*src_ip_spec*} {*dest_ip_spec*} [*icmp_type* [*icmp_code*] | *icmp_message*] [**precedence** *precedence* | **dscp-field** *dscp*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

set qos acl ip {*acl_name*} {{**dscp** *dscp*} | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*] **tcp** {*src_ip_spec*} [{*operator*} {*port*} [*port*]] {*dest_ip_spec*} [{*operator*} {*port*} [*port*]] [**established**] [**precedence** *precedence* | **dscp-field** *dscp*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

set qos acl ip {*acl_name*} {{**dscp** *dscp*} | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*] **udp** {*src_ip_spec*} [{*operator*} {*port*} [*port*]] {*dest_ip_spec*} [{*operator*} {*port*} [*port*]] [**precedence** *precedence* | **dscp-field** *dscp*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

set qos acl ip {*acl_name*} {{**dscp** *dscp*} | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*] **igmp** {*src_ip_spec*} {*dest_ip_spec*} [*igmp_type*] [**precedence** *precedence* | **dscp-field** *dscp*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

Syntax Description

acl_name	Unique name that identifies the list to which the entry belongs.
dscp *dscp*	Keyword and variable to set CoS and DSCP from configured DSCP values.
trust-cos	Keyword to specify DSCP is derived from the packet CoS.
trust-ipprec	Keyword to specify DSCP is derived from the packet's IP precedence.
trust-dscp	Keyword to specify DSCP is contained in the packet already.
microflow *microflow_name*	(Optional) Keyword and variable to specify the name of the microflow policing rule to be applied to packets matching the ACE.
aggregate *aggregate_name*	(Optional) Keyword and variable to specify the name of the aggregate policing rule to be applied to packets matching the ACE.
src_ip_spec	Source IP address and the source mask. See the "Usage Guidelines" section for the format.
before *editbuffer_index*	(Optional) Keyword and variable to insert the new ACE in front of another ACE.
modify *editbuffer_index*	(Optional) Keyword and variable to replace an ACE with the new ACE.

protocol	Keyword or number of an IP protocol; valid numbers are from **0** to **255** representing an IP protocol number. See the "Usage Guidelines" section for the list of valid keywords and corresponding numbers.
dest_ip_spec	Destination IP address and the destination mask. See the "Usage Guidelines" section for the format.
precedence *precedence*	(Optional) Keyword and variable to specify the precedence level to compare with an incoming packet; valid values are from **0** to **7** or by name. See the "Usage Guidelines" section for a list of valid names.
dscp-field *dscp*	(Optional) Keyword and variable to specify the DSCP field level to compare with an incoming packet. Valid values are from **0** to **7** or by name; valid names are **critical**, **flash**, **flash-override**, **immediate**, **internet**, **network**, **priority**, and **routine**.
icmp	Keyword to specify ICMP.
icmp-type	(Optional) ICMP message type; valid values are from **0** to **255**.
icmp-code	(Optional) ICMP message code; valid values are from **0** to **255**.
icmp-message	(Optional) ICMP message type name or ICMP message type and code name. See the "Usage Guidelines" section for a list of valid names.
tcp	Keyword to specify TCP.
operator	(Optional) Operands; valid values include **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range).
port	(Optional) TCP or UDP port number or name; valid port numbers are from **0** to **65535**. See the "Usage Guidelines" section for a list of valid names.
established	(Optional) For TCP protocol only—Keyword to specify an established connection.
udp	Keyword to specify UDP.
igmp	Keyword to specify IGMP.
igmp_type	(Optional) IGMP message type; valid values are from **0** to **15**.

Defaults

The default is there are no ACLs.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Configurations you make by entering any of these commands are saved to NVRAM and the switch only after you enter the **commit** command. Enter ACEs in batches and then enter the **commit** command to save them in NVRAM and the switch.

Use the **show qos acl info** command to view the edit buffer.

The **dscp** *dscp*, **trust-cos**, **trust-ipprec**, and **trust-dscp** keywords and variables are used to select a marking rule. Refer to the *Catalyst 6000 Family Software Configuration Guide* for additional marking rule information.

The optional **microflow** *microflow_name* and **aggregate** *aggregate_name* keywords and variables are used to configure policing in the ACE. Refer to the *Catalyst 6000 Family Software Configuration Guide* for additional policing rule information.

The *src_ip_spec*, optional **precedence** *precedence*, or **dscp-field** *dscp* keywords and variables are used to configure filtering.

When you enter the ACL name, follow these naming conventions:

- Maximum of 31 characters long 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

When you specify the source IP address and the source mask, use the form *source_ip_address source_mask* and follow these guidelines:

- The *source_mask* is required; 0 indicates a “care” bit, 1 indicates a “don’t-care” bit.
- Use a 32-bit quantity in four-part dotted-decimal format.
- Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.
- Use **host** source as an abbreviation for a *source* and *source-wildcard* of source 0.0.0.0.

When you enter a destination IP address and the destination mask, use the form *destination_ip_address destination_mask*. The destination mask is required.

- Use a 32-bit quantity in a four-part dotted-decimal format
- Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255
- Use **host**/source as an abbreviation for a *destination* and *destination-wildcard* of destination 0.0.0.0

Valid names for *precedence* are critical, flash, flash-override, immediate, internet, network, priority, and routine.

Valid names for *tos* are max-reliability, max-throughput, min-delay, min-monetary-cost, and normal.

Valid *protocol* keywords include **icmp** (1), **ip**, **ipinip** (4), **tcp** (6), **udp** (17), **igrp** (9), **eigrp** (88), **gre** (47), **nos** (94), **ospf** (89), **ahp** (51), **esp** (50), **pcp** (108), and **pim** (103). The IP protocol number is displayed in parentheses. Use the keyword **ip** to match any Internet Protocol.

ICMP packets that are matched by ICMP message type can also be matched by the ICMP message code.

Valid names for *icmp_type* and *icmp_code* are administratively-prohibited, alternate-address, conversion-error, dod-host-prohibited, dod-net-prohibited, echo, echo-reply, general-parameter-problem, host-isolated, host-precedence-unreachable, host-redirect, host-tos-redirect, host-tos-unreachable, host-unknown, host-unreachable, information-reply, information-request, mask-reply, mask-request, mobile-redirect, net-redirect, net-tos-redirect, net-tos-unreachable, net-unreachable, network-unknown, no-room-for-option, option-missing, packet-too-big, parameter-problem, port-unreachable, precedence-unreachable, protocol-unreachable, reassembly-timeout, redirect, router-advertisement, router-solicitation, source-quench, source-route-failed, time-exceeded, timestamp-reply, timestamp-request, traceroute, ttl-exceeded, and unreachable.

If the *operator* is positioned after the source and source-wildcard, it must match the source port. If the *operator* is positioned after the destination and destination-wildcard, it must match the destination port. The **range** operator requires two port numbers. All other operators require one port number only.

TCP port names can be used only when filtering TCP. Valid names for TCP ports are bgp, chargen, daytime, discard, domain, echo, finger, ftp, ftp-data, gopher, hostname, irc, klogin, kshell, lpd, nntp, pop2, pop3, smtp, sunrpc, syslog, tacacs-ds, talk, telnet, time, uucp, whois, and www.

UDP port names can be used only when filtering UDP. Valid names for UDP ports are biff, bootpc, bootps, discard, dns, dnsix, echo, mobile-ip, nameserver, netbios-dgm, netbios-ns, ntp, rip, snmp, snmptrap, sunrpc, syslog, tacacs-ds, talk, tftp, time, who, and xdmcp.

If no layer protocol number is entered, you can use this syntax:

set qos acl ip {*acl_name*} {**dscp** *dscp* | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*] {*src_ip_spec*} [**before** *editbuffer_index* | **modify** *editbuffer_index*]

If a Layer 4 protocol is specified, you can use this syntax:

set qos acl ip {*acl_name*} {**dscp** *dscp* | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*] {*protocol*} {*src_ip_spec*} {*dest_ip_spec*} [**precedence** *precedence* | **dscp-field** *dscp*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

If ICMP is used, you can use this syntax:

set qos acl ip {*acl_name*} {**dscp** *dscp* | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*] **icmp** {*src_ip_spec*} {*dest_ip_spec*} [*icmp_type* [*icmp_code*] | *icmp_message*] [**precedence** *precedence* | **dscp-field** *dscp*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

If TCP is used, you can use this syntax:

set qos acl ip {*acl_name*} {**dscp** *dscp* | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*] **tcp** {*src_ip_spec*} [{*operator*} {*port*} [*port*]] {*dest_ip_spec*} [{*operator*} {*port*} [*port*]] [**established**] [**precedence** *precedence* | **dscp-field** *dscp*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

If UDP is used, you can use this syntax:

set qos acl ip {*acl_name*} {**dscp** *dscp* | **trust-cos** | **trust-ipprec** | **trust-dscp**} [[**microflow** *microflow_name*] [**aggregate** *aggregate_name*] **udp** {*src_ip_spec*} [{*operator*} {*port*} [*port*]] {*dest_ip_spec*} [{*operator* {*port*} [*port*]] [**precedence** *precedence* | **dscp-field** *dscp*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

Examples

This example shows how to define a TCP access list:

```
Console> (enable) set qos acl ip my_acl trust-dscp microflow my-micro tcp 1.2.3.4
255.0.0.0 eq port 21 172.20.20.1 255.255.255.0
my_acl editbuffer modified. Use ‘commit’ command to apply changes.
Console> (enable)
```

This example shows how to define an ICMP access list:

```
Console> (enable) set qos acl ip icmp_acl trust-dscp my-micro icmp 1.2.3.4 255.255.0.0
172.20.20.1 255.255.255.0 precedence 3
my_acl editbuffer modified. Use ‘commit’ command to apply changes.
Console> (enable)
```

Related Commands

clear qos acl
commit
rollback
show qos acl info

set qos acl ipx

Use the **set qos acl ipx** command to define IPX access lists.

set qos acl ipx {*acl_name*} {**dscp** *dscp* | **trust-cos**} [**aggregate** *aggregate_name*] {*protocol*} {*src_net*} [*dest_net.*[*dest_node*] [[*dest_net_mask.*]*dest_node_mask*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

Syntax Description

acl_name	Unique name that identifies the list to which the entry belongs.
dscp *dscp*	Keyword and variable to set CoS and DSCP from configured DSCP values.
trust-cos	Keyword to specify that the DSCP is derived from the packet CoS.
aggregate *aggregate_name*	(Optional) Keyword and variable to specify the name of the aggregate policing rule to be applied to packets matching the ACE.
protocol	Keyword or number of an IPX protocol; valid values are from **0** to **255** representing an IPX protocol number. See the "Usage Guidelines" section for a list of valid keywords and corresponding numbers.
src_net	Number of the network from which the packet is being sent. See the "Usage Guidelines" section for format guidelines.
dest_net.	(Optional) Mask to be applied to destination-node. See the "Usage Guidelines" section for format guidelines.
dest_node	(Optional) Node on destination-network of the packet being sent.
dest_net_mask.	(Optional) Mask to be applied to the destination network. See the "Usage Guidelines" section for format guidelines.
dest_node_mask	(Optional) Mask to be applied to destination-node. See the "Usage Guidelines" section for format guidelines.
before *editbuffer_index*	(Optional) Keyword and variable to insert the new ACE in front of another ACE.
modify *editbuffer_index*	(Optional) Keyword and variable to replace an ACE with the new ACE.

Defaults

There are no default ACL mappings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **dscp** *dscp* and **trust-cos** keywords and variables are used to select a marking rule. Refer to the *Catalyst 6000 Family Software Configuration Guide* for additional marking rule information.

The **dscp** *dscp* and **trust-cos** keywords and variables are not supported on systems configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2).

The optional **aggregate** *aggregate_name* keyword and variable are used to configure policing in the ACE. Refer to the *Catalyst 6000 Family Software Configuration Guide* for additional policing rule information.

Use the **show security acl** command to display the list.

The *src_ip_spec*, optional **precedence** *precedence*, or **dscp-field** *dscp* keywords and variables, are used to configure filtering.

When you enter the ACL name, follow these naming conventions:

- Maximum of 31 characters long 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

Valid *protocol* keywords include **ncp** (17), **rip** (1), **sap** (4), and **spx** (5). The IP network number is listed in parentheses.

The *src_net* and *dest_net* variables are eight-digit hexadecimal numbers that uniquely identify network cable segments. When you specify the *src_net* or *dest_net*, use the following guidelines:

- It can be a number in the range 0 to FFFFFFFF. A network number of -1 or **any** matches all networks.
- You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.

The *dest_node* is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (xxxx.xxxx.xxxx).

The *destination_mask* is of the form N.H.H.H or H.H.H where N is the destination network mask and H is the node mask. It can be specified only when the destination node is also specified for the destination address.

The *dest_net_mask* is an eight-digit hexadecimal mask. Place ones in the bit positions you want to mask. The mask must be immediately followed by a period, which must in turn be immediately followed by destination-node-mask. You can enter this value only when *dest_node* is specified.

The *dest_node_mask* is a 48-bit value represented as a dotted triplet of 4-digit hexadecimal numbers (xxxx.xxxx.xxxx). Place ones in the bit positions you want to mask. You can enter this value only when *dest_node* is specified.

The *dest_net_mask* is an eight-digit hexadecimal number that uniquely identifies the network cable segment. It can be a number in the range 0 to FFFFFFFF. A network number of -1 or **any** matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA. Following are *dest_net_mask* examples:

- 123A
- 123A.1.2.3
- 123A.1.2.3 ffff.ffff.ffff
- 1.2.3.4 ffff.ffff.ffff.ffff

Examples

This example shows how to create an IPX ACE:

```
Console> (enable) set qos acl ipx my_IPXacl trust-cos aggregate my-agg -1
my_IPXacl editbuffer modified. Use `commit' command to apply changes.
Console> (enable)
```

Related Commands

clear qos acl
commit
rollback
show qos acl info

set qos acl mac

Use the **set qos acl mac** command to define MAC access lists.

set qos acl mac {*acl_name*} {**dscp** *dscp* | **trust-cos**} [**aggregate** *aggregate_name*] {*src_mac_addr_spec*} {*dest_mac_addr_spec*} [*ether-type*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

Syntax Description

acl_name	Unique name that identifies the list to which the entry belongs.
dscp *dscp*	Keyword and variable to set CoS and DSCP from configured DSCP values.
trust-cos	Keyword to specify that the DSCP is derived from the packet CoS.
aggregate *aggregate_name*	(Optional) Keyword and variable to specify the name of the aggregate policing rule to be applied to packets matching the ACE.
src_mac_addr_spec	Number of the source MAC address in the form *source_mac_address source_mac_address_mask*.
dest_mac_addr_spec	Number of the destination MAC address.
ether-type	(Optional) Name or number that matches the ethertype for Ethernet-encapsulated packets. See the "Usage Guidelines" section for a list of valid names and numbers.
before *editbuffer_index*	(Optional) Keyword and variable to insert the new ACE in front of another ACE.
modify *editbuffer_index*	(Optional) Keyword and variable to replace an ACE with the new ACE.

Defaults

There are no default ACL mappings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **dscp** *dscp* and **trust-cos** keywords and variables are used to select a marking rule. Refer to the *Catalyst 6000 Family Software Configuration Guide* for additional marking rule information.

The **dscp** *dscp* and **trust-cos** keywords and variables are not supported on systems configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2).

The optional **aggregate** *aggregate_name* keyword and variable are used to configure policing in the ACE. Refer to the *Catalyst 6000 Family Software Configuration Guide* for additional policing rule information.

When you enter the ACL name, follow these naming conventions:

- Maximum of 31 characters long 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

The *src_mac_addr_spec* is a 48-bit source MAC address and mask and entered in the form of *source_mac_address source_mac_address_mask* (for example, 08-11-22-33-44-55 ff-ff-ff-ff-ff-ff). Place ones in the bit positions you want to mask. When you specify the *src_mac_addr_spec*, follow these guidelines:

- The *source_mask* is required; 0 indicates a “care” bit, 1 indicates a “don’t-care” bit.
- Use a 32-bit quantity in 4-part dotted-decimal format.
- Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.
- Use **host** source as an abbreviation for a *source* and *source-wildcard* of source 0.0.0.0.

The *dest_mac_spec* is a 48-bit destination MAC address and mask and entered in the form of *dest_mac_address dest_mac_address_mask* (for example, 08-00-00-00-02-00/ff-ff-ff-00-00-00). Place ones in the bit positions you want to mask. The destination mask is mandatory. When you specify the *dest_mac_spec*, use the following guidelines:

- Use a 48-bit quantity in 6-part dotted-hexadecimal format for the source address and mask.
- Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 ff-ff-ff-ff-ff-ff.
- Use **host** source as an abbreviation for a *destination* and *destination-wildcard* of destination 0.0.0.0.

Valid names for ethertypes (and corresponding numbers) are Ethertalk (0x809B), AARP (0x8053), dec-mop-dump (0x6001), dec-mop-remote-console (0x6002), dec-phase-iv (0x6003), dec-lat (0x6004), dec-diagnostic-protocol (0x6005), dec-lavc-sca (0x6007), dec-amber (0x6008), dec-mumps (0x6009), dec-lanbridge (0x8038), dec-dsm (0x8039), dec-netbios (0x8040), dec-msdos (0x8041), banyan-vines-echo (0x0baf), xerox-ns-idp (0x0600), and xerox-address-translation (0x0601).

The *ether-type* is a 16-bit hexadecimal number written with a leading 0x.

Use the **show security acl** command to display the list.

Examples

This example shows how to create a MAC access list:

```
Console> (enable) set qos acl mac my_MACacl trust-cos aggregate my-agg any any

my_MACacl editbuffer modified. Use `commit' command to apply changes.
Console> (enable)
```

Related Commands

clear qos acl
commit
rollback
show qos acl info

set qos acl map

Use the **set qos acl map** command to attach an ACL to a specified port or VLAN.

set qos acl map *acl_name* {*mod/port* | *vlan*}

Syntax Description

acl_name	Name of the list to which the entry belongs.
mod/port	Number of the module and the port on the module.
vlan	Number of the VLAN; valid values are from **1** to **1005** and from **1025** to **4094**.

Defaults

There are no default ACL mappings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Caution This command may fail if you try to map an ACL to a VLAN and the NVRAM is full.

Caution Use the **copy** command to save the ACL configuration to Flash memory.

Examples

This example shows how to attach an ACL to a port:

```
Console> (enable) set qos acl map my_acl 2/1
ACL my_acl is attached to port 2/1.
Console> (enable)
```

This example shows how to attach an ACL to a VLAN:

```
Console> (enable) set qos acl map ftp_acl 4
ACL ftp_acl is attached to vlan 4.
Console> (enable)
```

This example shows what happens if you try to attach an ACL that has not been committed:

```
Console> (enable) set qos acl map new_acl 4
Commit ACL new_acl before mapping.
Console> (enable)
```

Related Commands

- clear qos acl
- commit
- rollback
- show qos acl map

set qos bridged-microflow-policing

Use the **set qos bridged-microflow-policing** command to enable or disable microflow policing of bridged packets on a per-VLAN basis.

set qos bridged-microflow-policing {**enable** | **disable**} *vlanlist*

Syntax Description

enable	Keyword to activate microflow policing functionality.
disable	Keyword to deactivate microflow policing functionality.
vlanlist	List of VLANs; valid values are from **1** to **1001** and from **1025** to **4094**.

Defaults

The default is intraVLAN QoS is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Layer 3 switching engine-based systems do not create NetFlow entries for bridged packets. Without a NetFlow entry, these packets cannot be policed at the microflow level. You must enter the **set qos bridged-microflow-policing enable** command if you want the bridged packets to be microflow policed.

This command is supported on systems configured with a Layer 3 switching engine only.

Examples

This example shows how to enable microflow policing:

```
Console> (enable) set qos bridged-microflow-policing enable 1-1000
QoS microflow policing is enabled for bridged packets on vlans 1-1000.
Console> (enable)
```

This example shows how to disable microflow policing:

```
Console> (enable) set qos bridged-microflow-policing disable 10
QoS microflow policing is disabled for bridged packets on VLAN 10.
Console> (enable)
```

Related Commands

show qos bridged-packet-policing

set qos cos-dscp-map

Use the **set qos cos-dscp map** command to set the CoS-to-DSCP mapping.

set qos cos-dscp-map *dscp1 dscp2... dscp8*

Syntax Description

dscp#	Number of the DSCP; 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 Mapping

CoS	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The CoS-to-DSCP map is used to map the CoS of packets arriving on trusted ports (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 switch has one map.

This command is supported on systems configured with a Layer 3 switching engine only.

Examples

This example shows how to set the CoS-to-DSCP mapping:

```
Console> (enable) set qos cos-dscp-map 20 30 1 43 63 12 13 8
QoS cos-dscp-map set successfully.
Console> (enable)
```

Related Commands

clear qos cos-dscp-map
show qos maps

set qos drop-threshold

Use the **set qos drop-threshold** command to program the transmit-queue and receive-queue drop thresholds on all ports in the system.

set qos drop-threshold 2q2t tx queue *q# thr1 thr2*

set qos drop-threshold {**1q4t** | **1p1q4t**} **rx queue** *q# thr1 thr2 thr3 thr4*

Syntax Description

2q2t tx	Keywords to specify the transmit-queue drop threshold.
1q4t | **1p1q4t rx**	Keywords to specify the receive-queue drop threshold.
queue *q#*	Keyword and variable to specify the queue; valid values are **1** and **2**.
thr1, thr2, thr3, thr4	Threshold percentage; valid values are from **1** to **100**.

Defaults

If you enable QoS, the following defaults apply:

- Transmit-queue drop thresholds:
  - Queue 1—80%, 100%
  - Queue 2—80%, 100%
- Receive-queue drop thresholds:
  - Queue 1—50%, 60%, 80%, 100% if the port is trusted
  - Queue 2—100%, 100%, 100%, 100% if the port is untrusted

If you disable QoS, the following defaults apply:

- Transmit-queue drop thresholds:
  - Queue 1—100%, 100%
  - Queue 2—100%, 100%
- Receive-queue drop thresholds: queue 1—100%, 100%, 100%, 100%

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The number preceding the **t** letter in the *port_type* (**2q2t**, **1q4t**, or **1p1q4t**) determines the number of threshold values the hardware supports. For example, with **2q2t**, the number of thresholds specified is two; with **1q4t** and **1p1q4t**, the number of thresholds specified is four. Due to the granularity of programming the hardware, the values set in hardware will be close approximations of the values provided.

The number preceding the **q** letter in the *port_type* determines the number of the queues that the hardware supports. For example, with **2q2t**, the number of queues specified is two; with **1q4t** and **1p1q4t**, the number of queues specified is four. The system defaults for the transmit queues attempt to keep the maximum latency through a port at a maximum of 10 ms.

The number preceding the **p** letter in the **1p1q4t** port types determines the threshold in the priority queue.

When you configure the drop threshold for **1p1q4t**, the drop threshold for the second queue is 100 percent and is not configurable.

The thresholds are all specified as percentages; 10 indicates a threshold when the buffer is 10 percent full.

The single-port ATM OC-12 module does not support transmit-queue drop thresholds.

Examples

This example shows how to assign the transmit-queue drop threshold:

```
Console> (enable) set qos drop-threshold 2q2t tx queue 1 40 80
Transmit drop thresholds for queue 1 set at 40% and 80%
Console> (enable)
```

These examples show how to assign the receive-queue drop threshold:

```
Console> (enable) set qos drop-threshold 1q4t rx queue 1 40 50 60 100
Receive drop thresholds for queue 1 set at 40% 50% 60% 100%
Console> (enable)

Console> (enable) set qos drop-threshold 1p1q4t rx queue 1 40 50 60 100
Receive drop thresholds for queue 1 set at 40% 50% 60% 100%
Console> (enable)
```

Related Commands

show qos info

set qos dscp-cos-map

Use the **set qos dscp-cos-map** command to set the DSCP-to-CoS mapping.

set qos dscp-cos-map *dscp_list:cos_value ...*

Syntax Description

dscp_list	Number of the DSCP; valid values are from **0** to **63**.
cos_value...	Number of the CoS; valid values are from **0** to **7**.

Defaults

The default DSCP-to-CoS configuration is listed in Table 2-17.

Table 2-17 DSCP-to-CoS Mapping

DSCP	0 to 7	8 to 15	16 to 23	24 to 31	32 to 39	40 to 47	48 to 55	56 to 63
CoS	0	1	2	3	4	5	6	7

Command Types

Switch command.

Command Modes

Privileged.

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 ports and contains a table of 64 DSCP values and their corresponding CoS values. The switch has one map.

This command is supported on systems configured with a Layer 3 switching engine only.

Examples

This example shows how to set the DSCP-to-CoS mapping:

```
Console> (enable) set qos dscp-cos-map 20-25:7 33-38:3
QoS dscp-cos-map set successfully.
Console> (enable)
```

Related Commands

clear qos map
show qos maps

set qos ipprec-dscp-map

Use the **set qos ipprec-dscp-map** command to set the IP precedence-to-DSCP map. This command applies to all packets and all ports.

set qos ipprec-dscp-map *dscp1 ... dscp8*

Syntax Description

dscp1#	Number of the IP precedence value; up to eight values can be specified.

Defaults

The default IP precedence-to-DSCP configuration is listed in Table 2-18.

Table 2-18 IP Precedence-to-DSCP Mapping

IPPREC	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Use this command to map the IP precedence of IP packets arriving on trusted ports (or flows) to a DSCP when the trust type is **trust-ipprec**. This map is a table of eight precedence values (0 through 7) and their corresponding DSCP values. The 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

This command is supported on systems configured with a Layer 3 switching engine only.

Examples

This example shows how to assign IP precedence-to-DSCP mapping and return to the default:

```
Console> (enable) set qos ipprec-dscp-map 20 30 1 43 63 12 13 8
QoS ipprec-dscp-map set successfully.
Console> (enable)
```

Related Commands

clear qos ipprec-dscp-map
show qos maps

set qos mac-cos

Use the **set qos mac-cos** command to set the CoS value to the MAC address and VLAN pair.

set qos mac-cos *dest_mac vlan cos*

Syntax Description

dest_mac	MAC address of the destination host.
vlan	Number of the VLAN; valid values are from **1** to **1001** and from **1025** to **4094**.
cos	CoS value; valid values are from **0** to **7**, higher numbers represent higher priority.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command has no effect on a switch configured with a PFC since the Layer 3 switching engine's result always overrides the Layer 2 result. Instead, use the **set qos acl** command.

The **set qos mac-cos** command creates a permanent CAM entry in the CAM table until you reset the active supervisor engine.

The port associated with the MAC address is learned when the first packet with this source MAC address is received. These entries do not age out.

The CoS for a packet going to the specified MAC address is overwritten even if it is coming from a trusted port.

If you enter the **show cam** command, entries made with the **set qos mac-cos** command display as dynamic because QoS considers them to be dynamic, but they do not age out.

Examples

This example shows how to assign the CoS value 3 to VLAN 2:

```
Console> (enable) set qos mac-cos 0f-ab-12-12-00-13 2 3
CoS 3 is assigned to 0f-ab-12-12-00-13 vlan 2.
Console> (enable)
```

Related Commands

clear qos mac-cos
show qos mac-cos

set qos map

Use the **set qos map** command to map a specific CoS value to the transmit- or receive-priority queues and the thresholds per available priority queue for all ports.

set qos map *port_type* **tx** | **rx** *q# thr#* **cos** *coslist*

set qos map *port_type* **tx** *q#* **cos** *coslist*

Syntax Description

port_type	Port type; valid values are **2q2t**, **1p3q1t**, and **1p2q2t** for transmit and **1p1q4t** and **1p1q0t** for receive. See the "Usage Guidelines" section for additional information.
tx	Keyword to specify the transmit queue.
rx	Keyword to specify the receive queue.
q#	Value determined by the number of priority queues provided at the transmit or receive end; valid values are **1** and **2**, with the higher value indicating a higher priority queue.
thr#	Value determined by the number of drop thresholds available at a port; valid values are **1** and **2**, with the higher value indicating lower chances of being dropped.
cos *coslist*	Keyword and variable to specify CoS values; valid values are from **0** through **7**, with the higher numbers representing a higher priority.

Defaults

The default mappings for all ports are shown in Table 2-19 and Table 2-20.

Table 2-19 CoS-to-Queue-to-Threshold Mapping (TX)

Queue	Threshold	Cos Values[1]
QoS enabled		
1	1	0, 1
2	1	2, 3, 4
3	1	6, 7
4	0	5
QoS disabled		
1	0	0, 1, 2, 3, 4, 5 ,6, 7

1. All CoS values, except CoS 5, are mapped to WRED. CoS 5, which is mapped to queue 4 does not have an associated WRED threshold.

Table 2-20 CoS-to-Queue Mapping (RX)

Queue	COS Values
QoS enabled	
1	0, 1, 2, 3, 4, 6, 7
2	5
QoS disabled	
1	0, 1, 2, 3, 4, 5, 6, 7

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you enter the **set qos map** *port_type* **tx** *q#* **cos** *coslist* command, the following is a list of possible port types available:

- **tx** *port_type* = **1p3q1t**
- **rx** *port_type* = **1p1q0t**

You can enter the *cos_list* variable as a single CoS value, multiple noncontiguous CoS values, a range of CoS values, or a mix of values. For example, you can enter any of the following: 0, or 0,2,3, or 0-3,7.

The priority queue number is 4 for transmit and queue number 2 for receive.

When specifying the priority queue for the **1p2q2t** port type, the priority queue number is 3 and the threshold number is 1.

The receive- and transmit-drop thresholds have this relationship:

- Receive-queue 1 (standard) threshold 1 = transmit-queue 1 (standard low priority) threshold 1
- Receive-queue 1 (standard) threshold 2 = transmit-queue 1 (standard low priority) threshold 2
- Receive-queue 1 (standard) threshold 3 = transmit-queue 2 (standard high priority) threshold 1
- Receive-queue 1 (standard) threshold 4 = transmit-queue 2 (standard high priority) threshold 2

Refer to the *Catalyst 6000 Family Software Configuration Guide* for additional usage guidelines.

Examples

This example shows how to assign the CoS values 1, 2, and 5 to the first queue and the first drop threshold in that queue:

```
Console> (enable) set qos map 2q2t tx 1 1 cos 1,2,5
Qos tx priority queue and threshold mapped to cos successfully.
Console> (enable)
```

This example shows how to assign the CoS values to queue 1 and threshold 2 in that queue:

```
Console> (enable) set qos map 2q2t tx 1 2 cos 3-4,7
Qos tx priority queue and threshold mapped to cos successfully.
Console> (enable)
```

This example shows how to map the CoS value 5 to strict-priority transmit-queue 3/drop-threshold 1:

```
Console> (enable) set qos map 1p2q2t tx 3 1 cos 5

Qos tx strict queue and threshold mapped to cos successfully.
Console> (enable)
```

Related Commands

clear qos map
show qos info

set qos policed-dscp-map

Use the **set qos policed-dscp-map** command to set the mapping of policed in-profile DSCPs.

set qos policed-dscp-map [**normal** | **excess**] *in_profile_dscp*:*policed_dscp*...

Syntax Description

normal	(Optional) Keyword to specify normal rate policers.
excess	(Optional) Keyword to specify excess rate policers.
in_profile_dscp	Number of the in-profile DSCP; valid values are from **0** through **63**.
:*policed_dscp*	Number of the policed DSCP; valid values are **0** through **63**.

Defaults

The default map is no markdown.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can enter *in_profile_dscp* as a single DSCP, multiple DSCPs, or a range of DSCPs (for example, 1 or 1,2,3 or 1-3,7).

The colon between *in_profile_dscp* and *policed_dscp* is required.

This command is supported on systems configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) only.

Examples

This example shows how to set the mapping of policed in-profile DSCPs:

```
Console> (enable) set qos policed-dscp-map 60-63:60 20-40:5
QoS policed-dscp-map set successfully.
Console> (enable)
```

Related Commands

clear qos policed-dscp-map
show qos maps
show qos policer

set qos policer

Use the **set qos policer** command to create a policing rule for ACL.

set qos policer {**microflow** *microflow_name*} {**rate** *rate*} {**burst** *burst*} {**drop** | **policed-dscp**}

set qos policer {**aggregate** *aggregate_name*} {**rate** *rate*} {**burst** *burst*} {**drop** | **policed-dscp**}

set qos policer {**aggregate** *aggregate_name*} {**rate** *rate*} **policed-dscp** {**erate** *erate*} {**drop** | **policed-dscp**} **burst** *burst*

Syntax Description

microflow *microflow_name*	Keyword and variable to specify the name of the microflow policing rule.
rate *rate*	Keyword and variable to specify the average rate; valid values are **0** and from **32** Kbps to **8** Gbps.
burst *burst*	Keyword and variable to specify the burst size; valid values are **0** and from **1** Kb to **32** Mb.
drop	Keyword to specify drop traffic.
policed-dscp	Keyword to specify policed DSCP.
aggregate *aggregate_name*	Keyword and variable to specify the name of the aggregate policing rule.
erate *erate*	Keyword and variable to specify the excess rate value; valid values are **0** and from **32** Kbps to **8** Gbps.

Defaults

The default is no policing rules or aggregates are configured.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Before microflow policing can occur, you must define a microflow policing rule. Policing allows the switch to limit the bandwidth consumed by a flow of traffic.

The Catalyst 6000 family switch supports up to 63 microflow policing rules. When a microflow policer is used in any ACL that is attached to any port or VLAN, the NetFlow flow mask is bumped up to full flow.

Before aggregate policing can occur, you must create an aggregate and a policing rule for that aggregate. The Catalyst 6000 family switch supports up to 1023 aggregates and 1023 policing rules.

When both normal and excess rates are zero, you can specify any *burst* size. If the normal and excess rates are zero, the value is ignored and set internally by hardware.

The excess rate must be greater than or equal to the normal rate.

The **set qos policer aggregate** command allows you to configure an aggregate flow and a policing rule for that aggregate. When you enter the **microflow** *microflow_name* **rate** *rate* **burst** *burst*, the range for the average rate is 32 Kbps to 8 Gbps and the range for the burst size is 1 Kb (entered as 1) to 32 Mb (entered as 32000). The burst can be set lower, higher, or equal to the rate. Modifying an existing aggregate rate limit entry causes that entry to be modified in NVRAM and in the switch if that entry is currently being used.

Note We recommend a 32-Kb minimum value burst size. Due to the nature of the traffic at different customer sites, coupled with the hardware granularity, smaller values occasionally result in lower rates than the specified rate. If you experiment with smaller values but problems occur, increase the burst rate to this minimum recommended value.

Modifying an existing microflow or aggregate rate limit modifies that entry in NVRAM as well as in the switch if it is currently being used.

When you enter the policing name, follow these naming conventions:

- Maximum of 31 characters long 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

Examples

This example shows how to create a microflow policing rule for ACL:

```
Console> (enable) set qos policer microflow my-micro rate 1000 burst 10000 policed-dscp
QoS policer for microflow my-micro set successfully.
Console> (enable)
```

These examples show how to create an aggregate policing rule for ACL:

```
Console> (enable) set qos policer aggregate my-agg rate 1000 burst 2000 drop
QoS policer for aggregate my-aggset successfully.
Console> (enable)

Console> (enable) set qos policer aggregate test3 rate 64 policed-dscp erate 128 drop burst 96
QoS policer for aggregate test3 created successfully.
Console> (enable)
```

Related Commands

clear qos policer
show qos policer

set qos policy-source

Use the **set qos policy-source** command to set the QoS policy source.

set qos policy-source local | **cops**

Syntax Description

local	Keyword to set the policy source to local NVRAM configuration.
cops	Keyword to set the policy source to COPS-PR configuration.

Defaults

The default is all ports are set to local.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you set the policy source to **local**, the QoS policy is taken from local configuration stored in NVRAM. If you set the policy source to **local** after it was set to **cops**, the QoS policy reverts back to the local configuration stored in NVRAM.

When you set the policy source to **cops**, all global configurations to the device, such as the DSCP-to-marked-down DSCP, is taken from policy downloaded to the PEP by the PDP. Configuration of each physical port, however, is taken from COPS-PR only if the policy source for that port has been set to **cops**.

Examples

This example shows how to set the policy source to COPS-PR:

```
Console> (enable) set qos policy-source cops
QoS policy source for the switch set to COPS.
Console> (enable)
```

This example shows how to set the policy source to local NVRAM:

```
Console> (enable) set qos policy-source local
QoS policy source for the switch set to local.
Console> (enable)
```

This example shows the output if you attempt to set the policy source to COPS-PR and no COPS-PR servers are available:

```
Console> (enable) set qos policy-source cops
QoS policy source for the switch set to COPS.
Warning: No COPS servers configured. Use the ‘set cops server’ command
to configure COPS servers.
Console> (enable)
```

Related Commands

clear qos config
show qos policy-source

set qos rsvp

Use the **set qos rsvp** command to turn on or turn off the RSVP feature on the switch, set the time in minutes after which the RSVP databases get flushed (when the policy server dies), and set the local policy.

set qos rsvp enable | **disable**

set qos rsvp policy-timeout *timeout*

set qos rsvp local-policy forward | **reject**

Syntax Description

enable	Keyword to activate the RSVP feature.
disable	Keyword to deactivate the RSVP feature.
policy-timeout *timeout*	Keyword and variable to specify the time in minutes after which the RSVP databases get flushed; valid values are from **1** to **65535** minutes.
local-policy forward | **reject**	Keywords to specify the policy configuration local to the network device to either accept existing flows and forward them or not accept new flows.

Defaults

The default is the RSVP feature is disabled, policy-timeout is 30 minutes, and local-policy is forward.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The local-policy guidelines are as follows:

- There is no connection with the policy server.
- New flows that come up after connection with the policy server have been lost.
- Old flows that come up after the PDP policy times out.

Examples

This example shows how to enable RSVP:

```
Console> (enable) set qos rsvp enable
RSVP enabled. Only RSVP qualitative service supported.
QoS must be enabled for RSVP.
Console> (enable)
```

This example shows how to disable RSVP:

```
Console> (enable) set qos rsvp disable
RSVP disabled on the switch.
Console> (enable)
```

This example shows how to set the policy-timeout interval:

```
Console> (enable) set qos rsvp policy-timeout 45
RSVP database policy timeout set to 45 minutes.
Console> (enable)
```

This example shows how to set the policy-timeout interval:

```
Console> (enable) set qos rsvp local-policy forward
RSVP local policy set to forward.
Console> (enable)
```

Related Commands **show qos rsvp**

set qos rxq-ratio

Use the **set qos rxq-ratio** command to set the amount of packet buffer memory allocated to high-priority incoming traffic and low-priority incoming traffic.

set qos rxq-ratio *port_type queue1_val queue2_val... queueN_val*

Syntax Description

port_type	Port type; valid value is **1p1q0t** and **1p1q8t**.
queue1_val	Percentage of low-priority traffic; valid values are from **1** to **99** and must total 100 with the *queue2_val* value.
queue2_val	Percentage of high-priority traffic; valid values are from **1** to **99** and must total 100 with the *queue1_val* value.
queueN_val	Percentage of strict-priority traffic; valid values are from **1** to **99** and must total 100 with the *queue1_val* and *queue1_val* values.

Defaults

The default is 80:20 (queue 1 and queue 2) if you enable QoS and 100:0 (queue 1 and queue 2) if you disable QoS.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Caution Use caution when using this command. When entering the **set qos rxq-ratio** command, all ports go through a link up and down condition.

The values set in hardware are close approximations of the values provided. For example, if you specify 0 percent, the actual value programmed is not necessarily 0.

The **rxq** ratio is determined by the traffic mix in the network. High-priority traffic is typically a smaller fraction of the traffic. Because the high-priority queue gets more service, you should set the high-priority queue lower than the low-priority queue.

The strict-priority queue requires no configuration.

Examples

This example shows how to set the receive-queue size ratio:

```
Console> (enable) set qos rxq-ratio 1p1q0t 80 20
QoS rxq-ratio is set successfully.
Console> (enable)
```

Related Commands

show qos info

set qos statistics export

Use the **set qos statistics export** command to globally enable or disable statistics data gathering from hardware.

set qos statistics export {**enable** | **disable**}

Syntax Description

enable	Keyword to enable statistics data gathering.
disable	Keyword to disable statistics data gathering.

Defaults

The default is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Statistics polling does not occur if statistics are disabled, regardless of any other settings.

You must designate an export destination prior to entering this command. If an export destination is not set, this message displays:

```
Warning: Export destination not set. Use the 'set qos statistics export destination'
command to configure the export destination.
```

Examples

This example shows how to enable statistics polling:

```
Console> (enable) set qos statistics export enable
QoS statistics export enabled.
Export destination: Stargate, port 9996
Console> (enable)
```

Related Commands

show qos statistics export info

set qos statistics export aggregate

Use the **set qos statistics export aggregate** command to enable or disable statistics data export on an aggregate policer.

set qos statistics export aggregate *name* {**enable** | **disable**}

Syntax Description

name	(Optional) Name of the policer.
enable	Keyword to enable statistics data export for the named aggregate policer.
disable	Keyword to disable statistics data export for the named aggregate policer.

Defaults

The default is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

To export data, you should enable statistics on the port as well. Also, you must globally enable statistics and data export (see the **set qos statistics export** command).

This command is supported on systems configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) only.

Examples

This example shows how to enable statistics export:

```
Console> (enable) set qos statistics export aggregate ipagg_3 enable
Statistics data export enabled for aggregate policer ipagg_3.
Export destination: 172.20.15.1 (Stargate), port 9996
Console> (enable)
```

Related Commands

set qos statistics export
show mac
show qos statistics export info

set qos statistics export destination

Use the **set qos statistics export destination** command to specify the statistics data export destination address.

set qos statistics export destination {*host_name* | *host_ip*} [*port*]

set qos statistics export destination {*host_name* | *host_ip*} [**syslog** [{*facility severity*}]]

Syntax Description

host_name	Host name.
host_ip	Host IP address.
port	(Optional) UDP port number.
syslog	(Optional) Keyword to specify the syslog port.
facility	(Optional) Value to specify the type of facility to export; see the "Usage Guidelines" section for a list of valid values.
severity	(Optional) Value to specify 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 Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Valid *facility* values are **kern**, **user**, **mail**, **daemon**, **auth**, **lpr**, **news**, **uucp**, **cron**, **local0**, **local1**, **local2**, **local3**, **local4**, **local5**, **local6**, and **local7**.

Valid *severity* levels are **emerg**, **alert**, **crit**, **err**, **warning**, **notice**, **info**, and **debug**.

Examples

This example shows how to specify the statistics data export destination address:

```
Console> (enable) set qos statistics export destination stargate 9996
Statistics data export destination set to stargate port 9996.
Console> (enable)
```

Related Commands

set qos statistics export
show qos statistics export info

set qos statistics export interval

Use the **set qos statistics export interval** command to specify how often a port and/or aggregate policer statistics data is read and exported.

set qos statistics export interval *interval*

Syntax Description

interval	Export time interval; valid values are from **30** seconds to **65535** seconds.

Defaults

The default is 30 seconds.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to set the export interval:

```
Console> (enable) set qos statistics export interval 35
Statistics export interval set to 35 seconds.
Console> (enable)
```

Related Commands

show qos statistics export info

set qos statistics export port

Use the **set qos statistics export port** command to enable or disable statistics data export on a port.

set qos statistics export port *mod/port* {**enable** | **disable**}

Syntax Description

mod/port	(Optional) Number of the module and the port on the module.
enable	Keyword to enable statistics data export.
disable	Keyword to disable statistics data export.

Defaults

The default is disabled.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

For data export to be performed, you should enable statistics on the aggregate policer as well. You must globally enable statistics and data export (see the **set qos statistics export** command).

Examples

This example shows how to enable statistics export on a port:

```
Console> (enable) set qos statistics export port 2/5 enable
Statistics data export enabled on port 2/5.
Console> (enable)
```

Related Commands

show qos statistics export info

set qos txq-ratio

Use the **set qos txq-ratio** command to set the amount of packet buffer memory allocated to high-priority traffic and low-priority traffic.

set qos txq-ratio *port_type queue1_val queue2_val... queueN_val*

Syntax Description

port_type	Port type; valid values are **2q2t**, **1p2q2t**, and **1p2q1t**.
queue1_val	Percentage of low-priority traffic; valid values are from **1** to **99** and must total 100 with the *queue2_val* value.
queue2_val	Percentage of high-priority traffic; valid values are from **1** to **99** and must total 100 with the *queue1_val* value.
queueN_val	Percentage of strict-priority traffic; valid values are from **1** to **99** and must total 100.

Defaults

The default for **2q2t** is 80:20 if you enable QoS and 100:0 if you disable QoS. The default for **1p2q2t** is 70:15:15 if you enable QoS and 100:0:0 if you disable QoS.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Caution Use caution when using this command. When entering the **set qos txq-ratio** command, all ports go through a link up and down condition.

The values set in hardware will be close approximations of the values provided. For example, even if you specify 0 percent, the actual value programmed will not necessarily be 0.

The **txq** ratio is determined by the traffic mix in the network. Because high-priority traffic is typically a smaller fraction of the traffic and because the high-priority queue gets more service, you should set the high-priority queue lower than the low-priority queue.

The strict-priority queue requires no configuration.

Examples

This example shows how to set the transmit-queue size ratio:

```
Console> (enable) set qos txq-ratio 2q2t 75 25
QoS txq-ratio is set successfully.
Console> (enable)
```

Related Commands

show qos info

set qos wred

Use the **set qos wred** command to configure the WRED threshold parameters for the specified port type.

set qos wred *port_type* [**tx**] **queue** *q#* {[*thr1Lo*:]*thr1Hi*} {[*thr2Lo*:]*thr2Hi*}...

Syntax Description

port_type	Port type; valid values are **1p2q2t**, **1p2q1t**, **1p3q1t**, and **1p1q8t**.
tx	(Optional) Keyword to specify the parameters for output queuing.
queue *q#*	Keyword and variable to specify the queue to which the arguments apply; valid values are **1** through **3**.
thr1Lo	(Optional) Percentage of the lower threshold size for the first WRED curve; valid values are **1** to **100**.
thr1Hi	Percentage of the upper threshold size for the first WRED curve; valid values are **1** to **100**.
thr2Lo	(Optional) Percentage of the lower threshold size for the second WRED curve; valid values are **1** to **100**.
thr2Hi	Percentage of the upper threshold size for the second WRED curve; valid values are **1** to **100**.
thr#	Percentage of the buffer size; valid values are **1** to **100**.

Defaults

The default thresholds are as follows:

- For **1p2q2t** = 40:70 (threshold1) and 70:100 (threshold2) (low:high percentage)/queue
- For **1p3q1t** = 70:100 (low:high)

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The queue values range from 1 to 3. Queue 4 is the strict-priority queue and does not have an associated WRED threshold. The thresholds are all specified as percentages ranging from 1 to 100. A value of 10 indicates a threshold when the buffer is 10 percent full.

The colon between the low and high threshold values is required.

Examples

This example shows how to configure lower and upper threshold values for queue 1:

```
Console> (enable) set qos wred 1p2q2t queue 1 20:60 40:90
WRED thresholds for queue 1 set to 20:60 and 40:90 on all WRED-capable 1p2q2t ports.
Console> (enable)
```

This example shows how to configure the upper threshold value for queue 1:

```
Console> (enable) set qos wred 1p3q1t tx queue 1 20
WRED thresholds for queue 1 set to 0:20 on all WRED-capable 1p3q1t ports.
Console> (enable)
```

Related Commands

clear qos config
show qos info

set qos wrr

Use the **set qos wrr** command to specify the weights that determine how many packets will transmit out of one queue before switching to the other queue.

set qos wrr *port_type queue1_val queue2_val...*

Syntax Description

port_type	Port type; valid values are **2q2t**, **1p2q2t**, **1p3q1t**, and **1p2q1t**.
queue#_val	Number of weights for queues 1, 2, or 3; valid values are from **1** to **255**.

Defaults

The default WRR with QoS enabled for port type **1p3q1t** is as follows:

- Queue 1 = 100
- Queue 2 = 150
- Queue 3 = 200

With QoS disabled, the default is 255 for all three queues.

The default WRR for port types **2q2t** and **1p2q2t** is 4:255.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The WRR weights are used to partition the bandwidth between the queues in the event all queues are not empty. For example, weights of 1:3 mean that one queue gets 25 percent of the bandwidth and the other gets 75 percent as long as both queues have data.

Weights of 1:3 do not necessarily lead to the same results as when the weights are 10:30. In the latter case, more data is serviced from each queue and the latency of packets serviced from the other queue goes up. For best results, 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.

The values set in hardware will be close approximations of the values provided. For example, even if you specify 0 percent, the actual value programmed will not necessarily be 0. Whatever weights you choose, make sure that the resulting byte values programmed (see the **show qos info** command with the **runtime** keyword) are at least equal to the MTU size.

The ratio achieved is only an approximation of what you specify since the cutoff is on a packet and midway through a packet. For example, if you specify that the ratio services 1000 bytes out of the low-priority queue, and there is a 1500-byte packet in the low-priority queue, the entire 1500-byte packet is transmitted because the hardware services an entire packet.

For **1p2q2t** and **2q2t**, only two queues can be set; the third queue is strict priority.

For **1p3q1t**, three queues can be set; a fourth queue is strict priority.

Examples

This example shows how to specify the weights for queue 1 and queue 2 to 30 and 70:

```
Console> (enable) set qos wrr 2q2t 30 70
QoS wrr ratio is set successfully.
Console> (enable)
```

Related Commands

show qos info
show qos statistics

set radius deadtime

Use the **set radius deadtime** command to set the time to skip RADIUS servers that do not reply to an authentication request.

set radius deadtime *minutes*

Syntax Description

minutes	Length of time a RADIUS server does not respond to an authentication request; valid values are from **0** to **1440** minutes.

Defaults

The default is 0 minutes.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If only one RADIUS server is configured or if all the configured servers are marked dead, deadtime will be ignored since no alternate servers are available. By default, the deadtime is 0 minutes; the RADIUS servers are not marked dead if they do not respond.

Examples

This example shows how to set the RADIUS deadtime to 10 minutes:

```
Console> (enable) set radius deadtime 10
Radius deadtime set to 10 minutes.
Console> (enable)
```

Related Commands

show radius

set radius key

Use the **set radius key** command to set the encryption and authentication for all communication between the RADIUS client and the server.

set radius key *key*

Syntax Description

key	Name of the key to authenticate the transactions between the RADIUS client and the server.

Defaults

The default of the key is set to null.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The key you set must be the same one as configured in the RADIUS server. All leading spaces are ignored; spaces within and at the end of the key are not ignored. Double quotes are not required even if there are spaces in the key, unless the quotes themselves are part of the key. The length of the key is limited to 65 characters; it can include any printable ASCII characters except tabs.

If you configure a RADIUS key on the switch, make sure you configure an identical key on the RADIUS server.

Examples

This example shows how to set the RADIUS encryption and authentication key to Make my day:

```
Console> (enable) set radius key Make my day
Radius key set to Make my day.
Console> (enable)
```

Related Commands

show radius

set radius retransmit

Use the **set radius retransmit** command to specify the number of times the RADIUS servers are tried before giving up on the server.

set radius retransmit *count*

Syntax Description

count	Number of times the RADIUS servers are tried before giving up on the server; valid values are from **1** to **100**.

Defaults

The default is two times (three attempts).

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to set the retransmit attempts to 3:

```
Console> (enable) set radius retransmit 3
Radius retransmit count set to 3.
Console> (enable)
```

Related Commands

show radius

set radius server

Use the **set radius server** command to set up the RADIUS server.

set radius server *ipaddr* [**auth-port** *port*] [**acct-port** *port*] [**primary**]

Syntax Description

ipaddr	Number of the IP address or IP alias in dot notation a.b.c.d.
auth-port *port*	(Optional) Keyword and variable to specify a destination UDP port for RADIUS authentication messages.
acct-port *port*	(Optional) Keyword and variable to specify a destination UDP port for RADIUS accounting messages.
primary	(Optional) Keyword to specify this server be contacted first.

Defaults

The default **auth-port** is 181, and the default **acct-port** is 1813.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you configure multiple RADIUS servers, the first server configured is the primary. Authentication requests are sent to this server first. You can specify a particular server as primary by using the **primary** keyword. You can add up to three RADIUS servers.

The *ipaddr* value can be entered as an IP alias or an IP address in dot notation a.b.c.d.

If you set the **auth-port** *port* to 0, the RADIUS server will not be used for authentication. If you set the **acct-port** *port* to 0, the RADIUS server will not be used for accounting.

If you configure a RADIUS key on the switch, make sure you configure an identical key on the RADIUS server.

You must specify a RADIUS server before enabling RADIUS on the switch.

Examples

This example shows how to add a primary server using an IP alias:

```
Console> (enable) set radius server everquest.com auth-port 0 acct-port 1646 primary
everquest.com added to RADIUS server table as primary server.
Console> (enable)
```

This example shows how to add a primary server using an IP address:

```
Console> (enable) set radius server 172.22.11.12 auth-port 0 acct-port 1722 primary
172.22.11.12 added to RADIUS server table as primary server
Console> (enable)
```

Related Commands **show radius**

set radius timeout

Use the **set radius timeout** command to set the time between retransmissions to the RADIUS server.

set radius timeout *seconds*

Syntax Description

seconds	Number of seconds to wait for a reply; valid values are from **1** to **1000** seconds.

Defaults

The default timeout is 5 seconds.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to set the time between retransmissions to 7 seconds:

```
Console> (enable) set radius timeout 7
Radius timeout set to 7 seconds.
Console> (enable)
```

Related Commands

show radius

set rcp username

Use the **set rcp username** command to specify your username for rcp file transfers.

set rcp username *username*

Syntax Description

username	Username up to 14 characters long.

Defaults

There are no default settings for this command.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The username can be a maximum of 40 characters, must be different from “root,” and not a null string.

The only case where you cannot configure the rcp *username* is for the VMPS database where you will use an rcp VMPS username. Use the **set vmps downloadmethod** command to specify the rcp VMPS username.

Examples

This example shows how to set the username for rcp:

```
Console> (enable) set rcp username jdoe
Console> (enable)
```

Related Commands

clear rcp
set vmps downloadmethod
show rcp

set rgmp

Use the **set rgmp** command to enable or disable the RGMP feature on the switch.

set rgmp {**enable** | **disable**}

Syntax Description

enable	Keyword to enable RGMP on the switch.
disable	Keyword to disable RGMP on the switch.

Defaults

The default is RGMP is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set rgmp** command affects the entire switch. You cannot enable or disable RGMP on a per-VLAN basis.

The RGMP feature is operational only if IGMP snooping is enabled on the switch (see the **set igmp** command).

Examples

This example shows how to enable RGMP on the switch:

```
Console> (enable) set rgmp enable
RGMP is enabled.
Console> (enable)
```

This example shows how to disable RGMP on the switch:

```
Console> (enable) set rgmp disable
RGMP is disabled.
Console> (enable)
```

Related Commands

clear rgmp statistics
set igmp
show rgmp group
show rgmp statistics

set rspan

Use the **set rspan** command to create remote SPAN sessions.

set rspan disable source [*rspan_vlan* | **all**]

set rpsan disable destination [*mod/port* | **all**]

set rspan source {*src_mod/src_ports...* | *vlans...* | **sc0**} {*rspan_vlan*} [**rx** | **tx** | **both**] [**multicast** {**enable** | **disable**}] [**filter** *vlans...*] [**create**]

set rspan destination *mod/port* {*rspan_vlan*} [**inpkts** {**enable** | **disable**}] [**learning** {**enable** | **disable**}] [**create**]

Syntax Description

disable source	Keywords to disable remote SPAN source information.
rspan_vlan	(Optional) Remote SPAN VLAN.
all	(Optional) Keyword to disable all remote SPAN source or destination sessions.
disable destination	Keywords to disable remote SPAN destination information.
mod/port	(Optional) Remote SPAN destination port.
src_mod/src_ports...	Monitored ports (remote SPAN source).
vlans...	Monitored VLANs (remote SPAN source).
sc0	Keyword to specify the inband port is a valid source.
rx	(Optional) Keyword to specify that information received at the source (ingress SPAN) is monitored.
tx	(Optional) Keyword to specify that information transmitted from the source (egress SPAN) is monitored.
both	(Optional) Keyword to specify that information both transmitted from the source (ingress SPAN) and received (egress SPAN) at the source are monitored.
multicast enable	(Optional) Keywords to enable monitoring multicast traffic (egress traffic only).
multicast disable	(Optional) Keywords to disable monitoring multicast traffic (egress traffic only).
filter *vlans*	(Optional) Keywords to monitor traffic on selected VLANs on source trunk ports.
create	(Optional) Keyword to create a new remote SPAN session instead of overwriting the previous SPAN session.
inpkts enable	(Optional) Keywords to allow the remote SPAN destination port to receive normal ingress traffic (from the network to the bus) while forwarding the remote SPAN traffic.

inpkts disable	(Optional) Keywords to disable the receiving of normal inbound traffic on the remote SPAN destination port.
learning enable	(Optional) Keywords to enable learning for the remote SPAN destination port.
learning disable	(Optional) Keywords to disable learning for the remote SPAN destination port.

Defaults

The defaults are as follows:

- Remote SPAN is disabled.
- No VLAN filtering.
- Monitoring multicast traffic is enabled.
- Learning is enabled.
- inpkts is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

The *rspan_vlan* variable is optional in the **set rspan disable source** command and required in the **set rspan source** and **set rspan destination** command set.

After you enable SPAN, system defaults are used if no parameters were ever set. If you changed parameters, these are stored in NVRAM, and the new parameters are used.

Use a network analyzer to monitor ports.

Use the **inpkts** keyword with the **enable** option to allow the remote SPAN destination port to receive normal incoming traffic in addition to the traffic mirrored from the remote SPAN source. Use the **disable** option to prevent the remote SPAN destination port from receiving normal incoming traffic.

You can specify an MSM port as the remote SPAN source port. However, you cannot specify an MSM port as the remote SPAN destination port.

When you enable the **inpkts** option, a warning message notifies you that the destination port does not join STP and may cause loops if this option is enabled.

If you do not specify the keyword **create** and you have only one session, the session will be overwritten. If a matching *rspan_vlan* or destination port exists, the particular session will be overwritten (with or without specifying **create**). If you specify the keyword **create** and there is no matching *rspan_vlan* or destination port, the session will be created.

Each switch can source only one remote SPAN session (ingress, egress, or both). When you configure a remote ingress or bidirectional SPAN session in a source switch, the limit for local ingress or bidirectional SPAN session is reduced to one. There are no limits on the number of remote SPAN sessions carried across the network within the remote SPAN session limits.

You can configure any VLAN as a remote SPAN VLAN as long as these conditions are met:

- The same remote SPAN VLAN is used for a remote SPAN session in the switches.
- All the participating switches have appropriate hardware and software.
- No unwanted access port is configured in the remote SPAN VLAN.

Examples

This example shows how to disable all enabled source sessions:

```
Console> (enable) set rspan disable source all
This command will disable all remote span source session(s).
Do you want to continue (y/n) [n]? y
Disabled monitoring of all source(s) on the switch for remote span.
Console> (enable)
```

This example shows how to disable one source session to a specific VLAN:

```
Console> (enable) set rspan disable source 903
Disabled monitoring of all source(s) on the switch for rspan_vlan 903.
Console> (enable)
```

This example shows how to disable all enabled destination sessions:

```
Console> (enable) set rspan disable destination all
This command will disable all remote span destination session(s).
Do you want to continue (y/n) [n]? y
Disabled monitoring of remote span traffic on ports 9/1,9/2,9/3,9/4,9/5,9/6.
Console> (enable)
```

This example shows how to disable one destination session to a specific port:

```
Console> (enable) set rspan disable destination 4/1
Disabled monitoring of remote span traffic on port 4/1.
Console> (enable)
```

Related Commands

show rspan

set security acl adjacency

Use the **set security acl adjacency** command to set an entry for the adjacency table.

set security acl adjacency *adjacency_name dest_vlan dest_mac* [*source_mac* [**mtu** *mtu_size*] | **mtu** *mtu_size*]

Syntax Description

adjacency_name	Name of the adjacency table entry.
dest_vlan	Name of the destination VLAN.
dest_mac	Destination MAC address.
source_mac	(Optional) Source MAC address.
mtu *mtu_size*	(Optional) Keyword and variable to specify packet size in bytes.

Defaults

The default size for the MTU is 9600 bytes.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The order of ACEs in a PBF VACL is important. The adjacency table entry has to be defined in the VACL before the redirect ACE because the redirect ACE uses it to redirect traffic. Refer to the *Catalyst 6000 Family Software Configuration Guide* for detailed information on configuring PBF VACLs.

You can set the MTU for cases in which jumbo frames are sent using PBF.

Examples

This example shows how to set an entry for the adjacency table:

```
Console> (enable) set security acl adjacency ADJ1 11 0-0-0-0-0-B 0-0-0-0-0-A
Console> (enable)
```

This example shows how to set an entry for the adjacency table with a specific MTU size:

```
Console> (enable) set security acl adjacency a_1 2 0-0a-0a-0a-0a-0a 9000
Console> (enable)
```

Related Commands

clear security acl
commit
show security aclo

set security acl capture-ports

Use the **set security acl capture-ports** command to set the ports (specified with the **capture** option in the **set security acl ip**, **set security acl ipx**, and **set security acl mac** commands) to show traffic captured on these ports.

set security acl capture-ports {*mod/ports...*}

Syntax Description

mod/ports...	Module and port number.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Configurations you make by entering this command are saved in NVRAM. This command *does not* require that you enter the **commit** command.

The module and port specified in this command are added to the current ports configuration list.

This command works with Ethernet ports only; you cannot set ATM ports.

The ACL capture will not work unless the capture port is in the spanning tree forwarding state for the VLAN.

Examples

This example shows how to set a port to capture traffic:

```
Console> (enable) set security acl capture-ports 3/1
Successfully set 3/1 to capture ACL traffic.
Console> (enable)
```

This example shows how to set multiple ports to capture traffic:

```
Console> (enable) set security acl capture-ports 1/1-10
Successfully set the following ports to capture ACL traffic: 1/1-2.
Console> (enable)
```

Related Commands

clear security acl capture-ports
show security acl capture-ports

set security acl ip

Use the **set security acl ip** command to create a new entry in a standard IP VACL and append the new entry at the end of the VACL.

set security acl ip {*acl_name*} {**permit** | **deny**} {*src_ip_spec*} [**before** *editbuffer_index* | **modify** *editbuffer_index*] [**log**]

set security acl ip {*acl_name*} [**permit** | **deny**] **arp**

set security acl ip {*acl_name*} {**permit** | **deny** | **redirect** {*adj_name* | *mod_num/port_num*}} {*protocol*} {*src_ip_spec*} {*dest_ip_spec*} [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**capture**] [**before** *editbuffer_index* | **modify** *editbuffer_index*] [**log**]

set security acl ip {*acl_name*} {**permit** | **deny** | **redirect** {*mod_num/port_num*}} [**ip**] {*src_ip_spec*} {*dest_ip_spec*} [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**capture**] [**before** *editbuffer_index* | **modify** *editbuffer_index*] [**log**]

set security acl ip {*acl_name*} {**permit** | **deny** | **redirect** {*mod_num/port_num*}} [**icmp** | **1**] {*src_ip_spec*} {*dest_ip_spec*} [*icmp_type*] [*icmp_code*] | [*icmp_message*] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**capture**] [**before** *editbuffer_index* | **modify** *editbuffer_index*] [**log**]

set security acl ip {*acl_name*} {**permit** | **deny** | **redirect** {*mod_num/port_num*}} [**tcp** | **6**] {*src_ip_spec*} [*operator port* [*port*]] {*dest_ip_spec*} [*operator port* [*port*]] [**established**] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**capture**] [**before** *editbuffer_index* | **modify** *editbuffer_index*] [**log**]

set security acl ip {*acl_name*} {**permit** | **deny** | **redirect** {*mod_num/port_num*}} [**udp** | **17**] {*src_ip_spec*} [*operator port* [*port*]] {*dest_ip_spec*} [*operator port* [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**capture**] [**before** *editbuffer_index* | **modify** *editbuffer_index*] [**log**]

Syntax Description

acl_name	Unique name that identifies the lists to which the entry belongs.
permit	Keyword to allow traffic from the source IP address.
deny	Keyword to block traffic from the source IP address.
src_ip_spec	Source IP address and the source mask. See the “Usage Guidelines” section for the format.
before *editbuffer_index*	(Optional) Keyword and variable to insert the new ACE in front of another ACE.
modify *editbuffer_index*	(Optional) Keyword and variable to replace an ACE with the new ACE.
log	(Optional) Keyword to log denied packets.
arp	Keyword to specify ARP.
redirect	Keyword to specify to which switched ports the packet is redirected.
mod_num/port_num	Number of the module and port.
adj_name	Name of the adjacency table entry.

protocol	Keyword or number of an IP protocol; valid numbers are from **0** to **255** representing an IP protocol number. See the "Usage Guidelines" section for the list of valid keywords.
dest_ip_spec	Destination IP address and the destination mask. See the "Usage Guidelines" section for the format.
precedence *precedence*	(Optional) Keyword and variable to specify the precedence level; valid values are from **0** to **7** or by name. See the "Usage Guidelines" section for a list of valid names.
tos *tos*	(Optional) Keyword and variable to specify the type of service level; valid values are from **0** to **15** or by name. See the "Usage Guidelines" section for a list of valid names.
fragment	(Optional) Keyword to filter IP traffic that carries fragments.
capture	(Optional) Keyword to specify packets are switched normally and captured; **permit** must also be enabled.
ip	(Optional) Keyword to match any Internet Protocol packet.
icmp | **1**	(Optional) Keyword or number to match ICMP packets.
icmp-type	(Optional) ICMP message type name or a number; valid values are from **0** to **255**. See the "Usage Guidelines" section for a list of valid names.
icmp-code	(Optional) ICMP message code name or a number; valid values are from **0** to **255**. See the "Usage Guidelines" section for a list of valid names.
icmp-message	(Optional) ICMP message type name or ICMP message type and code name. See the "Usage Guidelines" section for a list of valid names.
tcp | **6**	(Optional) Keyword or number to match TCP packets.
operator	(Optional) Operands; valid values include **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range).
port	(Optional) Number or name of a TCP or UDP port; valid port numbers are from **0** to **65535**. See the "Usage Guidelines" section for a list of valid names.
established	(Optional) Keyword to specify an established connection; used only for TCP protocol.
udp | **17**	(Optional) Keyword or number to match UDP packets.

Defaults

There are no default ACLs and no default ACL-VLAN mappings. By default, ARP is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Configurations you make by entering this command are saved to NVRAM and hardware only after you enter the **commit** command. Enter ACEs in batches and then enter the **commit** command to save them in NVRAM and in the hardware.

The **arp** keyword is supported on switches configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2). If you use the **arp** keyword, this is supported on a per-ACL basis only; either ARP is allowed or ARP is denied.

If you use the **fragment** keyword in an ACE, this ACE applies to nonfragmented traffic and to the fragment with offset equal to zero in a fragmented flow.

A fragmented ACE that permits Layer 4 traffic from host A to host B also permits fragmented traffic from host A to host B regardless of the Layer 4 port.

If you use the **capture** keyword, the ports that capture the traffic and transmit out are specified by entering the **set security acl capture-ports** command.

When you enter the ACL name, follow these naming conventions:

- Maximum of 32 characters long 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

When you specify the source IP address and the source mask, use the form *source_ip_address source_mask* and follow these guidelines:

- The *source_mask* is required; 0 indicates a care bit, 1 indicates a don't-care bit.
- Use a 32-bit quantity in four-part dotted-decimal format.
- Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.
- Use **host** source as an abbreviation for a *source* and *source-wildcard* of source 0.0.0.0.

When you enter a destination IP address and the destination mask, use the form *destination_ip_address destination_mask*. The destination mask is required.

- Use a 32-bit quantity in a four-part dotted-decimal format.
- Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.
- Use **host**/source as an abbreviation for a *destination* and *destination-wildcard* of destination 0.0.0.0.

The **log** keyword is an option of **deny** only. If you want to change an existing VACL configuration to **deny** with **log**, you must first clear the VACL and then set it again.

The **log** keyword is supported on systems configured with Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) only.

Valid names for *precedence* are critical, flash, flash-override, immediate, internet, network, priority, and routine.

Valid names for *tos* are max-reliability, max-throughput, min-delay, min-monetary-cost, and normal.

Valid *protocol* keywords include **icmp** (1), **ip**, **ipinip** (4), **tcp** (6), **udp** (17), **igrp** (9), **eigrp** (88), **gre** (47), **nos** (94), **ospf** (89), **ahp** (51), **esp** (50), **pcp** (108), and **pim** (103). The IP number is displayed in parentheses. Use the keyword **ip** to match any Internet Protocol.

ICMP packets that are matched by ICMP message type can also be matched by the ICMP message code.

Valid names for *icmp_type* and *icmp_code* are administratively-prohibited, alternate-address, conversion-error, dod-host-prohibited, dod-net-prohibited, echo, echo-reply, general-parameter-problem, host-isolated, host-precedence-unreachable, host-redirect, host-tos-redirect, host-tos-unreachable, host-unknown, host-unreachable, information-reply, information-request, mask-reply, mask-request, mobile-redirect, net-redirect, net-tos-redirect, net-tos-unreachable, net-unreachable, network-unknown, no-room-for-option, option-missing, packet-too-big, parameter-problem, port-unreachable, precedence-unreachable, protocol-unreachable, reassembly-timeout, redirect, router-advertisement, router-solicitation, source-quench, source-route-failed, time-exceeded, timestamp-reply, timestamp-request, traceroute, ttl-exceeded, and unreachable.

If the operator is positioned after the source and source-wildcard, it must match the source port. If the operator is positioned after the destination and destination-wildcard, it must match the destination port. The range operator requires two port numbers. All other operators require one port number.

TCP port names can be used only when filtering TCP. Valid names for TCP ports are bgp, chargen, daytime, discard, domain, echo, finger, ftp, ftp-data, gopher, hostname, irc, klogin, kshell, lpd, nntp, pop2, pop3, smtp, sunrpc, syslog, tacacs-ds, talk, telnet, time, uucp, whois, and www.

UDP port names can be used only when filtering UDP. Valid names for UDP ports are biff, bootpc, bootps, discard, dns, dnsix, echo, mobile-ip, nameserver, netbios-dgm, netbios-ns, ntp, rip, snmp, snmptrap, sunrpc, syslog, tacacs-ds, talk, tftp, time, who, and xdmcp.

The number listed with the protocol type is the layer protocol number (for example, **udp** | **17**).

If no layer protocol number is entered, you can enter the following syntax:

set security acl ip {*acl_name*} {**permit** | **deny**} {*src_ip_spec*} [**before** *editbuffer_index* | **modify** *editbuffer_index*]

If a Layer 4 protocol is specified, you can enter the following syntax:

set security acl ip {*acl_name*} {**permit** | **deny** | **redirect** *mod_num/port_num*} {*protocol*} {*src_ip_spec*} {*dest_ip_spec*} [**precedence** *precedence*] [**tos** *tos*] [**capture**] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

For IP, you can enter the following syntax:

set security acl ip {*acl_name*} {**permit** | **deny** | **redirect** {*mod_num/port_num*}} [**ip**] {*src_ip_spec*} {*dest_ip_spec*} [**precedence** *precedence*] [**tos** *tos*] [**capture**] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

For ICMP, you can enter the following syntax:

set security acl ip {*acl_name*} {**permit** | **deny** | **redirect** {*mod_num/port_num*}} [**icmp** | **1**] {*src_ip_spec*} {*dest_ip_spec*} [*icmp_type*] [*icmp_code*] | [*icmp_message*] [**precedence** *precedence*] [**tos** *tos*] [**capture**] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

For TCP, you can use the following syntax:

set security acl ip {*acl_name*} {**permit** | **deny** | **redirect** {*mod_num/port_num*}} [**tcp** | **6**] {*src_ip_spec*} [*operator port* [*port*]] {*dest_ip_spec*} [*operator port* [*port*]] [**established**] [**precedence** *precedence*] [**tos** *tos*] [**capture**] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

For UDP, you can use the following syntax:

set security acl ip {*acl_name*} {**permit** | **deny** | **redirect** {*mod_num/port_num*}} [**udp** | **17**] {*src_ip_spec*} [*operator port* [*port*]] {*dest_ip_spec*} [*operator port* [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**capture**] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

Examples

These examples show different ways to use the **set security acl ip** commands to configure IP security ACL:

```
Console> (enable) set security acl ip IPACL1 deny 1.2.3.4 0.0.0.0
IPACL1 editbuffer modified.  Use ‘commit’ command to apply changes.
Console> (enable)

Console> (enable) set security acl ip IPACL1 deny host 171.3.8.2 before 2
IPACL1 editbuffer modified. Use ‘commit’ command to apply changes.
Console> (enable)

Console> (enable) set security acl ip IPACL1 permit any any
IPACL1 editbuffer modified. Use ‘commit’ command to apply changes.
Console> (enable)

Console> (enable) set security acl ip IPACL1 redirect 3/1 ip 3.7.1.2 0.0.0.255 host
255.255.255.255 precedence 1 tos min-delay
IPACL1 editbuffer modified. Use ‘commit’ command to apply changes.
Console> (enable)

Console> (enable) set security acl ip IPACL1 permit ip host 60.1.1.1 host 60.1.1.98
capture
IPACL1 editbuffer modified. Use ’commit’ command to apply changes.
```

Related Commands

clear security acl
clear security acl capture-ports
clear security acl map
commit
show security acl
show security acl capture-ports
set security acl map
set security acl capture-ports

set security acl ipx

Use the **set security acl ipx** command to create a new entry in a standard IPX VACL and to append the new entry at the end of the VACL.

set security acl ipx {*acl_name*} {**permit** | **deny** | **redirect** *mod_num/port_num*} {*protocol*} {*src_net*} [*dest_net.*[*dest_node*] [[*dest_net_mask.*]*dest_node_mask*]] [**capture**] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

Syntax Description

acl_name	Unique name that identifies the list to which the entry belongs.
permit	Keyword to allow traffic from the specified source IPX address.
deny	Keyword to block traffic from the specified source IPX address.
redirect	Keyword to redirect traffic from the specified source IPX address.
mod_num/port_num	Number of the module and port.
protocol	Keyword or number of an IPX protocol; valid values are from **0** to **255** representing an IPX protocol number. See the "Usage Guidelines" section for a list of valid keywords amd corresponding numbers.
src_net	Number of the network from which the packet is being sent. See the "Usage Guidelines" section for format guidelines.
dest_net.	(Optional) Number of the network from which the packet is being sent.
.*dest_node*	(Optional) Node on destination-network to which the packet is being sent.
dest_net_mask.	(Optional) Mask to be applied to the destination network. See the "Usage Guidelines" section for format guidelines.
dest_node_mask	(Optional) Mask to be applied to the destination-node. See the "Usage Guidelines" section for format guidelines.
capture	(Optional) Keyword to specify packets are switched normally and captured.
before *editbuffer_index*	(Optional) Keyword and variable to insert the new ACE in front of another ACE.
modify *editbuffer_index*	(Optional) Keyword and variable to replace an ACE with the new ACE.

Defaults

There are no default ACLs and no default ACL-VLAN mappings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Configurations you make by entering this command are saved to NVRAM and hardware only after you enter the **commit** command. Enter ACEs in batches and then enter the **commit** command to save all of them in NVRAM and in the hardware.

If you use the **capture** keyword, the ports that capture the traffic and transmit out are specified by entering the **set security acl capture-ports** command.

When you enter the ACL name, follow these naming conventions:

- Maximum of 32 characters long 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

Valid *protocol* keywords include **ncp** (17), **netbios** (20), **rip** (1), **sap** (4), and **spx** (5).

The *src_net* and *dest_net* variables are eight-digit hexadecimal numbers that uniquely identify network cable segments. When you specify the *src_net* or *dest_net*, use the following guidelines:

- It can be a number in the range 0 to FFFFFFFF. A network number of -1 or **any** matches all networks.
- You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.

The **.***dest_node* is a 48-bit value represented by a dotted triplet of 4-digit hexadecimal numbers (xxxx.xxxx.xxxx).

The *dest_net_mask* is an eight-digit hexadecimal mask. Place ones in the bit positions you want to mask. The mask must be immediately followed by a period, which must in turn be immediately followed by the destination-node-mask. You can enter this value only when *dest_node* is specified.

The *dest_node_mask* is a 48-bit value represented as a dotted triplet of 4-digit hexadecimal numbers (xxxx.xxxx.xxxx). Place ones in the bit positions you want to mask. You can enter this value only when *dest_node* is specified.

The *dest_net_mask* is an eight-digit hexadecimal number that uniquely identifies the network cable segment. It can be a number in the range 0 to FFFFFFFF. A network number of -1 or **any** matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA. Following are *dest_net_mask* examples:

- 123A
- 123A.1.2.3
- 123A.1.2.3 ffff.ffff.ffff
- 1.2.3.4 ffff.ffff.ffff.ffff

Use the **show security acl** command to display the list.

Examples

This example shows how to block traffic from a specified source IPX address:

```
Console> (enable) set security acl ipx IPXACL1 deny 1.a
IPXACL1 editbuffer modified. Use ‘commit’ command to apply changes.
Console> (enable)
```

This example shows how to deny traffic from hosts in specific subnet (10.1.2.0/8):

```
Console> (enable) set security acl ipx SERVER deny ip 10.1.2.0 0.0.0.255 host 10.1.1.100
IPXACL1 editbuffer modified. Use ‘commit’ command to apply changes.
Console> (enable)
```

Related Commands

clear security acl
clear security acl capture-ports
clear security acl map
commit
set security acl map
set security acl capture-ports
show security acl
show security acl capture-ports

set security acl log

Use the **set security acl log** command to configure the security ACL log table.

set security acl log maxflow *max_number*

set security acl log ratelimit *pps*

Syntax Description

maxflow *max_number*	Keyword and variable to specify the maximum flow pattern number in packets per second; valid values are from **256** to **2048**.
ratelimit *pps*	Keyword and variable to specify the redirect rate in packets per second; valid values are from **500** to **5000**.

Defaults

The default *max_number* is 500 pps and the default *ratelimit* is 2500 pps.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The command is supported on systems configured with Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) only.

The **set security acl log maxflow** command tries to allocate a new log table based on the maximum flow pattern number to store logged packet information. If successful, the new buffer replaces the old one and all flows in the old table are cleared. If either memory is not enough or the maximum number is over the limit, an error message is displayed and the command is dropped.

The **set security acl log ratelimit** command tries to set the redirect rate in packets per second. If the configuration is over the range, the command is discarded and the range is displayed on the console.

Examples

This example shows how to set the maximum flow:

```
Console> (enable) set security acl log maxflow 322
Log table size set to 322 flow entries.
Console> (enable)
```

This example shows how to set the rate limit:

```
Console> (enable) set security acl log ratelimit 3444
Max logging eligible packet rate set to 3444pps.
Console> (enable)
```

Related Commands

clear security acl log flow
set security acl log
show security acl log

set security acl mac

Use the **set security acl mac** command to create a new entry in a non-IP or non-IPX protocol VACL and to append the new entry at the end of the VACL.

set security acl mac {*acl_name*} {**permit** | **deny**} {*src_mac_addr_spec*} {*dest_mac_addr_spec*} [*ether-type*] [**capture**] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

Syntax Description

acl_name	Unique name that identifies the list to which the entry belongs.
permit	Keyword to allow traffic from the specified source MAC address.
deny	Keyword to block traffic from the specified source MAC address.
src_mac_addr_spec	Source MAC address and mask in the form *source_mac_address source_mac_address_mask.*
dest_mac_addr_spec	Destination MAC address and mask.
ether-type	(Optional) Number or name that matches the ethertype for Ethernet-encapsulated packets; valid values are **0x0600**, **0x0601**, **0x0BAD**, **0x0BAF**, **0x6000-0x6009**, **0x8038-0x8042**, **0x809b**, and **0x80f3**. See the "Usage Guidelines" section for a list of valid names.
capture	(Optional) Keyword to specify packets are switched normally and captured.
before *editbuffer_index*	(Optional) Keyword and variable to insert the new ACE in front of another ACE.
modify *editbuffer_index*	(Optional) Keyword and variable to replace an ACE with the new ACE.

Defaults

There are no default ACLs and no default ACL-VLAN mappings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Configurations you make by entering this command are saved to NVRAM and hardware only after you enter the **commit** command. Enter ACEs in batches and then enter the **commit** command to save all of them in NVRAM and in the hardware.

If you use the **capture** keyword, the ports that capture the traffic and transmit out are specified by entering the **set security acl capture-ports** command.

When you enter the ACL name, follow these naming conventions:

- Maximum of 32 characters long 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

The *src_mac_addr_spec* is a 48-bit source MAC address and mask and entered in the form of *source_mac_address source_mac_address_mask* (for example, 08-11-22-33-44-55 ff-ff-ff-ff-ff-ff). Place ones in the bit positions you want to mask. When you specify the *src_mac_addr_spec*, follow these guidelines:

- The *source_mask* is required; 0 indicates a care bit, 1 indicates a don't-care bit.
- Use a 32-bit quantity in four-part dotted-decimal format.
- Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.
- Use **host** source as an abbreviation for a *source* and *source-wildcard* of source 0.0.0.0.

The *dest_mac_spec* is a 48-bit destination MAC address and mask and entered in the form of *dest_mac_address dest_mac_address_mask* (for example, 08-00-00-00-02-00/ff-ff-ff-00-00-00). Place ones in the bit positions you want to mask. The destination mask is mandatory. When you specify the *dest_mac_spec*, use the following guidelines:

- Use a 48-bit quantity in 6-part dotted-hexadecimal format for a source address and mask.
- Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0-0-0-0-0-0 ff-ff-ff-ff-ff-ff.
- Use **host** source as an abbreviation for a *destination* and *destination-wildcard* of destination 0-0-0-0-0-0.

Valid names for ethertypes (and corresponding numbers) are Ethertalk (0x809B), AARP (0x8053), dec-mop-dump (0x6001), dec-mop-remote-console (0x6002), dec-phase-iv (0x6003), dec-lat (0x6004), dec-diagnostic-protocol (0x6005), dec-lavc-sca (0x6007), dec-amber (0x6008), dec-mumps (0x6009), dec-lanbridge (0x8038), dec-dsm (0x8039), dec-netbios (0x8040), dec-msdos (0x8041), banyan-vines-echo (0x0baf), xerox-ns-idp (0x0600), and xerox-address-translation (0x0601).

Use the **show security acl** command to display the list.

Examples

This example shows how to block traffic to an IP address:

```
Console> (enable) set security acl mac MACACL1 deny 01-02-02-03-04-05
MACACL1 editbuffer modified. User 'commit' command to apply changes.
Console> (enable)
```

Related Commands

clear security acl
clear security acl capture-ports
clear security acl map
commit
set security acl map
set security acl capture-ports
show security acl
show security acl capture-ports

set security acl map

Use the **set security acl map** command to map an existing VACL to a VLAN.

set security acl map *acl_name vlan*

Syntax Description

acl_name	Unique name that identifies the list to which the entry belongs.
vlan	Number of the VLAN to be mapped to the VACL; valid values are from **1** to **1005** and from **1025** to **4094**.

Defaults

There are no default ACLs and no default ACL-VLAN mappings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Configurations you make by entering this command are saved in NVRAM. This command *does not* require that you enter the **commit** command. Each VLAN can be mapped to only one ACL of each type (IP, IPX, and MAC). An ACL can be mapped to a VLAN only after you have committed the ACL.

When you enter the ACL name, follow these naming conventions:

- Maximum of 32 characters long 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

Caution Use the **copy** command to save the ACL configuration to Flash memory.

Examples

This example shows how to map an existing VACL to a VLAN:

```
Console> (enable) set security acl map IPACL1 1
ACL IPACL1 mapped to vlan 1
Console> (enable)
```

This example shows the output if you try to map an ACL that has not been committed:

```
Console> (enable) set security acl map IPACL1 1
Commit ACL IPACL1 before mapping.
Console> (enable)
```

This example shows the output if you try to map an ACL that is already mapped to a VLAN for the ACL type (IP, IPX, or MAC):

```
Console> (enable) set security acl map IPACL2 1
Mapping for this type already exists for this VLAN.
Console> (enable)
```

Related Commands

clear security acl
clear security acl map
commit
show security acl

set snmp access

Use the **set snmp access** command to define the access rights of an SNMP group.

set snmp access [**-hex**] {*groupname*} {**security-model** {**v1** | **v2c**}} [**read** [**-hex**] {*readview*}] [**write** [**-hex**] {*writeview*}] [**notify** [**-hex**] {*notifyview*}] [**volatile** | **nonvolatile**]

set snmp access [**-hex**] {*groupname*} {**security-model v3** {**noauthentication** | **authentication** | **privacy**}} [**read** [**-hex**] {*readview*}] [**write** [**-hex**] {*writeview*}] [**notify** [**-hex**] {*notifyview*}] [**context** [**-hex**] *contextname* [**exact** | **prefix**]] [**volatile** | **nonvolatile**]

Syntax Description

-hex	(Optional) Keyword to display the *groupname, readview, writeview, notifyview,* and *contextname* in a hexadecimal format.
groupname	Name of the SNMP group.
security-model v1 | **v2c**	Keywords to specify security-model v1 or v2c.
read *readview*	(Optional) Keyword and variable to specify the name of the view that allows you to see the MIB objects.
write *writeview*	(Optional) Keyword and variable to specify the name of the view that allows you to configure the contents of the agent.
notify *notifyview*	(Optional) Keyword and variable to specify the name of the view that allows you to send a trap about MIB objects.
v3	Keyword to specify security model v3.
noauthentication	Keyword to specify security model is not set to use authentication protocol.
authentication	Keyword to specify the type of authentication protocol.
privacy	Keyword to specify the messages sent on behalf of the user are protected from disclosure.
volatile	(Optional) Keyword to specify that the storage type is defined as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Keyword to specify that the storage type is defined as persistent memory and the content remains after the device is turned off and on again.
context *contextname*	(Optional) Keyword and variable to specify the name of the context string and the way to match the context string; maximum of 32 characters.
exact	(Optional) Keyword to specify that an exact match between the *contextname* and the value of vacmAccessContextPrefix is required to select this entry.
prefix	(Optional) Keyword to specify that only a match between vacmAccessContextPrefix and the starting portion of *contextname* is required to select this entry.

Defaults

The defaults are as follows:

- storage type is **nonvolatile**.
- **read** *readview* is Internet OID space.
- **write** *writeview* is NULL OID.
- **notify** *notifyview* is NULL OID.
- **context** *contextname* is a NULL string.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use special characters for *groupname*, *readview*, *writeview*, and *notifyview* (nonprintable delimiters for these parameters), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

readview is assumed to be every object belonging to the Internet (1.3.6.1) OID space; you can use the read option to override this state.

For *writeview*, you must also configure write access.

For *notifyview*, if a view is specified, any notifications in that view are sent to all users associated with the group (an SNMP server host configuration must exist for the user).

For *contextname*, the string is treated as either a full context name or the prefix of a context name, depending on whether you enter the **exact** or **prefix** keyword. If you enter the **prefix** keyword, this allows you to enter a simple form of wildcarding. For example, if you enter a *contextname* of vlan, vlan-1 and vlan-100 will be selected.

If you do not enter a context name, a NULL context string is used.

Examples

This example shows how to set the SNMP access rights for a group:

```
Console> (enable) set snmp access cisco-group security-model v3 authentication
SNMP access group was set to cisco-group version v3 level authentication, readview
internet, nonvolatile.
Console> (enable)
```

Related Commands

clear snmp access
show snmp access
show snmp context

set snmp community

Use the **set snmp community** command to set SNMP communities and associated access types.

set snmp community {**read-only** | **read-write** | **read-write-all**} [*community_string*]

Syntax Description

read-only	Keyword to assign read-only access to the specified SNMP community.
read-write	Keyword to assign read-write access to the specified SNMP community.
read-write-all	Keyword to assign read-write access to the specified SNMP community.
community_string	(Optional) Name of the SNMP community.

Defaults

The default is the following communities and access types are defined:

- public—**read-only**
- private—**read-write**
- secret—**read-write-all**

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

There are three configurable SNMP communities, one for each access type. If you do not specify the community string, the community string configured for that access type is cleared.

To support the access types, you also need to configure four MIB tables: vacmContextTable, vacmSecurityToGroupTable, vacmAccessTable, and vacmViewTreeFamilyTable. Use the **clear config snmp** command to reset these tables to the default values.

Examples

This example shows how to set read-write access to the SNMP community called yappledapple:

```
Console> (enable) set snmp community read-write yappledapple
SNMP read-write community string set to yappledapple.
Console> (enable)
```

This example shows how to clear the community string defined for read-only access:

```
Console> (enable) set snmp community read-only
SNMP read-only community string cleared.
Console> (enable)
```

Related Commands

clear config
clear snmp community
show snmp
show snmp community

set snmp extendedrmon netflow

Use the **set snmp extendedrmon netflow** command to enable or disable the SNMP extended RMON support for the NAM module.

set snmp extendedrmon netflow {**enable** | **disable**} {*mod*}

Syntax Description

enable	Keyword to enable the extended RMON support.
disable	Keyword to disable the extended RMON support.
mod	Module number of the extended RMON NAM.

Defaults

The default is SNMP-extended RMON NetFlow is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to enable SNMP-extended RMON NetFlow support:

```
Console> (enable) set snmp extendedrmon netflow enable 2
Snmp extended RMON netflow enabled
Console> (enable)
```

This example shows how to disable SNMP-extended RMON NetFlow support:

```
Console> (enable) set snmp extendedrmon netflow disable 2
Snmp extended RMON netflow disabled
Console> (enable)
```

This example shows the response when the SNMP-extended RMON NetFlow feature is not supported:

```
Console> (enable) set snmp extendedrmon enable 4
NAM card is not installed.
Console> (enable)
```

Related Commands

set snmp rmon
show snmp

set snmp group

Use the **set snmp group** command to establish the relationship between an SNMP group and a user with a specific security model.

set snmp group [**-hex**] {*groupname*} **user** [**-hex**] {*username*}
{**security-model** {**v1** | **v2c** | **v3**}} [**volatile** | **nonvolatile**]

Syntax Description

-hex	(Optional) Keyword to display the *groupname* and *username* in a hexadecimal format.
groupname	Name of the SNMP group that defines an access control; the maximum length is 32 bytes.
user	Keyword to specify the SNMP group username.
username	Name of the SNMP user that belongs to the SNMP group; the maximum length is 32 bytes.
security-model v1 | **v2c** | **v3**	Keywords to specify security-model v1, v2c, or v3.
volatile	(Optional) Keyword to specify that the storage type is defined as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Keyword to specify that the storage type is defined as persistent memory and the content remains after the device is turned off and on again.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use special characters for *groupname* or *username* (nonprintable delimiters for these parameters), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

Examples

This example shows how to set the SNMP group:

```
Console> (enable) set snmp group cisco-group user joe security-model v3
SNMP group was set to cisco-group user joe and version v3,nonvolatile.
Console> (enable)
```

Related Commands

clear snmp group
show snmp group

set snmp notify

Use the **set snmp notify** command to set the notifyname entry in the snmpNotifyTable and the notifytag entry in the snmpTargetAddrTable.

set snmp notify [**-hex**] {*notifyname*} **tag** [**-hex**] {*notifytag*}
[**trap** | **inform**] [**volatile** | **nonvolatile**]

Syntax Description

-hex	(Optional) Keyword to display the notifyname and notifytag in a hexadecimal format.
notifyname	Identifier to index the snmpNotifyTable.
tag	Keyword to specify the tag name in the taglist.
notifytag	Name of entries in the snmpTargetAddrTable.
trap	(Optional) Keyword to specify all messages that contain snmpv2-Trap PDUs.
inform	(Optional) Keyword to specify all messages that contain InfoRequest PDUs.
volatile	(Optional) Keyword to specify that the storage type is defined as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Keyword to specify that the storage type is defined as persistent memory and the content remains after the device is turned off and on again.

Defaults

The defaults are storage type is **volatile** and notify type is **trap**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use special characters for the *notifyname* and *notifytag* (nonprintable delimiters for these parameters), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

Examples

This example shows how to set the SNMP notify for a specific notifyname:

```
Console> (enable) set snmp notify hello tag world inform
SNMP notify name was set to hello with tag world notifyType inform, and storageType
nonvolatile.
Console> (enable)
```

Related Commands

clear snmp notify
show snmp notify

set snmp rmon

Use the **set snmp rmon** command to enable or disable SNMP RMON support.

set snmp rmon {**enable** | **disable**}

Syntax Description

enable	Keyword to activate SNMP RMON support.
disable	Keyword to deactivate SNMP RMON support.

Defaults

The default is RMON support is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

RMON statistics are collected on a segment basis.

The RMON feature deinstalls all of the domains for all of the interfaces on an Ethernet module that has been removed from the system.

When you enable RMON, the supported RMON groups for Ethernet ports are Statistics, History, Alarms, and Events as specified in RFC 1757.

Use of this command requires a separate software license.

Examples

This example shows how to enable RMON support:

```
Console> (enable) set snmp rmon enable
SNMP RMON support enabled.
Console> (enable)
```

This example shows how to disable RMON support:

```
Console> (enable) set snmp rmon disable
SNMP RMON support disabled.
Console> (enable)
```

Related Commands

show port counters

set snmp rmonmemory

Use the **set snmp rmonmemory** command to set the memory usage limit in percentage.

set snmp rmonmemory *percentage*

Syntax Description

percentage	Memory usage limit; see the "Usage Guidelines" section for additional information.

Defaults

The default is 85 percent.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

When using this command, setting the percentage value to 85 does not mean that RMON can use 85 percent of memory, it means that you cannot create new RMON entries or restore entries from the NVRAM if the memory usage exceeds 85 percent.

If you expect the device to run other sessions such as Telnet, a lower value should be set to the memory limit. Otherwise, the new Telnet sessions may fail because the available memory is not enough.

Examples

This example shows how to set the memory usage limit:

```
Console> (enable) set snmp rmonmemory 90
Console> (enable)
```

Related Commands

show snmp rmonmemory

set snmp targetaddr

Use the **set snmp targetaddr** command to configure the SNMP target address entries in the snmpTargetAddressTable.

set snmp targetaddr [**-hex**] {*addrname*} **param** [**-hex**] {*paramsname*}{*ipaddr*} [**udpport** {*port*}] [**timeout** {*value*}] [**retries** {*value*}] [**volatile** | **nonvolatile**] [**taglist** {[**-hex**] *tag*}] [[**-hex**] **tag** *tagvalue*]

Syntax Description

-hex	(Optional) Keyword to display *addrname*, *paramsname*, *tagvalue*, and *tag* in a hexadecimal format.
addrname	Unique identifier to index the snmpTargetAddrTable; the maximum length is 32 bytes.
param	Keyword to specify an entry in the snmpTargetParamsTable that provides parameters to be used when generating a message to the target; the maximum length is 32 bytes.
paramsname	Entry in the snmpTargetParamsTable; the maximum length is 32 bytes.
ipaddr	IP address of the target.
udpport *port*	(Optional) Keyword and variable to specify which UDP port of the target host to use.
timeout *value*	(Optional) Keyword and variable to specify the number of timeouts.
retries *value*	(Optional) Keyword and variable to specify the number of retries.
volatile	(Optional) Keyword to specify that the storage type is defined as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Keyword to specify that the storage type is defined as persistent memory and the content remains after the device is turned off and on again.
taglist *tag*	(Optional) Keyword and variable to specify a tag name in the taglist.
tag *tagvalue*	(Optional) Keyword and variable to specify the tag name.

Defaults

The defaults are as follows:

- storage type is **nonvolatile**.
- **udpport** is 162.
- **timeout** is 1500.
- **retries** is 3.
- **taglist** is NULL.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use special characters for the *addrname*, *paramsname*, *tag*, and *tagvalue* (nonprintable delimiters for these parameters), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

The maximum *tagvalue* and *taglist* length is 255 bytes.

Examples

This example shows how to set the target address in the snmpTargetAddressTable:

```
Console> (enable) set snmp targetaddr foo param bar 10.1.2.4 udp 160 timeout 10 retries 3
taglist tag1 tag2 tag3
SNMP targetaddr name was set to foo with param bar ipAddr 10.1.2.4, udpport 160, timeout
10, retries 3, storageType nonvolatile with taglist tag1 tag2 tag3.
Console> (enable)
```

Related Commands

clear snmp targetaddr
show snmp targetaddr

set snmp targetparams

Use the **set snmp targetparams** command to configure the SNMP parameters used in the snmpTargetParamsTable when generating a message to a target.

set snmp targetparams [**-hex**] {*paramsname*} **user** [**-hex**] {*username*} {**security-model** {**v1** | **v2c**}} {**message-processing** {**v1** | **v2c** | **v3**}} [**volatile** | **nonvolatile**]

set snmp targetparams [**-hex**] {*paramsname*} **user** [**-hex**] {*username*} {**security-model v3**} {**message-processing v3** {**noauthentication** | **authentication** | **privacy**}} [**volatile** | **nonvolatile**]

Syntax Description

-hex	(Optional) Keyword to display the *paramsname* and *username* in a hexadecimal format.
paramsname	Name of the parameter in the snmpTargetParamsTable; the maximum length is 32 bytes.
user	Keyword to specify the SNMP group username.
username	Name of the SNMP user that belongs to the SNMP group; the maximum length is 32 bytes.
security-model v1 | **v2c**	Keywords to specify security-model v1 or v2c.
message-processing v1 | **v2c** | **v3**	Keywords to specify the version number used by the message processing model.
security-model v3	Keyword to specify security-model v3.
message-processing v3	Keywords to specify v3 is used by the message-processing model.
noauthentication	Keyword to specify the security model is not set to use the authentication protocol.
authentication	Keyword to specify the type of authentication protocol.
privacy	Keyword to specify the messages sent on behalf of the user are protected from disclosure.
volatile	(Optional) Keyword to specify that the storage type is defined as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Keyword to specify that the storage type is defined as persistent memory and the content remains after the device is turned off and on again.

Defaults

The default storage type is **volatile**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use special characters for the *paramsname* and *username* (nonprintable delimiters for these parameters), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

Examples

This example shows how to set target parameters in the snmpTargetParamsTable:

```
Console> (enable) set snmp targetparams bar user joe security-model v3 message-processing
v3 authentication
SNMP target params was set to bar v3 authentication, message-processing v3, user joe
nonvolatile.
Console> (enable)
```

Related Commands

clear snmp targetparams
show snmp targetparams

set snmp trap

Use the **set snmp trap** command set to enable or disable the different SNMP traps on the system or to add an entry into the SNMP authentication trap receiver table.

set snmp trap {**enable** | **disable**} [**all** | **auth** | **bridge** | **chassis** | **config** | **entity** | **entityfru** | **envfan** | **envpower** | **envshutdown** | **ippermit** | **module** | **stpx** | **syslog** | **system** | **vmps** | **vtp**]

set snmp trap *rcvr_addr rcvr_community* [**port** *rcvr_port*] [**owner** *rcvr_owner*] [**index** *rcvr_index*]

Syntax Description

enable	Keyword to enable SNMP traps.
disable	Keyword to disable SNMP traps.
all	(Optional) Keyword to specify all trap types and all port traps. See the "Usage Guidelines" section before using this option.
auth	(Optional) Keyword to specify the authenticationFailure trap from RFC 1157.
bridge	(Optional) Keyword to specify the newRoot and topologyChange traps from RFC 1493 (the BRIDGE-MIB).
chassis	(Optional) Keyword to specify the chassisAlarmOn and chassisAlarmOff traps from the CISCO-STACK-MIB.
config	(Optional) Keyword to specify the sysConfigChange trap from the CISCO-STACK-MIB.
entity	(Optional) Keyword to specify the entityMIB trap from the ENTITY-MIB.
entityfru	(Optional) Keyword to specify the entity field replaceable unit (FRU).
envpower	(Optional) Keyword to specify the environmental power.
envshutdown	(Optional) Keyword to specify the environmental shutdown.
ippermit	(Optional) Keyword to specify the IP Permit Denied access from the CISCO-STACK-MIB.
module	(Optional) Keyword to specify the moduleUp and moduleDown traps from the CISCO-STACK-MIB.
stpx	(Optional) Keyword to specify the STPX trap.
syslog	(Optional) Keyword to specify the syslog notification traps.
system	(Optional) Keyword to specify the system.
vmps	(Optional) Keyword to specify the vmVmpsChange trap from the CISCO-VLAN-MEMBERSHIP-MIB.
vtp	(Optional) Keyword to specify the VTP from the CISCO-VTP-MIB.
rcvr_addr	IP address or IP alias of the system to receive SNMP traps.
rcvr_community	Community string to use when sending authentication traps.
port *rcvr_port*	(Optional) Keyword and variable to specify the UDP port and port number; valid values are from **0** to **65535**.

owner *rcvr_owner*	(Optional) Keyword and variable to specify the user who configured the settings for the SNMP trap; the valid value is a character string from 1 to 21 characters in length.
index *rcvr_index*	(Optional) Keyword and variable variable to specify index entries with the same *rcvr_addr*; valid values are from **0** to **65535**.

Defaults

The default is SNMP traps are disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

An IP permit trap is sent when unauthorized access based on the IP permit list is attempted.

Use the **show snmp** command to verify the appropriate traps were configured.

To use this command, you must configure all notification tables including the snmpTargetAddrTable, snmpTargetParamsTable, and snmpNotifyTable tables.

Use the **all** option to enable or disable all trap types and all port traps.

Use the **set port trap** command to enable or disable a single port or a range of ports.

The *rcvr_index* is required only when you want to enter another entry with the same *rcvr_addr*.

Examples

This example shows how to enable SNMP chassis traps:

```
Console> (enable) set snmp trap enable chassis
SNMP chassis alarm traps enabled.
Console> (enable)
```

This example shows how to enable all traps:

```
Console> (enable) set snmp trap enable
All SNMP traps enabled.
Console> (enable)
```

This example shows how to disable SNMP chassis traps:

```
Console> (enable) set snmp trap disable chassis
SNMP chassis alarm traps disabled.
Console> (enable)
```

This example shows how to add an entry in the SNMP trap receiver table:

```
Console> (enable) set snmp trap 192.122.173.42 public
SNMP trap receiver added.
Console> (enable)
```

Related Commands

clear snmp trap
set port trap
show snmp
test snmp trap

set snmp user

Use the **set snmp user** command to configure a new SNMP user.

set snmp user [**-hex**] {*username*} {**remote** {*engineid*}} [**authentication** {**md5** | **sha** | *authpassword*}] [**privacy** {*privpassword*}] [**volatile** | **nonvolatile**]

Syntax Description

-hex	(Optional) Keyword to display *username* in a hexadecimal format.
username	Name of the SNMP user.
remote *engineid*	Keyword and variable to specify the remote SNMP engine ID.
authentication	(Optional) Keyword to specify the authentication protocol.
md5	Keyword to specify HMAC-MD5-96 authentication protocol.
sha	Keyword to specify HMAC-SHA-96 authentication protocol.
authpassword	Password for authentication.
privacy *privpassword*	(Optional) Keyword and variable to enable the host to encrypt the contents of the message sent to or from the agent; the maximum length is 32 bytes.
volatile	(Optional) Keyword to specify that the storage type is defined as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Keyword to specify that the storage type is defined as persistent memory and the content remains after the device is turned off and on again.

Defaults

The default storage type is **volatile**. If you do not specify **authentication**, the security level default will be **noauthentication**. If you do not specify **privacy**, the default will be no privacy.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use special characters for *username* (nonprintable delimiters for this parameter), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

authpassword and *privpassword* must be hexadecimal characters without delimiters in between.

Examples

This example shows how to set a specific username:

```
Console> (enable) set snmp user joe
Snmp user was set to joe authProt no-auth  privProt no-priv with engineid 00:00.
Console> (enable)
```

This example shows how to set a specific username, authentication, and authpassword:

```
Console> (enable) set snmp user John authentication md5 arizona2
Snmp user was set to John authProt md5 authPasswd arizona2. privProt no-priv wi.
Console> (enable)
```

Related Commands

clear snmp user
show snmp user

set snmp view

Use the **set snmp view** command to configure the SNMP MIB view.

set snmp view [**-hex**]{*viewname*}{*subtree*}[**mask**] [**included** | **excluded**] [**volatile** | **nonvolatile**]

Syntax Description

-hex	(Optional) Keyword to display the *viewname* in a hexadecimal format.
viewname	Name of a MIB view.
subtree	MIB subtree.
mask	(Optional) Keyword to specify that the bit mask is used with the subtree. A bit mask can be all ones, all zeros, or any combination; the maximum length is 3 bytes.
included | **excluded**	(Optional) Keywords to specify that the MIB subtree is included or excluded.
volatile	(Optional) Keyword to specify that the storage type is defined as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Keyword to specify that the storage type is defined as persistent memory and the content remains after the device is turned off and on again.

Defaults

The defaults are as follows:

- Storage type is **volatile**.
- Bit mask is NULL.
- MIB subtree is included.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use special characters for *viewname* (nonprintable delimiters for this parameter), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

A MIB subtree with a mask defines a view subtree. The MIB subtree can be in OID format or a text name mapped to a valid OID.

Examples

This example shows how to assign a subtree to the view public:

```
Console> (enable) set snmp view public 1.3.6.1 included
Snmp view name was set to public with subtree 1.3.6.1 included, nonvolatile.
Control> (enable)
```

This example shows the response when the subtree is incorrect:

```
Console> (enable) set snmp view stats statistics excluded
Statistics is not a valid subtree OID
Control> (enable)
```

Related Commands

clear snmp view
show snmp view

set span

Use the **set span** command to enable or disable SPAN and to set up the switch port and VLAN analyzer for multiple SPAN sessions.

set span disable [*dest_mod/dest_port* | **all**]

set span {*src_mod/src_ports* | *src_vlans* | **sc0**} {*dest_mod/dest_port*} [**rx** | **tx** | **both**] [**inpkts** {**enable** | **disable**}] [**learning** {**enable** | **disable**}] [**multicast** {**enable** | **disable**}] [**filter** *vlans*...] [**create**]

Syntax Description

disable	Keyword to disable SPAN.
dest_mod	(Optional) Monitoring module (SPAN destination).
dest_port	(Optional) Monitoring port (SPAN destination).
all	(Optional) Keyword to disable all SPAN sessions.
src_mod	Monitored module (SPAN source).
src_ports	Monitored ports (SPAN source).
src_vlans	Monitored VLANs (SPAN source).
sc0	Keyword to specify the inband port is a valid source.
rx	(Optional) Keyword to specify that information received at the source (ingress SPAN) is monitored.
tx	(Optional) Keyword to specify that information transmitted from the source (egress SPAN) is monitored.
both	(Optional) Keyword to specify that information both transmitted from the source (ingress SPAN) and received (egress SPAN) at the source are monitored.
inpkts enable	(Optional) Keywords to enable the receiving of normal inbound traffic on the SPAN destination port.
inpkts disable	(Optional) Keywords to disable the receiving of normal inbound traffic on the SPAN destination port.
learning enable	(Optional) Keywords to enable learning for the SPAN destination port.
learning disable	(Optional) Keywords to disable learning for the SPAN destination port.
multicast enable	(Optional) Keywords to enable monitoring multicast traffic (egress traffic only).
multicast disable	(Optional) Keywords to disable monitoring multicast traffic (egress traffic only).
filter *vlans*	(Optional) Keyword and variable to monitor traffic on selected VLANs on source trunk ports.
create	(Optional) Keyword to create a SPAN port.

Defaults

The default is SPAN is disabled, no VLAN filtering is enabled, multicast is enabled, input packets are disabled, and learning is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

After you enable SPAN, system defaults are used if no parameters were ever set. If you changed parameters, the old parameters are stored in NVRAM, and the new parameters are used.

Use a network analyzer to monitor ports.

If you specify multiple SPAN source ports, the ports can belong to different VLANs.

A maximum of two **rx** or **both** SPAN sessions and four **tx** SPAN sessions can exist simultaneously. If you use a remote SPAN station, the maximum number of **rx** or **both** SPAN sessions is one.

Use the **inpkts** keyword with the **enable** option to allow the SPAN destination port to receive normal incoming traffic in addition to the traffic mirrored from the SPAN source. Use the **disable** option to prevent the SPAN destination port from receiving normal incoming traffic.

You can specify an MSM port as the SPAN source port. However, you cannot specify an MSM port as the SPAN destination port.

When you enable the **inpkts** option, a warning message notifies you that the destination port does not join STP and may cause loops if this option is enabled.

When you configure multiple SPAN sessions, the destination module number/port number must be known to index the particular SPAN session.

If you do not specify the keyword **create** and you have only one session, the session will be overwritten. If a matching destination port exists, the particular session will be overwritten (with or without specifying **create**). If you specify the keyword **create** and there is no matching destination port, the session will be created.

If any VLANs on SPAN source port(s) are blocked by spanning tree, you may see extra packets transmitted on the destination port that were not actually transmitted out of the source port(s). The extra packets seen at the destination port are packets sent through the switch fabric to the source port and then blocked by spanning tree at the source port.

Examples

This example shows how to configure SPAN so that both transmit and receive traffic from port 1/1 (the SPAN source) is mirrored on port 2/1 (the SPAN destination):

```
Console> (enable) set span 1/1 2/1
Enabled monitoring of Port 1/1 transmit/receive traffic by Port 2/1
Console> (enable)
```

This example shows how to set VLAN 522 as the SPAN source and port 2/1 as the SPAN destination:

```
Console> (enable) set span 522 2/1
Enabled monitoring of VLAN 522 transmit/receive traffic by Port 2/1
Console> (enable)
```

This example shows how to set VLAN 522 as the SPAN source and port 3/12 as the SPAN destination. Only transmit traffic is monitored. Normal incoming packets on the SPAN destination port are allowed:

```
Console> (enable) set span 522 2/12 tx inpkts enable
SPAN destination port incoming packets enabled.
Enabled monitoring of VLAN 522 transmit traffic by Port 2/12
Console> (enable)
```

This example shows how to set port 3/2 as the SPAN source and port 2/2 as the SPAN destination:

```
Console> (enable) set span 3/2 2/2 tx create
Enabled monitoring of port 3/2 transmit traffic by Port 2/1
Console> (enable)
```

This example shows how to disable SPAN if multiple SPAN sessions are not defined:

```
Console> (enable) set span disable
This command WILL disable your span session(s).
Do you want to continue (y/n) [n]?y
Disabled all sessions
Console> (enable)
```

This example shows what happens if you try to enter the **set span disable** command (without the destination module number/port number defined) and multiple SPAN sessions are defined:

```
Console> (enable) set span disable
Multiple active span sessions. Please specify span destination to disable.
Console> (enable)
```

Related Commands

clear config
show span

set spantree backbonefast

Use the **set spantree backbonefast** command to enable or disable the spanning tree BackboneFast Convergence feature.

set spantree backbonefast {**enable** | **disable**}

Syntax Description

enable	Keyword to enable BackboneFast Convergence.
disable	Keyword to disable BackboneFast Convergence.

Defaults

The default is BackboneFast convergence is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

This command is not available in MISTP mode.

This command is not available in MST mode.

For BackboneFast Convergence to work, you must enable it on all switches in the network.

When you try to enable BackboneFast and the switch is in MISTP or MISTP-PVST+ mode, this message displays:

```
Cannot enable backbonefast when the spantree mode is MISTP-PVST+.
```

Examples

This example shows how to enable BackboneFast Convergence:

```
Console> (enable) set spantree backbonefast enable
Backbonefast enabled for all VLANs.
Console> (enable)
```

Related Commands

show spantree

set spantree bpdu-skewing

Use the **set spantree bpdu-skewing** command to enable or disable collection of the spanning tree BPDU skewing detection statistics.

set spantree bpdu-skewing {**enable** | **disable**}

Syntax Description

enable	Keyword to enable BPDU skewing detection statistics collection.
disable	Keyword to disable BPDU skewing detection statistics collection.

Defaults

The default is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

You can use this command to troubleshoot slow network convergence due to skewing. Skewing occurs when spanning tree timers lapse, expected BPDUs are not received, and spanning tree detects topology changes. The difference between the expected result and the BPDUs actually received is a "skew." The skew causes BPDUs to reflood the network to keep the spanning tree topology database up to date.

Examples

This example shows how to enable the BPDU skew detection feature:

```
Console> (enable) set spantree bpdu-skewing enable
Spantree bpdu-skewing enabled on this switch.
Console> (enable)
```

This example shows how to disable the BPDU skew detection feature:

```
Console> (enable) set spantree bpdu-skewing disable
Spantree bpdu-skewing disabled on this switch.
Console> (enable)
```

Related Commands

show spantree bpdu-skewing

set spantree channelcost

Use the **set spantree channelcost** command to set the channel path cost and to automatically adjust the channel port costs.

set spantree channelcost {*channel_id* | **all**} *cost*

Syntax Description

channel_id	Channel identification number.
all	Keyword to configure all channels.
cost	Channel port costs.

Defaults

The port cost is updated automatically based on the current port costs of the channeling ports.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can use this command when your switch is in LACP channel mode or in PAgP channel mode.

For differences between PAgP and LACP, refer to the "Guidelines for Port Configuration" section of the "Configuring EtherChannel" chapter of the *Catalyst 6000 Family Software Configuration Guide*.

Examples

This example shows how to set the channel 768 path cost to 12.

```
Console> (enable) set spantree channelcost 768 12
Port(s) 1/1-2 port path cost are updated to 19.
Channel 768 cost is set to 12.
Warning: channel cost may not be applicable if channel is broken.
Console> (enable)
```

This example shows how to set all channel path costs to 15:

```
Console> (enable) set spantree channelcost all 15
Port(s) 1/1-2 port path cost are updated to 24.
Channel 768 cost is set to 15.
Port(s) 4/3-4 cost is set to 15.
channel 769 cost is set to 15.
Port(s) 4/7-8 cost is set to 15.
channel 770 cost is set to 15.
Warning: channel cost may not be applicable if channel is broken.
Console> (enable)
```

Related Commands

- clear lacp-channel statistics
- set channelprotocol
- set lacp-channel system-priority
- set port lacp-channel
- set spantree channelcost
- set spantree channelvlancost
- show lacp-channel
- show port lacp-channel

set spantree channelvlancost

Use the **set spantree channelvlancost** command to set the channel VLAN path cost and adjust the port VLAN costs of the ports that belong to the channel.

set spantree channelvlancost *channel_id cost*

Syntax Description

channel_id	Number of the channel identification.
cost	Port costs of the ports in the channel.

Defaults

The command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You must set the channel VLAN cost one channel at a time.

You can use this command when your system is in LACP channel mode or PAgP channel mode.

For differences between PAgP and LACP, refer to the "Guidelines for Port Configuration" section of the "Configuring EtherChannel" chapter of the *Catalyst 6000 Family Software Configuration Guide*.

Examples

This example shows how to set the VLAN cost to 10 for channel 768:

```
Console> (enable) set spantree channelvlancost 768 10
Port(s) 1/1-2 vlan cost are updated to 24.
Channel 768 vlancost is set to 10.
Console> (enable)
```

Related Commands

clear lacp-channel statistics
set channelprotocol
set lacp-channel system-priority
set port lacp-channel
set spantree channelcost
show lacp-channel
show port lacp-channel

set spantree defaultcostmode

Use the **set spantree defaultcostmode** command to specify the spanning tree default port cost mode.

set spantree defaultcostmode {**short** | **long**}

Syntax Description

short	Keyword to set the default port cost for port speeds slower than 10 Gb.
long	Keyword to set the default port cost mode port speeds of 10 Gb and faster.

Defaults

The default is short.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set spantree defaultcostmode long** command is available in PVST+ mode only. If you enter this command in MISTP or MISTP-PVST+ mode, this message displays:

```
In MISTP or MISTP-PVST+ mode, default portcost and portinstancecost always
use long format default values.
```

All switches in a network must have the same default. If any switch in the network supports port speeds of 10 Gb and greater, the default cost mode must be set to **long** on all the switches in the network.

For port speeds of 1 Gb and greater, the default port cost should be set to **long**. For port speeds less than 10 Gb, the default port cost can be set to **short**.

The default path cost is based on port speed; see Table 2-21 and Table 2-22 for default settings.

Table 2-21 Default Port Cost—Short Mode

Port Speed	Default Port Cost
4 Mb	250
10 Mb	100
16 Mb	62
100 Mb	19
155 Mb	14
1 Gb	4
10 Gb	2

Table 2-22 Default Port Cost—Long Mode

Port Speed	Default Port Cost
100 Kb	200,000,000
1 Mb	20,000,000
10 Mb	2,000,000
100 Mb	200,000
1 Gb	20,000
10 Gb	2,000
100 Gb	200
1 Tb	20
10 Tb	2

Examples

This example shows how to set the spanning tree default port cost mode:

```
Console> (enable) set spantree defaultcostmode long
Portcost and portvlancost set to use long format default values.
Console> (enable)
```

Related Commands

show spantree defaultcostmode

set spantree disable

Use the **set spantree disable** command to disable the spanning tree algorithm for all VLANs or a specific VLAN or disable spanning tree instance.

set spantree disable *vlan*

set spantree disable all

set spantree disable mistp-instance *instance*

set spantree disable mistp-instance all

Syntax Description

vlan	Number of the VLAN; valid values are from **1** to **1005** and from **1025** to **4094**.
all	Keyword to specify all VLANs.
mistp-instance *instance*	Keyword and variable to specify the instance number; valid values are from **1** to **16**.
mistp-instance all	Keywords to delete all instances.

Defaults

The default is spanning tree is enabled, and all instances are enabled (flooding disabled).

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

If you do not specify a VLAN number or an instance number, 1 is assumed.

When an instance is enabled, the Spanning Tree Protocol starts running on that instance.

When an instance is disabled, the switch stops sending out config TLVs for that instance and starts flooding incoming TLVs for the same instance (but checks the VLAN mapping on the incoming side). All the traffic running on the VLANs mapped to the instance is flooded as well.

This command is not available in MST mode.

Examples

This example shows how to disable the spanning tree for VLAN 1:

```
Console> (enable) set spantree disable 1
VLAN 1 bridge spanning tree disabled.
Console> (enable)
```

This example shows how to disable spanning tree for a specific instance:

```
Console> (enable) set spantree disable mistp-instance 2
MI-STP instance 2 disabled.
Console> (enable)
```

Related Commands

set spantree enable
show spantree

set spantree enable

Use the **set spantree enable** command to enable the spanning tree algorithm for all VLANs, a specific VLAN, a specific instance, or all instances.

set spantree enable *vlans*

set spantree enable all

set spantree enable mistp-instance *instance*

set spantree enable mistp-instance all

Syntax Description

vlans	Number of the VLAN; valid values are from **1** to **1005** and from **1025** to **4094**.
all	Keyword to specify all VLANs.
mistp-instance *instance*	Keyword and variable to specify the instance number; valid values are from **1** to **16**.
mistp-instance all	Keywords to enable all instances.

Defaults

The default is enabled, and all instances are enabled (flooding disabled).

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

MISTP and VTP pruning cannot be enabled at the same time.

If you do not specify a VLAN number or an instance number, 1 is assumed.

This command is not available in MST mode.

Examples

This example shows how to activate spanning tree for VLAN 1:

```
Console> (enable) set spantree enable 1
VLAN 1 bridge spanning tree enabled.
Console> (enable)
```

This example shows how to activate spanning tree for an instance:

```
Console> (enable) set spantree enable mistp-instance 1
-STP instance 1 enabled.
Console> (enable)
```

Related Commands set spantree disable
show spantree

set spantree fwddelay

Use the **set spantree fwddelay** command to set the bridge forward delay for a VLAN or an instance.

set spantree fwddelay *delay* [*vlans*]

set spantree fwddelay *delay* **mistp-instance** [*instances*]

set spantree fwddelay *delay* **mst**

Syntax Description

delay	Number of seconds for the bridge forward delay; valid values are from **4** to **30** seconds.
vlans	(Optional) Number of the VLAN; valid values are from **1** to **1005** and from **1025** to **4094**.
mistp-instance *instances*	Keyword and optional variable to specify the instance number; valid values are from **1** to **16**.
mst	Keyword to set the forward delay time for the IST instance and all MST instances; see the "Usage Guidelines" section for more information.

Defaults

The default is the bridge forward delay is set to 15 seconds for all VLANs.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not specify a VLAN number or an instance number, 1 is assumed.

This command is not supported by the NAM.

If you enable MISTP, you cannot set the VLAN bridge forward delay.

If you enable PVST+, you cannot set the instance bridge forward delay.

If you enter the **set spantree fwddelay** *delay* **mst** command, you set the forward delay time for the IST instance and all MST instances. You do not need to set the forward delay time for each MST instance.

Examples

This example shows how to set the bridge forward delay for VLAN 100 to 16 seconds:

```
Console> (enable) set spantree fwddelay 16 100
Spantree 100 forward delay set to 16 seconds.
Console> (enable)
```

This example shows how to set the bridge forward delay for an instance to 16 seconds:

```
Console> (enable) set spantree fwddelay 16 mistp-instance 1
Instance 1 forward delay set to 16 seconds.
Console> (enable)
```

This example shows how to set the bridge forward delay for the IST and all MST instances to 15 seconds:

```
Console> (enable) set spantree fwddelay 15 mst
MST forward delay set to 15 seconds.
Console> (enable)
```

Related Commands **show spantree**

set spantree global-default

Use the **set spantree global-default** command to set the global states on the switch.

set spantree global-default portfast {**enable** | **disable**}

set spantree global-default loop-guard {**enable** | **disable**}

set spantree global-default bpdu-guard {**enable** | **disable**}

set spantree global-default bpdu-filter {**enable** | **disable**}

Syntax Description

portfast	Keyword to set the global PortFast state.
enable	Keyword to enable the global state.
disable	Keyword to disable the global state.
loop-guard	Keyword to set the global loop guard state.
bpdu-guard	Keyword to set the global BPDU guard state.
bpdu-filter	Keyword to set the global BPDU filter state.

Defaults

All ports are in nonedge state.

Loop guard is disabled on all ports.

BPDU guard is disabled on all ports.

BPDU filter is disabled on all ports.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to disable the global PortFast state on the switch:

```
Console> (enable) set spantree global-default portfast disable
Spantree global portfast state disabled on this switch.
Console> (enable)
```

This example shows how to enable the global loop guard state on the switch:

```
Console> (enable) set spantree global-default loop-guard enable
Spantree global loop-guard state enabled on the switch.
Console> (enable)
```

This example shows how to disable the global BPDU guard state on the switch:

```
Console> (enable) set spantree global-default bpdu-guard disable
Spantree global-default bpdu-guard disabled on this switch.
Console> (enable)
```

This example shows how to disable the global BPDU filter state on the switch:

```
Console> (enable) set spantree global-default bpdu-filter disable
Spantree global-default bpdu-filter disabled on this switch.
Console> (enable)
```

Related Commands

clear spantree mst
set spantree mst config
set spantree mst redetect-protocol
set spantree portfast bpdu-filter
set spantree portfast bpdu-guard
show spantree mst config

set spantree guard

Use the **set spantree guard** command to enable or disable the spanning tree root guard or loop guard feature on a per-port basis.

set spantree guard {**none** | **root** | **loop**} *mod/port*

Syntax Description

none	Keyword to disable the spanning tree guard feature.
root	Keyword to enable the root guard feature.
loop	Keyword to enable the loop guard feature.
mod/port	Number of the module and ports on the module.

Defaults

The default is root guard and loop guard are disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you enable loop guard on a channel and the first link becomes unidirectional, loop guard will block the entire channel until the affected port is removed from the channel.

You can use the root guard feature to prevent switches from becoming the root switch. The root guard feature forces a port to become a designated port so that no switch on the other end of the link can become a root switch.

When you enable root guard, it is automatically applied to all of the active instances or VLANs to which that port belongs. When you disable root guard, it is disabled for the specified ports. If a port goes into the root-inconsistent state, it automatically goes into the listening state. Disabling loop guard moves all loop-inconsistent ports to the listening state.

When using the loop guard feature, follow these guidelines:

- Use care when enabling loop guard. Loop guard is useful only in those topologies where there are blocked ports. Topologies where there are no blocked ports are loop free by definition and do not need this feature to be enabled.
- Enable loop guard only on root and alternate root ports.
- Use loop guard mainly on access switches.
- You cannot enable loop guard on PortFast-enabled or dynamic VLAN ports.
- You cannot enable PortFast on loop guard-enabled ports.
- You cannot enable loop guard if root guard is enabled.

Examples

This example shows how to enable root guard:

```
Console> (enable) set spantree guard root 5/1
Rootguard on port 5/1 is enabled.
Warning!! Enabling rootguard may result in a topolopy change.
Console> (enable)
```

This example shows how to enable the loop guard feature:

```
Console> (enable) set spantree guard loop 5/1
Rootguard is enabled on port 5/1, enabling loopguard will disable rootguard on
 this port.
Do you want to continue (y/n) [n]? y
Loopguard on port 5/1 is enabled.
Console> (enable)
```

Related Commands

show spantree guard

set spantree hello

Use the **set spantree hello** command to set the bridge hello time for a VLAN or an instance.

set spantree hello *interval* [*vlans*]

set spantree hello *interval* **mistp-instance** *instances*

set spantree hello *interval* **mst**

Syntax Description

interval	Number of seconds the system waits before sending a bridge hello message (a multicast message indicating that the system is active); valid values are from **1** to **10** seconds.
vlans	(Optional) Number of the VLAN; valid values are from **1** to **1005** and from **1025** to **4094**.
mistp-instance *instances*	Keyword and variable to specify the instance number; valid values are from **1** to **16**.
mst	Keyword to set the hello time for the IST instance and all MST instances. See the "Usage Guidelines" section for more information.

Defaults

The default is the bridge hello time is set to 2 seconds for all VLANs.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not specify a VLAN number or an instance number, 1 is assumed.

This command is not supported by the NAM.

If you enable MISTP, you cannot set the VLAN hello time.

If you enable PVST+, you cannot set the instance hello time.

If you enter the **set spantree hello** *interval* **mst** command, you set the hello time for the IST instance and all MST instances. You do not need to set the hello time for each MST instance.

Examples

This example shows how to set the spantree hello time for VLAN 100 to 3 seconds:

```
Console> (enable) set spantree hello 3 100
Spantree 100 hello time set to 3 seconds.
Console> (enable)
```

This example shows how to set the spantree hello time for an instance to 3 seconds:

```
Console> (enable) set spantree hello 3 mistp-instance 1
Spantree 1 hello time set to 3 seconds.
Console> (enable)
```

This example shows how to set the spantree hello time for the IST and all MST instances to 2 seconds:

```
Console> (enable) set spantree hello 2 mst
MST hello time set to 2 seconds.
Console> (enable)
```

Related Commands show spantree

set spantree macreduction

Use the **set spantree macreduction** command to enable or disable the spanning tree MAC address reduction feature.

set spantree macreduction enable | **disable**

Syntax Description

enable	Keyword to enable MAC address reduction.
disable	Keyword to disable MAC address reduction.

Defaults

The default is MAC address reduction is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The MAC address reduction feature is used to enable extended-range VLAN identification and allows the switch to support a large number of spanning tree instances with a very limited number of MAC addresses and still maintain the IEEE 802.1D bridge-ID requirement for each STP instance.

You cannot disable this feature if extended-range VLANs exist.

You cannot disable this feature on chassis with 64 MAC addresses.

Examples

This example shows how to disable the MAC address reduction feature:

```
Console> (enable) set spantree macreduction disable
MAC address reduction disabled
Console> (enable)
```

Related Commands

show spantree

set spantree maxage

Use the **set spantree maxage** command to set the bridge maximum aging time for a VLAN or an instance.

set spantree maxage *agingtime* [*vlans*]

set spantree maxage *agingtime* **mistp-instance** *instances*

set spantree maxage *agingtime* **mst**

Syntax Description

agingtime	Maximum number of seconds that the system retains the information received from other bridges through Spanning Tree Protocol; valid values are from **6** to **40** seconds.
vlans	(Optional) Number of the VLAN; valid values are from **1** to **1005** and from **1025** to **4094**.
mistp-instance *instances*	Keyword and variable to specify the instance number; valid values are from **1** to **16**.
mst	Keyword to set the maximum aging time for the IST instance and all MST instances. See the "Usage Guidelines" section for more information.

Defaults

The default configuration is 20 seconds for all VLANs.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not specify a VLAN number or an instance number, 1 is assumed.

This command is not supported by the NAM.

If you enable MISTP, you cannot set the VLAN maximum aging time.

If you enable PVST+, you cannot set the instance maximum aging time.

If you enter the **set spantree maxage** *agingtime* **mst** command, you set the maximum aging time for the IST instance and all MST instances. You do not need to set the maximum aging time for each MST instance.

Examples

This example shows how to set the maximum aging time for VLAN 1000 to 25 seconds:

```
Console> (enable) set spantree maxage 25 1000
Spantree 1000 max aging time set to 25 seconds.
Console> (enable)
```

This example shows how to set the maximum aging time for an instance to 25 seconds:

```
Console> (enable) set spantree maxage 25 mistp-instance 1
Instance 1 max aging time set to 25 seconds.
Console> (enable)
```

This example shows how to set the maximum aging time for the IST and all MST instances to 20 seconds:

```
Console> (enable) set spantree maxage 20 mst
MST max age set to 20 seconds.
Console> (enable)
```

Related Commands **show spantree**

set spantree mode

Use the **set spantree mode** command to configure the type of Spanning Tree Protocol mode to run.

set spantree mode {**mistp** | **pvst+** | **mistp-pvst+** | **mst**}

Syntax Description

mistp	Keyword to specify MISTP mode.
pvst+	Keyword to specify PVST+ mode.
mistp-pvst+	Keywords to allow the switch running MISTP to tunnel BPDUs with remote switches running PVST+.
mst	Keyword to specify MST mode.

Defaults

The default is PVST+.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

When you connect through Telnet into a switch and try to change the spanning tree mode from PVST+ to MISTP or MISTP-PVST+, and no VLANs are mapped to any instance on that switch, this warning message displays:

```
Console> (enable) set spantree mode mistp
Warning!! Changing the STP mode from a telnet session will disconnect the
session because there are no VLANs mapped to any MISTP instance.
Do you want to continue [n]?
```

When you connect through Telnet into a switch and try to change the spanning tree mode from MISTP or MISTP-PVST+ to PVST+, or when you connect through Telnet into a switch and try to change the spanning tree mode from PVST+ to MISTP or MISTP-PVST+ and additional VLAN-instance mappings are on that switch, this warning message displays:

```
Console> (enable) set spantree mode pvst+
Warning!! Changing the STP mode from a telnet session might disconnect the
session.
Do you want to continue [n]?
```

When you change from MISTP to PVST+ and over 8000 VLAN ports are currently configured on the switch, this warning message displays:

```
Console> (enable) set spantree mode pvst+
Warning!! This switch has 12345 VLAN-ports currently configured for STP.
Going out of MISTP mode could impact system performance.
Do you want to continue [n]?
```

If you change the spanning tree mode from PVST+ to MISTP or MISTP to PVST+, the STP mode previously running stops, all the information collected at runtime is used to build the port database for the new mode, and the new STP mode restarts the computation of the active topology from zero. All the parameters of the previous STP per VLAN or per instance are kept in NVRAM.

If you change the spanning tree mode from PVST+ to MISTP or MISTP to PVST+ and BackboneFast is enabled, this message displays:

```
Console> (enable) set spantree mode mistp
Cannot change the spantree mode to MISTP when backbonefast is enabled.
```

Examples

This example shows how to set the spanning tree mode to PVST+:

```
Console> (enable) set spantree mode pvst+
Warning!! Changing the STP mode from a telnet session might disconnect the session.
Do you want to continue [n]? y
Spantree mode set to PVST+.
Console> (enable)
```

This example shows what happens if you change the spanning tree mode from PVST+ to MISTP:

```
Console> (enable) set spantree mode mistp
Warning!! Changing the STP mode from a telnet session will disconnect the session because
there are no VLANs mapped to any MISTP instance.
Do you want to continue [n]? y
Console> (enable)
```

This example shows how to set the spanning tree mode to MST:

```
Console> (enable) set spantree mode mst
Warning!! Changing the STP mode from a telnet session will disconnect the sessi
n because there are no VLANs mapped to any MISTP instance.
Do you want to continue [n]? y
Console> (enable)
```

Related Commands

set vlan
show spantree

set spantree mst config

Use the **set spantree mst config** command to change the MST region information.

set spantree mst config {[**name** *name*] | [**revision** *number*]}

set spantree mst config commit

set spantree mst config rollback [**force**]

Syntax Description

name *name*	(Optional) Keyword and variable to specify the MST region name. See the "Usage Guidelines" section for more information.
revision *number*	(Optional) Keyword and variable to specify the MST region revision number; *number* is from **0** to **65535**. See the "Usage Guidelines" section for more information.
commit	Keyword to put the new MST VLAN mapping into effect.
rollback	Keyword to discard changes made to the MST configuration that have not been applied yet.
force	(Optional) Keyword to unlock the MST edit buffer when it is held by another user.

Defaults

Unless you specify a region name, no region name will be given.

The default revision number is 1.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The region name can be up to 32 characters long.

The region name and revision number are copied from NVRAM MST region information. You must enter the revision number if the revision number needs to be updated. The revision number is not incremented automatically each time that the MST configuration is committed.

Changes that you make to MST VLAN mapping are buffered, and by entering the **set spantree mst config commit** command, you put the new MST VLAN mapping into effect. After you enter the **set spantree mst config commit** command, the lock for the MST edit buffer is released.

If you enter the **set spantree mst config rollback** command, you discard the changes made to the MST region configuration that are not applied yet (only if you have locked the edit buffer). You can forcefully release the lock set by another user by entering the command **set spantreee mst config rollback force**.

The **set spantree mst config commit** and **set spantree mst config rollback** commands are stored in NVRAM.

Examples

This example shows how to configure an MST region and to give that region a name and revision number:

```
Console> (enable) set spantree mst config name test-lab revision 10
Edit Buffer modified. Use 'set spantree mst config commit' to apply the
changes
Console> (enable)
```

This example shows how to put the new MST VLAN mapping into effect:

```
Console> (enable) set spantree mst config commit
Console> (enable)
```

This example shows how to discard MST region configuration when you hold the MST edit buffer:

```
Console> (enable) set spantree mst config rollback
Console> (enable)
```

This example shows how to unlock the MST edit buffer when it is held by another user:

```
Console> (enable) set spantree mst config rollback force
Console> (enable)
```

Related Commands

clear spantree mst
show spantree mst
show spantree mst config

set spantree mst link-type

Use the **set spantree mst link-type** command to configure the link type of a port.

set spantree mst link-type *mod/port* {**auto** | **point-to-point** | **shared**}

Syntax Description

mod/port	Number of the module and the port on the module.
auto	Keyword to derive the link from either a half-duplex or full-duplex link type. See the "Usage Guidelines" section for more information about **auto**.
point-to-point	Keyword to connect the port to a point-to-point link.
shared	Keyword to connect the port to a shared medium.

Defaults

The default link type is **auto**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

MST rapid connectivity only works on point-to-point links between two bridges.

If the link type is set to **auto** and the link is a half-duplex link, then the link is a shared link. If the link type is set to **auto** and the link is a full-duplex link, then the link is a point-to-point link.

Examples

This example shows how to connect port 1 on module 3 to a point-to-point link:

```
Console> (enable) set spantree mst link-type 3/1 point-to-point
Link type set to point-to-point on port 3/1
Console> (enable)
```

Related Commands

clear spantree mst
set spantree global-default
set spantree mst redetect-protocol
set spantree mst config

set spantree mst maxhops

Use the **set spantree mst maxhops** command to set the spanning tree hop count.

set spantree mst maxhops *maxhops*

Syntax Description	*maxhops*	Maximum number of hops. Valid values are **1** to **40**.

Defaults

The bridge forward delay default is 20 seconds for all instances.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to set the maximum number of hops:

```
Console> (enable) set spantree mst maxhops 20
Console> (enable)
```

Related Commands

clear spantree mst
set spantree mst config
set spantree mst link-type
set spantree mst redetect-protocol
set spantree mst vlan
show spantree mst
show spantree mst config

set spantree mst redetect-protocol

Use the **set spantree mst redetect protocol** command to detect legacy bridges and the boundary ports of the MST region.

set spantree mst *mod/port* **redetect-protocol**

Syntax Description

mod/port	Number of the module and the port or range of ports on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is available in MST mode only and is not saved in NVRAM.

Examples

This example shows how to set protocol detection of legacy bridges and boundary ports on port 2 or module 3:

```
Console> (enable) set spantree mst 3/2 redetect-protocol
Spanning tree protocol detection forced on port 3/2
Console> (enable)
```

Related Commands

clear spantree mst
set spantree mst config
show spantree mst
show spantree mst config

set spantree mst vlan

Use the **set spantree mst vlan** command to configure the mapping of VLANs to an MST instance.

set spantree mst *instance* **vlan** *vlan*

Syntax Description

instance	Number of the instance; valid values are from **0** to **15**.
vlan *vlan*	Keyword and variable to specify the VLAN number; valid values are from **1** to **1005** and from **1025** to **4094**.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

All changes made to the region configuration (region information and VLAN mapping) are buffered. Only one user can hold the buffer at a time. This buffer is locked when you first enter the **set spantree mst** *instance* or **set spantree mst config** commands.

If the VLAN is already mapped to some other instance, the VLAN is unmapped from that instance and mapped to the new instance.

Each time you map a new VLAN or VLANs, they are added to the existing mapping.

All unmapped VLANs are mapped to MST instance 0 (IST).

Examples

This example shows how to map VLANs 400-499 to MST instance 4:

```
Console> (enable) set spantree mst 4 vlan 400-499
Edit Buffer modified. Use 'set spantree mst config commit' to apply the
changes
Console> (enable)
```

Related Commands

clear spantree mst
set spantree mst config
show spantree mst
show spantree mst config

set spantree portcost

Use the **set spantree portcost** command to set the path cost for a port.

set spantree portcost *mod/port cost* [**mst**]

Syntax Description

mod/port	Number of the module and the port on the module.
cost	Number of the path cost; see the "Usage Guidelines" section for additional information.
mst	(Optional) Keyword to set the path cost for an MST port.

Defaults

The default path cost is based on port speed; see Table 2-23 and Table 2-24 for default settings.

Table 2-23 Default Port Cost—Short Mode

Port Speed	Default Port Cost
4 Mb	250
10 Mb	100
16 Mb	62
100 Mb	19
155 Mb	14
1 Gb	4
10 Gb	2

Table 2-24 Default Port Cost—Long Mode

Port Speed	Default Port Cost
100 Kb	200000000 (200 million)
1 Mb	20000000 (20 million)
10 Mb	2000000 (2 million)
10 Mb	200000 (200 thousand)
1 Gb	20000 (20 thousand)
10 Gb	2000 (2 thousand)
100 Gb	200
1 Tb	20
10 Tb	2

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If the spanning tree mode is short and long or MISTP, valid cost values are from **1** to **65535**, otherwise, valid cost values are from **1** to **2000000**.

This command is not supported by the NAM.

The Spanning Tree Protocol uses port path costs to determine which port to select as a forwarding port. You should assign lower numbers to ports attached to faster media (such as full duplex) and higher numbers to ports attached to slower media.

Examples

This example shows how to set the port cost for port 12 on module 2 to 19:

```
Console> (enable) set spantree portcost 2/12 19
Spantree port 2/12 path cost set to 19.
Console> (enable)
```

Related Commands

set spantree defaultcostmode
show spantree

set spantree portfast

Use the **set spantree portfast** command to allow a port that is connected to a single workstation or PC to start faster when it is connected.

set spantree portfast *mod/port* {**enable** [**trunk**] | **disable** | **default**}

Syntax Description

mod/port	Number of the module and the port on the module.
enable	Keyword to enable the spanning tree PortFast-start feature on the port.
trunk	(Optional) Keyword to enable the spanning tree PortFast-start feature on the trunk port.
disable	Keyword to disable the spanning tree PortFast-start feature on the port.
default	Keyword to set the spanning tree start feature back to its default setting.

Defaults

The default is the PortFast-start feature is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

When a port configured with the **spantree portfast enable** command is connected, the port immediately enters the spanning tree forwarding state rather than going through the normal spanning tree states such as listening and learning.

If you enter the **trunk** keyword, the spanning tree port fast-start feature is enabled on the specified trunk port.

Examples

This example shows how to enable the spanning tree PortFast-start feature on port 2 on module 1:

```
Console> (enable) set spantree portfast 1/2 enable

Warning: Connecting layer 2 devices to a fast-start port can cause temporary spanning tree
loops. Use with caution.
Spantree port 1/2 fast start enabled.
Console> (enable)
```

This example shows how to enable the spanning tree PortFast-start feature on the trunk port:

```
Console> (enable) set spantree portfast 3/2 enable trunk
Warning: Connecting layer 2 devices to a fast-start port can cause temporary spanning tree
loops. Use with caution.
Spantree port 1/2 fast start enabled.
Console> (enable)
```

Related Commands show spantree portfast

set spantree portfast bpdu-filter

Use the **set spantree portfast bpdu-filter** command to enable or disable BPDU packet filtering on a port.

set spantree portfast bpdu-filter *mod/port* {**enable** | **disable** | **default**}

Syntax Description

mod/port	Number of the module and the port on the module.
enable	Keyword to enable BPDU packet filtering.
disable	Keyword to disable BPDU packet filtering.
default	Keyword to set BPDU packet filtering to the global BPDU packet filtering state. See the "Usage Guidelines" section for more information.

Defaults

The default is BPDU packet filtering is **default**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

BPDU packet filtering turns off BPDU transmission on PortFast-enabled ports and nontrunking ports.

If you enter the **default** keyword, the spanning tree port is set to the global BPDU filtering state.

To enable or disable BPDU filtering for all ports on the switch, enter the **set spantree global-default bpdu-filter** command.

Examples

This example shows how to enable BPDU filtering on module 3, port 4:

```
Console> (enable) set spantree portfast bpdu-filter 3/4 enable
Warning: Ports enabled with bpdu filter will not send BPDUs and drop all
received BPDUs. You may cause loops in the bridged network if you misuse
this feature.
Spantree port 3/4 bpdu filter enabled.
Console> (enable)
```

Related Commands

set spantree global-default
show spantree portfast

set spantree portfast bpdu-guard

Use the **set spantree portfast bpdu-guard** command to enable or disable spanning tree PortFast BPDU guard on a port.

set spantree portfast bpdu-guard *mod/port* {**enable** | **disable** | **default**}

Syntax Description

mod/port	Number of the module and the port on the module.
enable	Keyword to enable the spanning tree PortFast BPDU guard.
disable	Keyword to disable the spanning tree PortFast BPDU guard.
default	Keyword to set spanning tree PortFast BPDU guard to the global BPDU guard state. See the "Usage Guidelines" section for more information.

Defaults

The default is PortFast BPDU guard is **default**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

You must enable PortFast mode before you can enable PortFast BPDU guard for BPDU guard to work correctly.

When you enable PortFast BPDU guard, a nontrunking PortFast-enabled port is moved into an errdisable state when a BPDU is received on that port. When you disable a PortFast BPDU guard, a PortFast-enabled nontrunking port will stay up when it receives BPDUs, which may cause spanning tree loops.

If you enter the **default** keyword, the spanning tree port is set to the global BPDU guard state.

To enable or disable BPDU guard for all ports on the switch, enter the **set spantree global-default bpdu-guard** command.

Examples

This example shows how to enable BPDU guard on module 3, port 1:

```
Console> (enable) set spantree portfast bpdu-guard 3/1 enable
Spantree port 3/1 bpdu guard enabled.
Console> (enable)
```

Related Commands

set spantree global-default
show spantree portfast

set spantree portinstancecost

Use the **set spantree portinstancecost** command to assign the path cost of the port for the specified instances.

set spantree portinstancecost *mod/port* [**cost** *cost*] [*instances*]

set spantree portinstancecost *mod/port* [**cost** *cost*] **mst** [*instances*]

Syntax Description

mod/port	Number of the module and the port on the module.
cost *cost*	(Optional) Keyword and variable to indicate the path cost; see the "Usage Guidelines" section for additional information.
mst	Keyword to set the cost for an MST instance.
instances	(Optional) Instance number; valid values are from **0** to **15**.

Defaults

The default path cost is based on port speed; see Table 2-25 for default settings.

Table 2-25 Default Port Cost—Short Mode

Port Speed	Default Port Cost
4 Mb	250
10 Mb	100
16 Mb	62
100 Mb	19
155 Mb	14
1 Gb	4
10 Gb	2

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

If the spanning tree mode is short and long or MISTP, valid cost values are from **1** to **65535**, otherwise, valid cost values are from **1** to **2,000,000**.

The port instance cost applies to trunk ports only.

The value specified is used as the path cost of the port for the specified instances. The rest of the instances have a path cost equal to the port path cost set through the **set spantree instancecost** command (if not set, the value is the default path cost of the port).

Examples

These examples show how to use the **set spantree portinstancecost** command and explicitly specify the path cost of a port:

```
Console> (enable) set spantree portinstancecost 2/10 cost 6 1-10
Port 2/10 instances 11-16 have path cost 2000000.
Port 2/10 instances 1-10 have path cost 6.
This parameter applies to trunking ports only.
Console> (enable)
```

These examples show how to use the **set spantree portinstancecost** command without explicitly specifying the path cost of a port:

```
Console> (enable) set spantree portinstancecost 1/2
Port 1/2 Instances 1-1005 have path cost 3100.
Console> (enable)

Console> (enable) set spantree portinstancecost 1/2 16
Port 1/2 Instances 16,22-1005 have path cost 3100.
Console> (enable)
```

This example shows the display if you enter the command when PVST+ is enabled:

```
Console> (enable) set spantree portinstancecost 3/1
This command is only valid when STP is in MISTP or MISTP-PVST+ mode.
Console> (enable)
```

This example shows how to set the port cost for a specific MST instance:

```
Console> (enable) set spantree portinstancecost 2/10 cost 6 1-10 mst
Port 2/10 mst instances 1-10 have path cost 6.
This parameter applies to trunking ports only.
Console> (enable)
```

Related Commands

clear spantree portinstancecost
show spantree mistp-instance

set spantree portinstancepri

Use the **set spantree portinstancepri** command to set the port priority for instances in the trunk port.

set spantree portinstancepri *mod/port priority* [*instances*]

set spantree portinstancepri *mod/port priority* **mst** [*instances*]

Syntax Description

mod/port	Number of the module and the port on the module.
priority	Number that represents the cost of a link in a spanning tree bridge. The priority level is from **0** to **63**, with 0 indicating high priority and 63 indicating low priority.
mst	Keyword to specify the port priority for MST instances.
instances	(Optional) Instance number; valid values are from **0** to **15**.

Defaults

The default is the port priority is set to 0, with no instances specified.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

Use this command to add instances to a specified port priority level. Subsequent calls to this command do not replace instances that are already set at a specified port priority level.

This feature is not supported for the MSM.

The **set spantree portinstancepri** command applies to trunk ports only. If you enter this command, you see this message:

```
Port xx is not a trunk-capable port
```

Examples

This example shows how to set the port priority for module 1, port 2, on specific instances:

```
Console> (enable) set spantree portinstancepri 1/2 16 1-11
Port 1/2 instances 1-11 using portpri 16.
This parameter applies to trunking ports only.
Console> (enable)
```

This example shows how to set the port priority for module 8, port 1, on MST instance 2:

```
Console> (enable) set spantree portinstancepri 8/1 31 mst 2
Port 8/1 instances 2 using portpri 31.
Port 8/1 instances 0-1, 3-15 using portpri 32.
Console> (enable)
```

Related Commands clear spantree portinstancecost
show spantree mistp-instance

set spantree portpri

Use the **set spantree portpri** command to set the bridge priority for a spanning tree port.

set spantree portpri *mod/port priority* [**mst**]

Syntax Description

mod/port	Number of the module and the port on the module.
priority	Number that represents the cost of a link in a spanning tree bridge; valid values are from **0** to **63**, with 0 indicating high priority and 63, low priority.
mst	(Optional) Keyword to set the bridge priority for an MST port.

Defaults

The default is all ports with bridge priority are set to 32.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

Examples

This example shows how to set the priority of port 1 on module 4 to 63:

```
Console> (enable) set spantree portpri 4/1 63
Bridge port 4/1 priority set to 63.
Console> (enable)
```

Related Commands

show spantree

set spantree portvlancost

Use the **set spantree portvlancost** command to assign a lower path cost to a set of VLANs on a port.

set spantree portvlancost *mod/port* [**cost** *cost*] [*vlan_list*]

Syntax Description

mod/port	Number of the module and the port on the module.
cost *cost*	(Optional) Keyword and variable to set the path cost; valid values are from **1** to **65535**.
vlan_list	(Optional) Number of the VLAN; valid values are from **1** to **1005** and from **1025** to **4094**.

Defaults

The default path cost is based on port speed; see Table 2-26 and Table 2-27 for default settings.

Table 2-26 Default Port Cost—Short Mode

Port Speed	Default Port Cost
4 Mb	250
10 Mb	100
16 Mb	62
100 Mb	19
155 Mb	14
1 Gb	4
10 Gb	2

Table 2-27 Default Port Cost—Long Mode

Port Speed	Default Port Cost
100 Kb	200,000,000
1 Mb	20,000,000
10 Mb	2,000,000
10 Mb	200,000
1 Gb	20,000
10 Gb	2,000
100 Gb	200
1 Tb	20
10 Tb	2

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

This command is not supported in MISTP mode.

When setting the path cost for extended-range VLANs, you can create a maximum of 64 nondefault entries or create entries until NVRAM is full.

The value specified is used as the path cost of the port for the specified set of VLANs. The rest of the VLANs have a path cost equal to the port path cost set through the **set spantree portcost** command (if not set, the value is the default path cost of the port).

If you do not list a VLAN explicitly, the VLANs listed in prior invocations of this command are affected. If no cost is listed explicitly and previous cost values are specified in prior invocations, then the portvlancost is set to 1 less than the current port cost for a port. However, this may not assure load balancing in all cases.

Examples

These examples show how to use the **set spantree portvlancost** command and explicitly specify the path cost of a port:

```
Console> (enable) set spantree portvlancost 2/10 cost 25 1-20
Cannot set portvlancost to a higher value than the port cost, 10, for port 2/10.
Console> (enable)

Console> (enable) set spantree portvlancost 2/10 cost 1-20
Port 2/10 VLANs 1-20 have a path cost of 9.
Console> (enable)

Console> (enable) set spantree portvlancost 2/10 cost 4 1-20
Port 2/10 VLANs 1-20 have path cost 4.
Port 2/10 VLANs 21-1000 have path cost 10.
Console> (enable)

Console> (enable) set spantree portvlancost 2/10 cost 6 21
Port 2/10 VLANs 1-21 have path cost 6.
Port 2/10 VLANs 22-1000 have path cost 10.
Console> (enable)
```

These examples show how to use the **set spantree portvlancost** command without explicitly specifying the path cost of a port:

```
Console> (enable) set spantree portvlancost 1/2
Port 1/2 VLANs 1-1005 have path cost 3100.
Console> (enable)

Console> (enable) set spantree portvlancost 1/2 21
Port 1/2 VLANs 1-20,22-1005 have path cost 3100.
Port 1/2 VLANs 21 have path cost 3099.
Console> (enable)
```

Related Commands

clear spantree portvlancost
set channel vlancost
show spantree

set spantree portvlanpri

Use the **set spantree portvlanpri** command to set the port priority for a subset of VLANs in the trunk port.

set spantree portvlanpri *mod/port priority* [*vlans*]

Syntax Description

mod/port	Number of the module and the port on the module.
priority	Number that represents the cost of a link in a spanning tree bridge. The priority level is from **0** to **63**, with 0 indicating high priority and 63 indicating low priority.
vlans	(Optional) VLANs that use the specified priority level; valid values are from **1** to **1005**.

Defaults

The default is the port VLAN priority is set to 0, with no VLANs specified.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

This command is not supported by extended-range VLANs.

Use this command to add VLANs to a specified port priority level. Subsequent calls to this command do not replace VLANs that are already set at a specified port priority level.

This feature is not supported for the MSM.

The **set spantree portvlanpri** command applies only to trunk ports. If you enter this command, you see this message:

```
Port xx is not a trunk-capable port
```

Examples

This example shows how to set the port priority for module 1, port 2, on VLANs 21 to 40:

```
Console> (enable) set spantree portvlanpri 1/2 16 21-40
Port 1/2 vlans 3,6-20,41-1000 using portpri 32
Port 1/2 vlans 1-2,4-5,21-40 using portpri 16
Console> (enable)
```

Related Commands

clear spantree portvlanpri
show spantree

set spantree priority

Use the **set spantree priority** command to set the bridge priority for a VLAN or an instance when PVST+ or MISTP is running.

set spantree priority *bridge_priority vlans*

set spantree priority *bridge_priority* **mistp-instance** *instances*

set spantree priority *bridge_priority* **mst** *instances*

Syntax Description

bridge_priority	Number representing the priority of the bridge; see the "Usage Guidelines" section for valid values.
vlans	Number of the VLAN; valid values are from **1** to **1005** and from **1025** to **4094**.
mistp-instance *instances*	Keyword and variable to specify the instance numbers; valid values are from **1** to **16**.
mst *instances*	Keyword and variable to specify the MST instance numbers; valid values are from **1** to **15**.

Defaults

The default is the bridge priority is set to 32768.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM or the MSM.

If MISTP or the MAC reduction feature is enabled, valid *bridge_priority* values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440, with 0 indicating high priority and 61440, low priority.

If MISTP or the MAC reduction feature is disabled, valid *bridge_priority* values are from 0 to 65535.

If you enable MISTP, you cannot set the VLAN bridge priority.

If you enable PVST+, you cannot set the instance priority.

If you try to set instance priority with PVST+ enabled, this message displays:

```
This command is only valid when STP is in MISTP or MISTP-PVST+ mode.
```

Examples

This example shows how to set the bridge priority of instance 3:

```
Console> (enable) set spantree priority 14 mistp-instance 3
Instance 3 bridge priority set to 14.
Instance 3 does not exist.
Your configuration has been saved to NVRAM only.
Console> (enable)
```

This example shows how to set the bridge priority for MST instance 0:

```
Console> (enable) set spantree priority 28672 mst 0
MST Spantree 0 bridge priority set to 28672.
Console> (enable)
```

This example shows how to set the bridge priority for multiple MST instances:

```
Console> (enable) set spantree priority 28672 mst 0-4
MST Spantrees 0-4 bridge priority set to 28672.
Console> (enable)
```

Related Commands **show spantree**

set spantree root

Use the **set spantree root** command to set the primary or secondary root for specific VLANs, all VLANs of the switch, or an instance.

set spantree root [**secondary**] [*vlans*] [**dia** *network_diameter*] [**hello** *hello_time*]

set spantree root [**secondary**] **mistp-instance** *instance* [**dia** *network_diameter*] [**hello** *hello_time*]

set spantree root [**secondary**] **mst** *instance* [**dia** *network_diameter*] [**hello** *hello_time*]

Syntax Description

secondary	(Optional) Keyword to designate this switch as a secondary root, should the primary root fail.
vlans	(Optional) Number of the VLAN; valid values are from **1** to **1005** and from **1025** to **4094**.
dia *network_diameter*	(Optional) Keyword to specify the maximum number of bridges between any two points of end stations; valid values are from **1** through **7**.
hello *hello_time*	(Optional) Keyword to specify in seconds, the duration between the generation of configuration messages by the root switch.
mistp-instance *instance*	Keyword and variable to specify the instance number; valid values are from **1** to **16**.
mst *instance*	Keyword and variable to specify an MST instance; valide values are from **1** to **16**.

Defaults

If you do not specify the **secondary** keyword, the default is to make the switch the primary root.

The default value of the network diameter is 7.

If you do not specify the *hello_time* value, the current value of *hello_time* is calculated from the network diameter.

Usage Guidelines

If you do not specify a VLAN number, VLAN 1 is assumed.

This command is not supported by the NAM.

This command is run on backbone or distribution switches.

You can run the secondary root many times to create backup switches in case of a root failure.

The **set spantree root secondary** bridge priority value is 16384, except when MAC reduction or MISTP are enabled, then the value is 28672.

The **set spantree root** bridge priority value is 16384, except when MAC reduction or MISTP are enabled, then the value is 24576.

This command increases path costs to a value greater than 3000.

If you enable MISTP, you cannot set the VLAN root. If you enable PVST+, you cannot set the instance root.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to set the primary root for a range of VLANs:

```
Console> (enable) set spantree root 1-10 dia 4
VLANs 1-10 bridge priority set to 8192
VLANs 1-10 bridge max aging time set to 14 seconds.
VLANs 1-10 bridge hello time set to 2 seconds.
VLANs 1-10 bridge forward delay set to 9 seconds.
Switch is now the root switch for active VLANs 1-6.
Console> (enable)
```

This example shows how to set the primary root for an instance:

```
Console> (enable) set spantree root mistp-instance 2-4 dia 4
Instances 2-4 bridge priority set to 8192
VLInstances 2-4 bridge max aging time set to 14 seconds.
Instances 2-4 bridge hello time set to 2 seconds.
Instances 2-4 bridge forward delay set to 9 seconds.
Switch is now the root switch for active Instances 1-6.
Console> (enable)
```

This example shows how to set the primary root for MST instance 5:

```
Console> (enable) set spantree root mst 5
Instance 5 bridge priority set to 24576.
Instance 5 bridge max aging time set to 16.
Instance 5 bridge hello time set to 2.
Instance 5 bridge forward delay set to 15.
Switch is now the root switch for active Instance 5.
Console> (enable)
```

This example shows how to set the secondary root for MST instance 0:

```
Console> (enable) set spantree root secondary mst 0
Instance 0 bridge priority set to 28672.
Instance 0 bridge max aging time set to 20.
Instance 0 bridge hello time set to 2.
Instance 0 bridge forward delay set to 15.
Console> (enable)
```

This example shows how to set the maximum number of bridges and the hello time of the root for MST instance 0:

```
Console> (enable) set spantree root mst 0 dia 7 hello 2
Instance 0 bridge priority set to 24576.
Instance 0 bridge max aging time set to 20.
Instance 0 bridge hello time set to 2.
Instance 0 bridge forward delay set to 15.
Switch is now the root switch for active Instance 0.
Console> (enable)
```

These examples show that setting the bridge priority to 8192 was not sufficient to make this switch the root. The priority was further reduced to 7192 (100 less than the current root switch) to make this switch the root switch. However, reducing it to this value did not make it the root switch for active VLANs 16 and 17.

```
Console> (enable) set spantree root 11-20.
VLANs 11-20 bridge priority set to 7192
VLANs 11-10 bridge max aging time set to 20 seconds.
VLANs 1-10 bridge hello time set to 2 seconds.
VLANs 1-10 bridge forward delay set to 13 seconds.
Switch is now the root switch for active VLANs 11-15,18-20.
Switch could not become root switch for active VLAN 16-17.
Console> (enable)

Console> (enable) set spantree root secondary 22,24 dia 5 hello 1
VLANs 22,24 bridge priority set to 16384.
VLANs 22,24 bridge max aging time set to 10 seconds.
VLANs 22,24 bridge hello time set to 1 second.
VLANs 22,24 bridge forward delay set to 7 seconds.
Console> (enable)
```

Related Commands show spantree

set spantree uplinkfast

Use the **set spantree uplinkfast** command to enable fast switchover to alternate ports when the root port fails. This command applies to a switch, not to a WAN.

set spantree uplinkfast {**enable** | **disable**} [**rate** *station_update_rate*] [**all-protocols** {**off** | **on**}]

Syntax Description

enable	Keyword to enable fast switchover.
disable	Keyword to disable fast switchover.
rate *station_update_rate*	(Optional) Keyword and variable to specify the number of multicast packets transmitted per 100 ms when an alternate port is chosen after the root port goes down.
all-protocols	(Optional) Keyword to specify whether or not to generate multicast packets for all protocols (IP, IPX, AppleTalk, and Layer 2 packets).
off	(Optional) Keyword to turn off the all-protocols feature.
on	(Optional) Keyword to turn on the all-protocols feature.

Defaults

The default *station_update_rate* is 15 packets per 100 ms.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

This command is not available in MST mode.

The **set spantree uplinkfast enable** command has the following results:

- Changes the bridge priority to 49152 for all VLANs (allowed VLANs).
- Increases the path cost and portvlancost of all ports to a value greater than 3000.
- On detecting the failure of a root port, an instant cutover occurs to an alternate port selected by Spanning Tree Protocol.

If you run the **set spantree uplinkfast enable** command on a switch that has this feature already enabled, only the station update rate is updated. The rest of the parameters are not modified.

If you run the **set spantree uplinkfast disable** command on a switch, the UplinkFast feature is disabled but the switch priority and port cost values are not reset to the default settings. To reset the values to the default settings, enter the **clear spantree uplinkfast** command.

The default *station_update_rate* value is 15 packets per 100 ms, which is equivalent to a 1-percent load on a 10-Mbps Ethernet. If you specify this value as 0, the generation of these packets is turned off.

You do not have to turn on the all-protocols feature on Catalyst 6000 family switches that have both the UplinkFast and protocol filtering features enabled. Use the all-protocols feature only on Catalyst 6000 family switches that have UplinkFast enabled but do not have protocol filtering; upstream switches in the network use protocol filtering. You must enter the **all-protocols** option to inform the UplinkFast task whether or not to generate multicast packets for all protocols.

Examples

This example shows how to enable spantree UplinkFast and specify the number of multicast packets transmitted to 40 packets per 100 ms:

```
Console> (enable) set spantree uplinkfast enable rate 40
VLANs 1-4094 bridge priority set to 49152.
The port cost and portvlancost of all ports set to above 3000.
Station update rate set to 40 packets/100ms.
uplinkfast all-protocols field set to off.
uplinkfast enabled for bridge.
Console> (enable)
```

This example shows how to disable spantree UplinkFast:

```
Console> (enable) set spantree uplinkfast disable
Uplinkfast disabled for switch.
Use clear spantree uplinkfast to return stp parameters to default.
Console> (enable) clear spantree uplink
This command will cause all portcosts, portvlancosts, and the
bridge priority on all vlans to be set to default.
Do you want to continue (y/n) [n]? y
VLANs 1-1005 bridge priority set to 32768.
The port cost of all bridge ports set to default value.
The portvlancost of all bridge ports set to default value.
uplinkfast disabled for bridge.
Console> (enable)
```

This example shows how to turn on the all-protocols feature:

```
Console> (enable) set spantree uplinkfast enable all-protocols on
uplinkfast update packets enabled for all protocols.
uplinkfast enabled for bridge.
Console> (enable)
```

This example shows how to turn off the all-protocols feature:

```
Console> (enable) set spantree uplinkfast enable all-protocols off
uplinkfast all-protocols field set to off.
uplinkfast already enabled for bridge.
Console> (enable)
```

This example shows the output when instances have been configured:

```
Console> (enable) set spantree uplinkfast enable
Instances 1-15 bridge priority set to 49152.
The port cost and portinstancecost of all ports set to above 3000.
Station update rate set to 15 mpackets/100ms.
uplinkfast all-protocols field set to off.
uplinkfast already enabled for bridge.
Console> (enable)
```

Related Commands

clear spantree uplinkfast
show spantree uplinkfast

set summertime

Use the **set summertime** command to specify whether the system should set the clock ahead one hour during daylight saving time.

set summertime {**enable** | **disable**} [*zone*]

set summertime recurring [{*week*} {*day*} {*month*} {*hh*:*mm*} {*week* | *day* | *month* | *hh*:*mm*} [*offset*]]

set summertime date {*month*} {*date*} {*year*} {*hh*:*mm*} {*month* | *date* | *year* | *hh*:*mm*} [*offset*]

Syntax Description

enable	Keyword to cause the system to set the clock ahead one hour during daylight saving time.
disable	Keyword to prevent the system from setting the clock ahead one hour during daylight saving time.
zone	(Optional) Time zone used by the **set summertime** command.
recurring	Keyword to specify the summertime dates that recur every year.
week	Week of the month (**first**, **second**, **third**, **fourth**, **last**, **1**...**5**).
day	Day of the week (**Sunday**, **Monday**, **Tuesday**, and so forth).
month	Month of the year (**January**, **February**, **March**, and so forth).
hh:mm	Hours and minutes.
offset	(Optional) Amount of offset in minutes (**1** to **1440** minutes).
date	Day of the month (**1** to **31**).
year	Number of the year (**1993** to **2035**).

Defaults

By default, the **set summertime** command is disabled. Once enabled, the default for *offset* is 60 minutes, following U.S. standards.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

After you enter the **clear config** command, the dates and times are set to default.

Unless you configure it otherwise, this command advances the clock one hour at 2:00 a.m. on the first Sunday in April and moves back the clock one hour at 2:00 a.m. on the last Sunday in October.

Examples

This example shows how to cause the system to set the clock ahead one hour during daylight saving time:

```
Console> (enable) set summertime enable PDT
Summertime is enabled and set to “PDT”.
Console> (enable)
```

This example shows how to prevent the system from setting the clock ahead one hour during daylight saving time:

```
Console> (enable) set summertime disable
Summertime disabled.
Console> (enable)
```

This example shows how to set daylight saving time to the zonename AUS and repeat every year, starting from the third Monday of February at noon and ending at the second Saturday of August at 3:00 p.m. with an offset of 30 minutes:

```
Console> (enable) set summertime AUS recurring 3 Mon Feb 12:00 2 Saturday Aug 15:00 30
Summer time is disabled and set to 'AUS' with offset 30 minutes.
   start: 12:00:00 Sun Feb 13 2000
   end:   14:00:00 Sat Aug 26 2000
   Recurring, starting at 12:00:00 on Sunday of the third week of February and ending
   on Saturday of the fourth week of August.
Console> (enable)
```

This example shows how to set the daylight saving time to start on January 29, 1999 at 2:00 a.m. and end on August 19, 2004 at 3:00 p.m. with an offset of 30 minutes:

```
Console> (enable) set summertime date jan 29 1999 02:00 aug 19 2004 15:00 30
Summertime is disabled and set to ''
Start : Fri Jan 29 1999, 02:00:00
End   : Thu Aug 19 2004, 15:00:00
Offset: 30 minutes
Recurring: no
Console> (enable)
```

This example shows how to set recurring to reset default to US summertime:

```
Console> (enable) set summertime recurring 3 mon feb 4 thurs oct 8:00 500
Command authorization none.
Summertime is enabled and set to ‘’
Start : Mon Feb 21 2000, 03:00:00
End   : Fri Oct 20 2000, 08:00:00
Offset: 500 minutes (8 hours 20 minutes)
Recurring: yes, starting at 03:00am of third Monday of February and ending on 08:00am of
fourth Thursday of October.
Console> (enable)
```

Related Commands

show summertime

set system baud

Use the **set system baud** command to set the console port baud rate.

set system baud *rate*

Syntax Description

rate	Baud rate; valid rates are **600**, **1200**, **2400**, **4800**, **9600**, **19200**, and **38400**.

Defaults

The default is 9600 baud.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to set the system baud rate to 19200:

```
Console> (enable) set system baud 19200
System console port baud rate set to 19200.
Console> (enable)
```

Related Commands

show system

set system contact

Use the **set system contact** command to identify a contact person for the system.

set system contact [*contact_string*]

Syntax Description

contact_string	(Optional) Text string that contains the name of the person to contact for system administration. If you do not specify a contact string, the system contact string is cleared.

Defaults

The default is no system contact is configured.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to set the system contact string:

```
Console> (enable) set system contact Xena ext.24
System contact set.
Console> (enable)
```

Related Commands

show system

set system core-dump

Use the **set system core-dump** command to enable or disable the core dump feature.

set system core-dump {**enable** | **disable**}

Syntax Description

enable	Keyword to enable the core dump feature.
disable	Keyword to disable the core dump feature.

Defaults

The default is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The core dump feature generates a report of images when your system fails due to a software error. The core image is stored in the file system. From this file, you can examine an error condition of a process when it is terminated due to an exception.

The size of the file system depends on the memory card size. The core dump file generated is proportional to the size of the system DRAM. Make sure that you have enough memory available to store the core dump file.

In order to maintain the core dump image, the yield CPU is disabled during the core dump process. You should have a redundant supervisor engine installed to take over normal operations. If the switch has a redundant supervisor engine setup, the redundant supervisor engine takes over automatically before the core dump occurs. The previously active supervisor engine resets itself after the core dump completes.

Examples

This example shows how to enable the core dump feature:

```
Console> (enable) set system core-dump enable
(1) In the event of a system crash, this feature will
     cause a core file to be written out.
(2) Core file generation may take up to 20 minutes.
(3) Selected core file is slot0:crash.hz
(4) Please make sure the above device has been installed,
    and ready to use
Core-dump enabled
Console> (enable)
```

This example shows how to disable the core dump feature:

```
Console> (enable) set system core-dump disable
Core-dump disabled
Console> (enable)
```

Related Commands set system core-dump

set system core-file

Use the **set system core-file** command to specify the core image filename.

set system core-file {*device*:[*filename*]}

Syntax Description

device	Device where the core image file resides; valid values are **bootflash** and **slot0**.
filename	(Optional) Name of the core image file.

Defaults

The default *filename* is "crashinfo."

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

A device name check is performed when you enter the **set system core-file** command. If a valid device name is not found, an error message displays.

When a core dump occurs, the actual file written out will append the date to the filename in this format: _{yymmdd}-{hhmmss}.

Examples

This example shows how to use the default core image filename:

```
Console> (enable) set system core-file bootflash:
Attach default filename crashinfo to the device
System core-file set.
Console> (enable)
```

This example shows how to set the core image filename:

```
Console> (enable) set system core-file slot0:abc
System core-file set.
Console> (enable)
```

Related Commands

set system core-dump

set system countrycode

Use the **set system countrycode** command to specify the country where the system is physically located.

set system countrycode *code*

Syntax Description

code	Country code; see the "Usage Guidelines" section for format information.

Defaults

The default is US (United States).

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The country code is a 2-letter country code taken from ISO-3166 (for example, VA=Holy See [Vatican City State], VU=Vanuatu, and TF=French Southern Territories).

Examples

This example shows how to set the system country code:

```
Console> (enable) set system countrycode US
Country code is set to US.
Console> (enable)
```

set system crossbar-fallback

Use the **set system crossbar-fallback** command to select the action taken when the Switch Fabric Module fails.

set system crossbar-fallback {**bus-mode** | **none**}

Syntax Description

bus-mode	Keyword to fail to the system bus.
none	Keyword to not fail over to the system bus.

Defaults

The default is **bus-mode**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can either have the Switch Fabric Module fail over to the bus, or have the switch not fail over at all (in which case, the switch should be down).

This command is supported on systems configured with a Switch Fabric Module and the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) only.

Examples

This example shows how to set the Switch Fabric Module to fail over to the system bus:

```
Console> (enable) set system crossbar-fallback bus-mode
System crossbar-fallback set to bus-mode.
Console> (enable)
```

This example shows how to set the Switch Fabric Module to not fail over:

```
Console> (enable) set system crossbar-fallback none
System crossbar-fallback set to none.
Console> (enable)
```

Related Commands

show fabric channel

set system highavailability

Use the **set system highavailability** command to enable or disable high system availability for the switch.

set system highavailability {**enable** | **disable**}

Syntax Description

enable	Keyword to activate system high availability.
disable	Keyword to deactivate system high availability.

Defaults

The default is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

High availability provides Layer 2 and Layer 3 protocol redundancy.

If you enable high availability while the redundant supervisor engine is running, the switch checks the version compatibility between the two supervisor engines. If the versions are compatible, database synchronization occurs. When you disable high availability, database synchronization does not occur and protocols restart on the redundant supervisor engine after switchover.

If you disable high availability from the enabled state, synchronization from the active supervisor engine is stopped. On the redundant supervisor engine, current synchronization data is discarded. If you enable high availability from the disabled state, synchronization from the active supervisor engine to the redundant supervisor engine starts (if you have a redundant supervisor engine and its image version is compatible with the active supervisor engine).

Examples

This example shows how to enable high availability:

```
Console> (enable) set system highavailability enable
System high availability enabled.
Console> (enable)
```

This example shows how to disable high availability:

```
Console> (enable) set system highavailability disable
System high availability disabled.
Console> (enable)
```

Related Commands

set system highavailability versioning
show system highavailability

set system highavailability versioning

Use the **set system highavailability versioning** command to enable and disable support for supervisor engine image versioning.

set system highavailability versioning {**enable** | **disable**}

Syntax Description

enable	Keyword to activate system high-availability versioning.
disable	Keyword to deactivate system high-availability versioning.

Defaults

The default is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The high-availability versioning feature allows the Catalyst 6000 family switch to run different images on the active and redundant supervisor engines. When you enable image versioning, Flash image synchronization (from active to the redundant supervisor engines) does not occur, allowing active and redundant supervisor engines to run different images.

Caution When you disable image versioning, the active and redundant supervisor engines must run the same image version.

If you disable the image versioning option from the enabled state, no additional action is necessary on the redundant supervisor engine (the redundant supervisor engine should be running the same image as the active supervisor engine). If you want to load a different image, you have to restart the redundant supervisor engine.

If you enable the image versioning option from the disabled state and you have a redundant supervisor engine and active supervisor engine running a different image than that of the active supervisor engine, Flash synchronization will copy the active supervisor engine image to the redundant supervisor engine image and then restart it.

If you enable the image versioning option on the active supervisor engine and the redundant supervisor engine is running a different image, the NVRAM synchronization cannot occur because the NVRAM versions are not compatible. If this is the case, after switchover, the old NVRAM configuration on the supervisor engine is used.

Examples

This example shows how to enable high-availability versioning:

```
Console> (enable) set system highavailability versioning enable
Image versioning enabled.
Console> (enable)
```

This example shows how to disable high-availability versioning:

```
Console> (enable) set system highavailability versioning disable
Image versioning disabled.
Console> (enable)
```

Related Commands

set system highavailability
show system highavailability

set system location

Use the **set system location** command to identify the location of the system.

set system location [*location_string*]

Syntax Description

location_string	(Optional) Text string that indicates where the system is located.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not specify a location string, the system location is cleared.

Examples

This example shows how to set the system location string:

```
Console> (enable) set system location Closet 230 4/F
System location set.
Console> (enable)
```

Related Commands

show system

set system modem

Use the **set system modem** command to enable or disable modem control lines on the console port.

set system modem {**enable** | **disable**}

Syntax Description

enable	Keyword to activate modem control lines on the console port.
disable	Keyword to deactivate modem control lines on the console port.

Defaults

The default is modem control lines are disabled.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to disable modem control lines on the console port:

```
Console> (enable) set system modem disable
Modem control lines disabled on console port.
Console> (enable)
```

Related Commands

show system

set system name

Use the **set system name** command to configure a name for the system.

set system name [*name_string*]

Syntax Description

name_string	(Optional) Text string that identifies the system.

Defaults

The default is no system name is configured.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use the **set system name** command to assign a name to the switch, the switch name is used as the prompt string. However, if you specify a different prompt string using the **set prompt** command, that string is used for the prompt.

If you do not specify a system name, the system name is cleared and a DNS lookup is initiated for a system name. If a name is found, that is the name used; if no name is found, no name is designated.

The system name can be 255 characters long, and the prompt can be 20 characters long. The system name is truncated appropriately when used as a prompt; a greater-than symbol (>) is appended to the truncated system name. If the system name was found from a DNS lookup, it is truncated to remove the domain name.

If the prompt is obtained using the system name, it is updated whenever the system name changes. You can overwrite this prompt any time by setting the prompt manually. Any change in the prompt is reflected in all current open sessions.

If you do not specify a name, the system name is cleared.

Examples

This example shows how to set the system name to Information Systems:

```
Console> (enable) set system name Information Systems
System name set.
Console> (enable)
```

Related Commands

set prompt
show system

set system switchmode

Use the **set system switchmode** command to configure the switching mode for the system.

set system switchmode allow {**truncated** | **bus-only**}

Syntax Description

truncated	Keyword to specify truncated mode; see the "Usage Guidelines" section for additional information.
bus-only	Keyword to force the system to be in flow-through mode.

Defaults

The default is truncated.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you install a Switch Fabric Module in a Catalyst 6500 series switch, the traffic is forwarded to and from modules in one of the following modes:

- Flow-through mode—In this mode, data passes between the local bus and the supervisor engine bus. This mode is used for traffic to or from nonfabric-enabled modules.
- Truncated mode—In this mode, only the truncated data (the first 64 bytes of the frame) is sent over the switch fabric channel if both the destination and the source modules are fabric-enabled modules. If either the source or destination is not a fabric-enabled module, the data goes through the switch fabric channel and the data bus. The Switch Fabric Module does not get involved when traffic is forwarded between nonfabric-enabled modules.
- Compact mode—In this mode, a compact version of the DBus header is forwarded over the switch fabric channel, delivering the best possible switching rate. Nonfabric-enabled modules do not support the compact mode and will generate CRC errors if they receive frames in compact mode. This mode is only used if nonfabric-enabled modules are not installed in the chassis.

If you enter the **truncated** keyword and your system does not contain nonfabric-enabled modules, the system is placed in compact mode.

If you enter the **truncated** keyword and your system is configured with one or more nonfabric-enabled modules, the switch is allowed to go in truncated mode, *but only* if the number of fabric-enabled modules present in the system are equal or greater than the threshold. If the number of fabric-enabled modules present are less than the threshold, the system goes into flow-through mode.

Examples

This example shows how to set the switching mode to truncated:

```
Console> (enable) set system switchmode allow truncated
System switchmode allow set to truncated.
Console> (enable)
```

This example shows how to set the switching mode to bus-only:

```
Console> (enable) set system switchmode allow bus-only
System switchmode allow set to bus-only.
Console> (enable)
```

Related Commands

show system switchmode

set tacacs attempts

Use the **set tacacs attempts** command to configure the maximum number of login attempts allowed to the TACACS+ server.

set tacacs attempts *count*

Syntax Description

count	Number of login attempts allowed; valid values are from **1** to **10**.

Defaults

The default is three attempts.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to configure the TACACS+ server to allow a maximum of six login attempts:

```
Console> (enable) set tacacs attempts 6
Tacacs number of attempts set to 6.
Console> (enable)
```

Related Commands

show tacacs

set tacacs directedrequest

Use the **set tacacs directedrequest** command to enable or disable the TACACS+ directed-request option. When enabled, you can direct a request to any of the configured TACACS+ servers and only the username is sent to the specified server.

set tacacs directedrequest {**enable** | **disable**}

Syntax Description

enable	Keyword to send the portion of the address before the @ sign (the username) to the host specified after the @ sign.
disable	Keyword to send the entire address string to the default TACACS+ server.

Defaults

The default is the TACACS+ directed-request option is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you enable TACACS+ directed-request, you must specify a configured TACACS+ server after the @ sign. If the specified host name does not match the IP address of a configured TACACS+ server, the request is rejected. When TACACS+ directed-request is disabled, the Catalyst 6000 family switch queries the list of servers beginning with the first server in the list and then sends the entire string, accepting the first response from the server. This command is useful for sites that have developed their own TACACS+ server software to parse the entire address string and make decisions based on the contents of the string.

Examples

This example shows how to enable the **tacacs directedrequest** option:

```
Console> (enable) set tacacs directedrequest enable
Tacacs direct request has been enabled.
Console> (enable)
```

Related Commands

show tacacs

set tacacs key

Use the **set tacacs key** command to set the key for TACACS+ authentication and encryption.

set tacacs key *key*

Syntax Description

key	Printable ASCII characters used for authentication and encryption.

Defaults

The default value of *key* is null.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The key must be the same key used on the TACACS+ server. All leading spaces are ignored. Spaces within the key and at the end of the key are included. Double quotation marks are not required, even if there are spaces between words in the key, unless the quotation marks themselves are part of the key. The key can consist of any printable ASCII characters except the tab character.

The key length must be less than 100 characters long.

Examples

This example shows how to set the authentication and encryption key:

```
Console> (enable) set tacacs key Who Goes There
The tacacs key has been set to Who Goes There.
Console> (enable)
```

Related Commands

clear spantree uplinkfast
show tacacs

set tacacs server

Use the **set tacacs server** command to define a TACACS+ server.

set tacacs server *ip_addr* [**primary**]

Syntax Description

ip_addr	IP address of the server on which the TACACS+ server resides.
primary	(Optional) Keyword to designate the specified server as the primary TACACS+ server.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can configure a maximum of three servers. The primary server, if configured, is contacted first. If no primary server is configured, the first server configured becomes the primary server.

Examples

This example shows how to configure the server on which the TACACS+ server resides and to designate it as the primary server:

```
Console> (enable) set tacacs server 170.1.2.20 primary
170.1.2.20 added to TACACS server table as primary server.
Console> (enable)
```

Related Commands

clear tacacs server
show tacacs

set tacacs timeout

Use the **set tacacs timeout** command to set the response timeout interval for the TACACS+ server daemon. The TACACS+ server must respond to a TACACS+ authentication request before this interval expires or the next configured server is queried.

set tacacs timeout *seconds*

Syntax Description

seconds	Timeout response interval in seconds; valid values are from **1** to **255**.

Defaults

The default is 5 seconds.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to set the response timeout interval for the TACACS+ server to 8 seconds:

```
Console> (enable) set tacacs timeout 8
Tacacs timeout set to 8 seconds.
Console> (enable)
```

Related Commands

show tacacs

set test diaglevel

Use the **set test diaglevel** command to set the diagnostic level.

set test diaglevel {**complete** | **minimal** | **bypass**}

Syntax Description

complete	Keyword to specify complete diagnostics.
minimal	Keyword to specify minimal diagnostics.
bypass	Keyword to specify bypass diagnostics.

Defaults

The default is minimal diagnostics. See the "Usage Guidelines" section for more information about the three diagnostic levels.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Setting the diagnostic level determines the level of testing that occurs when the system or module is reset. The three levels are as follows:

- **complete**—This level runs all tests.
- **minimal**—This level runs only EARL tests for the supervisor engine and loopback tests for all ports in the system.
- **bypass**—This level skips all tests.

Note Although the default is **minimal**, we recommend that you set the diagnostic level at **complete**.

Examples

This example shows how to set the diagnostic level to complete:

```
Console> (enable) set test diaglevel complete
Diagnostic level set to complete.
Console> (enable)
```

This example shows how to set the diagnostic level to bypass:

```
Console> (enable) set test diaglevel bypass
Diagnostic level set to bypass.
Console> (enable)
```

Related Commands

show test

set time

Use the **set time** command to change the time of day on the system clock.

set time [*day_of_week*] [*mm/dd/yy*] [*hh:mm:ss*]

Syntax Description

day_of_week	(Optional) Day of the week.
mm/dd/yy	(Optional) Month, day, and year.
hh:mm:ss	(Optional) Current time in 24-hour format.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to set the system clock to Saturday, October 31, 1998, 7:50 a.m:

```
Console> (enable) set time sat 10/31/98 7:50
Sat Oct 31 1998, 07:50:00
Console> (enable)
```

Related Commands

show time

set timezone

Use the **set timezone** command to set the time zone for the system.

set timezone [*zone_name*] [*hours* [*minutes*]]

Syntax Description

zone_name	(Optional) Name of the time zone to be displayed.
hours	(Optional) Number of hours offset from UTC.
minutes	(Optional) Number of minutes offset from UTC. If the specified *hours* value is a negative number, then the *minutes* value is assumed to be negative as well.

Defaults

The default is the time zone is set to UTC.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set timezone** command is effective only when NTP is running. If you set the time explicitly and NTP is disengaged, the **set timezone** command has no effect. If you have enabled NTP and have not entered the **set timezone** command, the Catalyst 6000 family switch displays UTC by default.

Examples

This example shows how to set the time zone to pacific standard time with an offset of minus 8 hours from UTC:

```
Console> (enable) set timezone PST -8
Timezone set to “PST”, offset from UTC is -8 hours.
Console> (enable)
```

Related Commands

clear timezone
show timezone

set traffic monitor

Use the **set traffic monitor** command to configure the threshold at which a high-traffic log will be generated.

set traffic monitor *threshold*

Syntax Description

threshold	**1** to **100** percent.

Defaults

The threshold is set to 100 percent; no high-traffic log is created.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If backplane traffic exceeds the threshold configured by the **set traffic monitor** command, a high-traffic log is created. If the threshold is set to 100 percent, no high-traffic system warning is generated.

Examples

This example shows how to set the high-traffic threshold to 80 percent:

```
Console> (enable) set traffic monitor 80
Traffic monitoring threshold set to 80%.
Console> (enable)
```

Related Commands

show traffic

set trunk

Use the **set trunk** command to configure trunk ports and to add VLANs to the allowed VLAN list for existing trunks.

set trunk *mod/port* {**on** | **off** | **desirable** | **auto** | **nonegotiate**}[*vlans*] [**isl** | **dot1q** | **negotiate**]

set trunk all off

Syntax Description

mod/port	Number of the module and the port on the module.
on	Keyword to force the port to become a trunk port and persuade the neighboring port to become a trunk port. The port becomes a trunk port even if the neighboring port does not agree to become a trunk.
off	Keyword to force the port to become a nontrunk port and persuade the neighboring port to become a nontrunk port. The port becomes a nontrunk port even if the neighboring port does not agree to become a nontrunk port.
desirable	Keyword to cause the port to negotiate actively with the neighboring port to become a trunk link.
auto	Keyword to cause the port to become a trunk port if the neighboring port tries to negotiate a trunk link.
nonegotiate	Keyword to force the port to become a trunk port but prevent it from sending DTP frames to its neighbor.
vlans	(Optional) VLANs to add to the list of allowed VLANs on the trunk; valid values are from **1** to **1000** and **1025** to **4094**.
isl	(Optional) Keyword to specify an ISL trunk on a Fast or Gigabit Ethernet port.
dot1q	(Optional) Keyword to specify an IEEE 802.1Q trunk on a Fast or Gigabit Ethernet port.
negotiate	(Optional) Keyword to specify that the port become an ISL (preferred) or 802.1Q trunk, depending on the configuration and capabilities of the neighboring port.
all off	Keywords to turn off trunking on all ports.

Defaults

The default port mode is **auto**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

The following usage guidelines apply when using the **set trunk** command:

- If a trunk-type keyword (**isl**, **dot1q**, **negotiate**) is not specified when configuring an EtherChannel trunk, the current trunk type is not affected.
- To return a trunk to its default trunk type and mode, enter the **clear trunk** *mod/port* command.
- Trunking capabilities are hardware-dependent. Refer to the *Catalyst 6000 Family Module Installation Guide* to determine the trunking capabilities of your hardware, or enter the **show port capabilities** command.
- Catalyst 6000 family switches use the DTP to negotiate trunk links automatically on EtherChannel ports. Whether a port will negotiate to become a trunk port depends on both the mode and the trunk type specified for that port. Refer to the *Catalyst 6000 Family Software Configuration Guide* for detailed information on how trunk ports are negotiated.
- DTP is a point-to-point protocol. However, some internetworking devices might improperly forward DTP frames. You can avoid this problem by ensuring that trunking is turned **off** on ports connected to non-Catalyst 6000 family switch devices if you do not intend to trunk across those links. When enabling trunking on a link to a Cisco router, enter the **noneg** keyword to cause the port to become a trunk but not generate DTP frames.
- To remove VLANs from the allowed list for a trunk, enter the **clear trunk** *mod/port vlans* command. When you first configure a port as a trunk, the **set trunk** command always adds *all* VLANs to the allowed VLAN list for the trunk, even if you specify a VLAN range (the specified VLAN range is ignored).
- To remove VLANs from the allowed list, enter the **clear trunk** *mod/port vlans* command. To later add VLANs that were removed, enter the **set trunk** *mod/port vlans* command.
- You cannot change the allowed VLAN range on the MSM port. The MSM port can be configured only as an IEEE 802.1Q-type trunk.
- For trunking to be negotiated on EtherChannel ports, the ports must be in the same VTP domain. However, you can use the **on** or **noneg** mode to force a port to become a trunk, even if it is in a different domain.

Examples

This example shows how to set port 2 on module 1 as a trunk port:

```
Console> (enable) set trunk 1/2 on
Port(s) 1/2 trunk mode set to on.
Console> (enable)
```

This example shows how to add VLANs 5 through 50 to the allowed VLAN list for a trunk port (VLANs were previously removed from the allowed list with the **clear trunk** command):

```
Console> (enable) set trunk 1/1 5-50
Adding vlans 5-50 to allowed list.
Port(s) 1/1 allowed vlans modified to 1,5-50,101-1005.
Console> (enable)
```

This example shows how to set port 5 on module 4 as an 802.1Q trunk port in **desirable** mode:

```
Console> (enable) set trunk 4/5 desirable dot1q
Port(s) 4/5 trunk mode set to desirable.
Port(s) 4/5 trunk type set to dot1q.
Console> (enable)
```

Related Commands

clear trunk
set vtp
show trunk
show vtp statistics

set udld

Use the **set udld** command to enable or disable the UDLD information display on specified ports or globally on all ports.

set udld enable | **disable** [*mod/port*]

Syntax Description

enable	Keyword to enable the UDLD information display.
disable	Keyword to disable the UDLD information display.
mod/port	(Optional) Number of the module and port on the module.

Defaults

The defaults are as follows:

- UDLD global enable state—Globally disabled.
- UDLD per-port enable state for fiber-optic media—Enabled on all Ethernet fiber-optic ports.
- UDLD per-port enable state for twisted-pair (copper) media—Disabled on all Ethernet 10/100 and 1000BASE-TX ports.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

Whenever a unidirectional connection is detected, UDLD displays a syslog message to notify you and the network management application (through SNMP) that the port on which the misconfiguration has been detected has been disabled.

If you enter the global **set udld enable** or **disable** command, UDLD is globally configured. If UDLD is globally disabled, UDLD is automatically disabled on all interfaces, but the per-port enable (or disable) configuration is not changed. If UDLD is globally enabled, whether UDLD is running on an interface or not depends on its per-port configuration.

UDLD is supported on both Ethernet fiber and copper interfaces. UDLD can only be enabled on Ethernet fiber or copper interfaces.

Examples

This example shows how to enable the UDLD message display for port 1 on module 2:

```
Console> (enable) set udld enable 2/1
UDLD enabled on port 2/1.
Warning:UniDirectional Link Detection
should be enabled only on ports not connected to hubs,
media converters or similar devices.
Console> (enable)
```

This example shows how to disable the UDLD message display for port 1 on module 2:

```
Console> (enable) set udld disable 2/1
UDLD disabled on port 2/1.
Warning:UniDirectional Link Detection
should be enabled only on ports not connected to hubs,
media converters or similar devices.
Console> (enable)
```

This example shows how to enable the UDLD message display for all ports on all modules:

```
Console> (enable) set udld enable
UDLD enabled globally.

Console> (enable)
```

This example shows how to disable the UDLD message display for all ports on all modules:

```
Console> (enable) set udld disable
UDLD disabled globally
Console> (enable)
```

Related Commands **show udld**

set udld aggressive-mode

Use the **set udld aggressive-mode** command to enable or disable the UDLD aggressive mode on specified ports.

set udld aggressive-mode enable | **disable** *mod/port*

Syntax Description

enable	Keyword to enable UDLD aggressive mode.
disable	Keyword to disable UDLD aggressive mode.
mod/port	Number of the module and port on the module.

Defaults

The default is aggressive mode is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can use the aggressive mode in cases in which a port that sits on a bidirectional link stops receiving packets from its neighbor. When this happens, if aggressive mode is enabled on the port, UDLD will try to reestablish the connection with the neighbor. If connection is not reestablished after eight failed retries, the port is error disabled.

We recommend that you use this command on point-to-point links between Cisco switches only.

This command is not supported by the NAM.

Examples

This example shows how to enable aggressive mode:

```
Console> (enable) set udld aggressive-mode enable 2/1
Aggressive UDLD enabled on port 5/13.
Warning:Aggressive Mode for UniDirectional Link Detection
should be enabled only on ports not connected to hubs,
media converters or similar devices.
Console> (enable)
```

Related Commands

set udld
show udld

set udld interval

Use the **set udld interval** command to set the UDLD message interval timer.

set udld interval *interval*

Syntax Description

interval	Message interval in seconds; valid values are from **7** to **90** seconds.

Defaults

The default is 15 seconds.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

Examples

This example shows how to set the message interval timer:

```
Console> (enable) set udld interval 90
UDLD message interval set to 90 seconds
Console> (enable)
```

Related Commands

set udld
show udld

set vlan

Use the **set vlan** command to group ports into a VLAN, set the private VLAN type, or map or unmap VLANs to or from an instance.

set vlan {*vlans*}{*mod/ports*}

set vlan {*vlans*} [**name** *name*] [**type** *type*] [**state** *state*] [**said** *said*] [**mtu** *mtu*] [**bridge** *bridge_num*] [**mode** *bridge_mode*] [**stp** *stp_type*] [**translation** *vlan_num*] [**aremaxhop** *hopcount*] [**pvlan-type** *pvlan_type*] [**mistp-instance** *mistp_instance*] [**ring** *hex_ring_number*] [**decring** *decimal_ring_number*] [**parent** *vlan_num*] [**backupcrf** {**off** | **on**}] [**stemaxhop** *hopcount*] [**rspan**]

Syntax Description

vlans	Number identifying the VLAN; valid values are from **1** to **1000** and from **1025** to **4094**.
mod/ports	Number of the module and ports on the module belonging to the VLAN.
name *name*	(Optional) Keyword and variable to define a text string used as the name of the VLAN; valid values are from 1 to 32 characters.
type *type*	(Optional) Keyword and variable to identify the VLAN type.
state *state*	(Optional) Keyword and variable to specify whether the state of the VLAN is active or suspended.
said *said*	(Optional) Keyword and variable to specify the security association identifier; valid values are from **1** to **4294967294**.
mtu *mtu*	(Optional) Keyword and variable to specify the maximum transmission unit (packet size, in bytes) that the VLAN can use; valid values are from **576** to **18190**.
bridge *bridge_num*	(Optional) Keyword and variable to specify the identification number of the bridge; valid values are hexadecimal numbers from **0x1** to **0xF**.
mode *bridge_mode*	(Optional) Keyword and variable to specify the bridge mode; valid values are **srt** and **srb**.
stp *stp_type*	(Optional) Keyword and variable to specify the STP type; valid values are **ieee**, **ibm**, and **auto**.
translation *vlan_num*	(Optional) Keyword and variable to specify a translational VLAN used to translate FDDI or Token Ring to Ethernet; valid values are from **1** to **1000** and from **1025** to **4094**.
aremaxhop *hopcount*	(Optional) Keyword and variable to specify the maximum number of hops for All-Routes Explorer frames; valid values are from **1** to **13**.
pvlan-type *pvlan-type*	(Optional) Keyword and options to specify the private VLAN type. See the "Usage Guidelines" section for valid values.
mistp-instance *mistp_instance*	(Optional) Keyword and variable to specify the MISTP instance; valid values are **none** and from **1** to **16**.

ring *hex_ring_number*	(Optional) Keyword to specify the VLAN as the primary VLAN in a private VLAN.
decring *decimal_ring_number*	(Optional) Keyword and variable to specify the decimal ring number; valid values are from **1** to **4095**.
parent *vlan_num*	(Optional) Keyword and variable to specify the VLAN number of the parent VLAN; valid values are from **1** to **1000** and from **1025** to **4094**.
backupcrf off | **on**	(Optional) Keywords to specify whether the TrCRF is a backup path for traffic.
stemaxhop *hopcount*	(Optional) Keyword and variable to specify the maximum number of hops for Spanning Tree Explorer frames; valid values are from **1** to **14**.
rspan	(Optional) Keyword to create a VLAN for remote SPAN.

Defaults

The default values are as follows:

- Switched Ethernet ports and Ethernet repeater ports are in VLAN 1.
- *said* is 100001 for VLAN 1, 100002 for VLAN 2, 100003 for VLAN 3, and so forth.
- *type* is Ethernet.
- *mtu* is 1500 bytes.
- *state* is active.
- *hopcount* is 7.
- *pvlan type* is none.
- *mistp_instance* is no new instances have any VLANs mapped. For an existing VLAN, the existing instance configuration is used.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

If you are configuring normal-range VLANs, you cannot use the **set vlan** command until the Catalyst 6000 family switch is either in VTP transparent mode (**set vtp mode transparent**) or until a VTP domain name has been set (**set vtp domain name**). To create a private VLAN, UTP mode must be transparent.

VLAN 1 parameters are factory configured and cannot be changed.

If you specify a range of VLANs, you cannot use the VLAN name.

If you enter the **mistp-instance none** command, the specified VLANs are unmapped from any instance they are mapped to.

The **set vlan** *vlan_num* **mistp-instance** *mistp_instance* command is available in PVST+ mode.

You cannot set multiple VLANs for ISL ports using this command. The VLAN name can be from 1 to 32 characters in length. If you are adding a new VLAN or modifying an existing VLAN, the VLAN number must be within the range of 1 to 1000 and 1025 to 4094.

If you want to use the extended-range VLANs (1025 to 4094), you must enable the MAC address reduction feature using the **set spantree macreduction** command. When you enable MAC address reduction, the pool of MAC addresses used for the VLAN spanning tree is disabled, leaving a single MAC address that identifies the switch.

If you use the **rspan** keyword for remote SPAN VLANs, you should not configure an access port (except the remote SPAN destination ports) on these VLANs. Learning is disabled for remote SPAN VLANs.

If you use the **rspan** keyword for remote SPAN VLANs, only the **name** *name* and the **state** {**active** | **suspend**} variables are supported.

The **stemaxhop** *hopcount* parameter is valid only when defining or configuring TrCRFs.

The **bridge** *bridge_num*, **mode** *bridge_mode*, **stp** *stp_type*, and **translation** *vlan_num* keywords and values are supported only when the Catalyst 6000 family switch is used as a VTP server for Catalyst 5000 family switches in the Token Ring and FDDI networks.

You must configure a private VLAN on the supervisor engine.

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

- **primary** specifies the VLAN as the primary VLAN in a private VLAN.
- **isolated** specifies the VLAN as the isolated VLAN in a private VLAN.
- **community** specifies the VLAN as the community VLAN in a private VLAN.
- **twoway-community** specifies the VLAN as a bidirectional community VLAN that carries the traffic among community ports and to and from community ports to and from the MSFC.
- **none** specifies that the VLAN is a normal Ethernet VLAN, not a private VLAN.

Only regular VLANs with no access ports assigned to them can be used in private VLANs. Do not use the **set vlan** command to add ports to a private VLAN; use the **set pvlan** command to add ports to a private VLAN.

VLANs 1001, 1002, 1003, 1004, and 1005 cannot be used in private VLANs.

VLANs 1025 to 4094 are extended-range VLANs.

VLANs in a suspended state do not pass packets.

Examples

This example shows how to set VLAN 850 to include ports 3 through 7 on module 3:

```
Console> (enable) set vlan 850 3/4-7
VLAN 850 modified.
VLAN  Mod/Ports
---- ----------------------
850   3/4-7
Console> (enable)
```

This example shows how to set VLAN 7 as a primary VLAN:

```
Console> (enable) set vlan 7 pvlan-type primary
Console> (enable)
```

This example shows how to set VLAN 901 as an isolated VLAN:

```
Console> (enable) set vlan 901 pvlan-type isolated
Console> (enable)
```

This example shows how to set VLAN 903 as a community VLAN:

```
Console> (enable) set vlan 903 pvlan-type community
Console> (enable)
```

This example shows how to unmap all instances currently mapped to VLAN 5:

```
Console> (enable) set vlan 5 mistp-instance none
Vlan 5 configuration successful
Console> (enable)
```

Related Commands

clear config pvlan
clear pvlan mapping
clear vlan
set pvlan
set spantree macreduction
set vlan mapping
show pvlan
show pvlan mapping
show vlan

set vlan mapping

Use the **set vlan mapping** command to map reserved VLANs to nonreserved VLANs or map 802.1Q VLANs to ISL VLANs.

set vlan mapping reserved *vlan* **non-reserved** *vlan*

set vlan mapping dot1q *1q_vlan_num* **isl** *isl_vlan_num*

Syntax Description

reserved *vlan*	Keyword to specify the reserved VLAN; valid values are from **1006** to **1024**.
non-reserved *vlan*	Keyword and variable to specify the nonreserved VLAN; valid values are from **1** to **1000** and from **1025** to **4094**.
dot1q *1q_vlan_num*	Keyword and variable to specify the 802.1Q VLAN; valid values are from **1001** to **4094**.
isl *isl_vlan_num*	Keyword to specify the ISL VLAN; valid values are from **1** to **1024**.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

VLAN and MISTP instance mapping can be set only on the switch that is in either VTP server mode or in transparent mode.

IEEE 802.1Q VLAN trunks support VLANs 1 through 4094. ISL VLAN trunks support VLANs 1 through 1024 (1005 to 1024 are reserved). The switch automatically maps 802.1Q VLANs 1000 and lower to ISL VLANs with the same number.

Use this feature to map 802.1Q VLANs above 1000 to ISL VLANs.

The total of all mappings must be less than or equal to eight. Only one 802.1Q VLAN can be mapped 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.

The **reserved** *vlan* range is 1002 to 1024. You can map the entire reserved range with the exception of the default media VLANs 1002 to 1005.

You cannot overwrite existing VLAN mapping. If the VLAN number already exists, the command is aborted. You must first clear that mapping.

If the VLAN number does not exist, then either of the following occurs:

- If the switch is in server or transparent mode, the VLAN is created with all default values.
- If the switch is in client mode, then the command proceeds without creating the VLAN. A warning will be given indicating that the VLAN does not exist.

If the table is full, the command is aborted with an error message indicating the table is full.

dot1q VLANs are rejected if any extended-range VLANs are present.

Examples

This example shows how to map reserved VLAN 1010 to nonreserved VLAN 4000:

```
Console> (enable) set vlan mapping reserved 1010 non-reserved 4000
Vlan 1010 successfully mapped to 4000.
Console> (enable)
```

This example shows the display if you enter an existing mapping:

```
Console> (enable) set vlan mapping reserved 1011 non-reserved 4001
Vlan mapping from vlan 1011 to vlan 4001 already exists.
Console> (enable)
```

This example shows the display if the mapping table is full:

```
Console> (enable) set vlan mapping reserved 1010 non-reserved 4000
Vlan mapping table full. Maximum of 8 mappings allowed.
Console> (enable)
```

This example shows how to map VLAN 850 to ISL VLAN 1022:

```
Console> (enable) set vlan mapping dot1q 850 isl 1022
Vlan 850 configuration successful
Vlan mapping successful
Console> (enable)
```

This example shows the display if you enter a VLAN that does not exist:

```
Console> (enable) set vlan mapping dot1q 2 isl 1016
Vlan Mapping Set
Warning: Vlan 2 Nonexistent
Console> (enable)
```

This example shows the display if you enter an existing mapping:

```
Console> (enable) set vlan mapping dot1q 3 isl 1022
1022 exists in the mapping table. Please clear the mapping first.
Console> (enable)
```

This example shows the display if the mapping table is full:

```
Console> (enable) set vlan mapping dot1q 99 isl 1017
Vlan Mapping Table Full.
Console> (enable)
```

Related Commands

clear vlan mapping
show vlan

set vmps downloadmethod

Use the **set vmps downloadmethod** command to specify whether to use TFTP or rcp to download the VMPS database.

set vmps downloadmethod {**rcp** | **tftp**} [*username*]

Syntax Description

rcp	Keyword to specify rcp as the method for downloading the VMPS database.
tftp	Keyword to specify TFTP as the method for downloading the VMPS database.
username	(Optional) Username for downloading with rcp.

Defaults

If no method is specified, TFTP will be used.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The *username* option is not allowed if you specify **tftp** as the download method.

Examples

This example shows how to specify the method for downloading the VMPS database:

```
Console> (enable) set vmps downloadmethod rcp jdoe
vmps downloadmethod : RCP
rcp vmps username   : jdoe
Console> (enable)
```

Related Commands

download
set rcp username
show vmps

set vmps downloadserver

Use the **set vmps downloadserver** command to specify the IP address of the TFTP or rcp server from which the VMPS database is downloaded.

set vmps downloadserver *ip_addr* [*filename*]

Syntax Description

ip_addr	IP address of the TFTP or rcp server from which the VMPS database is downloaded.
filename	(Optional) VMPS configuration filename on the TFTP or rcp server.

Defaults

If *filename* is not specified, the **set vmps downloadserver** command uses the default filename vmps-config-database.1.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to specify the server from which the VMPS database is downloaded and how to specify the configuration filename:

```
Console> (enable) set vmps downloadserver 192.168.69.100 vmps_config.1
IP address of the server set to 192.168.69.100
VMPS configuration filename set to vmps_config.1
Console> (enable)
```

Related Commands

download
set vmps state
show vmps

set vmps server

Use the **set vmps server** command to configure the VMPS server.

set vmps server *ip_addr* [**primary**]

set vmps server retry *count*

set vmps server reconfirminterval *interval*

Syntax Description

ip_addr	IP address of the VMPS server.
primary	(Optional) Keyword to specify the device as the primary VMPS server.
retry *count*	Keyword and variable to specify the retry interval; valid values are from **1** to **10** minutes.
reconfirminterval *interval*	Keyword and variable to specify the reconfirmation interval; valid values are from **0** to **120** minutes.

Defaults

If no IP address is specified, VMPS uses the local VMPS configuration.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can specify the IP addresses of up to three VMPS servers. You can define any VMPS server as the primary VMPS server.

If the primary VMPS server is down, all subsequent queries go to a secondary VMPS server. VMPS checks on the primary server's availability once every five minutes. When the primary VMPS server comes back online, subsequent VMPS queries are directed back to the primary VMPS server.

To use a co-resident VMPS (when VMPS is enabled in a device), configure one of the three VMPS addresses as the IP address of interface sc0.

When you specify the **reconfirminterval** *interval*, enter 0 to disable reconfirmation.

Examples

This example shows how to define a primary VMPS server:

```
Console> (enable) set vmps server 192.168.10.140 primary
192.168.10.140 added to VMPS table as primary domain server.
Console> (enable)
```

This example shows how to define a secondary VMPS server:

```
Console> (enable) set vmps server 192.168.69.171
192.168.69.171 added to VMPS table as backup domain server.
Console> (enable)
```

Related Commands

clear vmps server
show vmps

set vmps state

Use the **set vmps state** command to enable or disable VMPS.

set vmps state {**enable** | **disable**}

Syntax Description

enable	Keyword to enable VMPS.
disable	Keyword to disable VMPS.

Defaults

By default, VMPS is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Before using the **set vmps state** command, you must use the **set vmps tftpserver** command to specify the IP address of the server from which the VMPS database is downloaded.

Examples

This example shows how to enable VMPS:

```
Console> (enable) set vmps state enable
Vlan membership Policy Server enabled.
Console> (enable)
```

This example shows how to disable VMPS:

```
Console> (enable) set vmps state disable
All the VMPS configuration information will be lost and the resources released on disable.
Do you want to continue (y/n[n]):y
VLAN Membership Policy Server disabled.
Console> (enable)
```

Related Commands

download
show vmps

set vtp

Use the **set vtp** command to set the options for VTP.

set vtp [**domain** *domain_name*] [**mode** {**client** | **server** | **transparent** | **off**}] [**passwd** *passwd*] [**pruning** {**enable** | **disable**}] [**v2** {**enable** | **disable**}]

Syntax Description

domain *domain_name*	(Optional) Keywords to define the name that identifies the VLAN management domain. The *domain_name* can be from 1 to 32 characters in length.
mode {**client** | **server** | **transparent** | **off**}	(Optional) Keywords to specify the VTP mode.
passwd *passwd*	(Optional) Keyword and variable to define the VTP password; the VTP password can be from 8 to 64 characters in length.
pruning {**enable** | **disable**}	(Optional) Keywords to enable or disable VTP pruning for the entire management domain.
v2 {**enable** | **disable**}	(Optional) Keywords to enable or disable version 2 mode.

Defaults

The defaults are as follows: server mode, no password, pruning disabled, and v2 disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

This command is not supported on extended-range VLANs.

VTP pruning and MISTP cannot be enabled at the same time.

All switches in a VTP domain must run the same version of VTP. VTP version 1 and VTP version 2 do not operate on switches in the same VTP domain.

If all switches in a domain are VTP version 2-capable, you only need to enable VTP version 2 on one switch (using the **set vtp v2 enable** command); the version number is then propagated to the other version 2-capable switches in the VTP domain.

If the VTP password has already been defined, entering **passwd 0** (zero) clears the VTP password.

VTP supports four different modes: server, client, transparent, and off. If you make a change to the VTP or VLAN configuration on a switch in server mode, that change is propagated to all of the switches in the same VTP domain.

If the receiving switch is in server mode and its revision number is higher than the sending switch, the configuration is not changed. If the revision number is lower, the configuration is duplicated.

VTP can be set to either server or client mode only when dynamic VLAN creation is disabled.

If the receiving switch is in server mode, the configuration is not changed.

If the receiving switch is in client mode, the client switch changes its configuration to duplicate the configuration of the server. Make sure to make all VTP or VLAN configuration changes on a switch in server mode.

If the receiving switch is in transparent mode, the configuration is not changed. Switches in transparent mode do not participate in VTP. If you make VTP or VLAN configuration changes on a switch in transparent mode, the changes are not propagated to the other switches in the network.

When you configure the VTP off mode, the switch functions the same as in VTP transparent mode except that VTP advertisements are not forwarded.

The **pruning** keyword is used to enable or disable VTP pruning for the VTP domain. VTP pruning causes information about each pruning-eligible VLAN to be removed from VTP updates if there are no stations belonging to that VLAN out a particular switch port. Use the **set vtp pruneeligible** and **clear vtp pruneeligible** commands to specify which VLANs should or should not be pruned when pruning is enabled for the domain.

Use the **clear config all** command to remove the domain from the switch.

For more information about VTP, refer to Chapter 10, "Configuring VTP," in the *Catalyst 6000 Family Configuration Guide*.

Caution Be careful when you use the **clear config all** command. This command clears the entire switch configuration, not just the VTP domain.

Examples

This example shows how to use the **set vtp** command:

```
Console> (enable) set vtp domain Engineering mode client
VTP domain Engineering modified
Console> (enable)
```

This example shows what happens if you try to change VTP to server or client mode and dynamic VLAN creation is enabled:

```
Console> (enable) set vtp mode server
Failed to Set VTP to Server. Please disable Dynamic VLAN Creation First.
Console> (enable)
```

This command shows how to set VTP to off mode:

```
Console> (enable) set vtp mode off
VTP domain modified
Console> (enable)
```

Related Commands

clear vlan
clear vtp pruneeligible
set vlan
set vtp pruneeligible
show vlan
show vtp domain

set vtp pruneeligible

Use the **set vtp pruneeligible** command to specify which VTP domain VLANs are pruning eligible.

set vtp pruneeligible *vlans*

Syntax Description

vlans	Range of VLAN numbers; valid values are from **2** to **1000**.

Defaults

The default is VLANs 2 through 1000 are eligible for pruning.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

VTP pruning causes information about each pruning-eligible VLAN to be removed from VTP updates if there are no stations belonging to that VLAN out a particular switch port. Use the **set vtp** command to enable VTP pruning.

By default, VLANs 2 through 1000 are pruning eligible. You do not need to use the **set vtp pruneeligible** command unless you have previously used the **clear vtp pruneeligible** command to make some VLANs pruning ineligible. If VLANs have been made pruning ineligible, use the **set vtp pruneeligible** command to make them pruning eligible again.

Examples

This example shows how to configure pruning eligibility for VLANs 120 and 150:

```
Console> set vtp pruneeligible 120,150
Vlans 120,150 eligible for pruning on this device.
VTP domain nada modified.
Console>
```

In this example, VLANs 200–500 were made pruning ineligible using the **clear vtp pruneeligible** command. This example shows how to make VLANs 220 through 320 pruning eligible again:

```
Console> set vtp pruneeligible 220-320
Vlans 2-199,220-320,501-1000 eligible for pruning on this device.
VTP domain Company modified.
Console>
```

Related Commands

clear vtp pruneeligible
set vlan
show vtp domain

show accounting

Use the **show accounting** command to display accounting setup and configuration information on the switch.

show accounting

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows the configuration details of a switch with RADIUS accounting enabled:

```
Console> (enable) show accounting
Event     Method1 Mode
-----     ------- -----
exec:     Radius  stop-only
connect:  Radius  stop-only
system:   -       -
commands:
config:   -       -
all:      -       -

TACACS+ Suppress for no username: disabled
Update Frequency: newinfo

Accounting information:
-----------------------

Active Accounted actions on tty2168059284l, User NULL Priv 15
 Task ID 3, EXEC Accounting record, 0,00:00:22 Elapsed
 task_id=3 start_time=934463479 timezone=UTC service=shell

Active Accounted actions on tty0l, User kannank Priv 15
 Task ID 2, EXEC Accounting record, 0,00:01:23 Elapsed
 task_id=2 start_time=934463418 timezone=UTC service=shell

Active Accounted actions on tty2168059284l, User danny Priv 15
 Task ID 4, Connection Accounting record, 0,00:00:07 Elapsed
 task_id=4 start_time=934463495 timezone=UTC service=connection protocol=telnet
addr=-1407968771 cmd=telnet 172.20.25.253
```

```
Overall Accounting Traffic:
          Starts   Stops  Active
Exec      1        0       2
Connect   0        0       1
Command   0        0       0
System    0        0       0

Console> (enable)
```

This example shows the configuration details of a switch with TACACS+ accounting enabled:

```
Console> (enable) show accounting
TACACS+:
Update: periodic (25 seconds)
Supress:   disabled

           Status    Mode
           --------  -----------
exec:      disabled  stop-only
connect:   disabled  stop-only
system:    disabled  stop-only
network:   disabled  stop-only
commands:
 config:   disabled  stop-only
 all:      disabled  stop-only

Radius:
           Status    Mode
           --------  -----------
exec:      disabled  stop-only
connect:   disabled  stop-only
system:    disabled  stop-only

 TACACS+ Suppress for no username: disabled
 Update Frequency: newinfo

 Accounting information:
 -----------------------

 Active Accounted actions on tty2168059284l, User NULL Priv 15
  Task ID 3, EXEC Accounting record, 0,00:00:22 Elapsed
  task_id=3 start_time=934463479 timezone=UTC service=shell

 Active Accounted actions on tty0l, User kannank Priv 15
  Task ID 2, EXEC Accounting record, 0,00:01:23 Elapsed
  task_id=2 start_time=934463418 timezone=UTC service=shell

 Active Accounted actions on tty2168059284l, User danny Priv 15
  Task ID 4, Connection Accounting record, 0,00:00:07 Elapsed
  task_id=4 start_time=934463495 timezone=UTC service=connection protocol=telnet
addr=-1407968771 cmd=telnet 172.20.25.253

 Overall Accounting Traffic:
          Starts   Stops  Active
 Exec      1        0       2
 Connect   0        0       1
 Command   0        0       0
 System    0        0       0

Console> (enable)
```

Related Commands

- set accounting commands
- set accounting connect
- set accounting exec
- set accounting suppress
- set accounting system
- set accounting update

show aclmerge

Use the **show aclmerge** command to display information about the ACL merge algorithm.

show aclmerge bdd

show aclmerge algo

Syntax Description

bdd	Keyword to display if BDD is enabled or disabled.
algo	Keyword to display the ACL merge algorithm currently in use.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to display the status of BDD:

```
Console> (enable) show aclmerge bdd
Bdd is not enabled.
On system restart bdd will be disabled.
Console> (enable)
```

This example shows how to display the ACL merge algorithm currently in use:

```
Console> (enable) show aclmerge algo
Current acl merge algorithm is odm.
Console> (enable)
```

Related Commands

set aclmerge algo
set aclmerge bdd

show alias

Use the **show alias** command to display a listing of defined command aliases.

show alias [*name*]

Syntax Description

name	(Optional) Name of the alias to be displayed.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If *name* is not specified, all defined aliases are displayed.

Examples

This example shows how to display all aliases:

```
Console> show alias
shint           show interface
cc              clear config
shf             show flash
sip             show ip route
Console>
```

Related Commands

clear alias
set alias

show arp

Use the **show arp** command to display the ARP table.

show arp [*ip_addr* | *hostname*] [**noalias**]

Syntax Description

ip_addr	(Optional) Number of the IP address.
hostname	(Optional) Name of the host.
noalias	(Optional) Keyword to force the display to show only IP addresses, not IP aliases.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

ARP aging time is the period of time that indicates when an ARP entry is removed from the ARP table. Set this value by entering the **set arp agingtime** command. The remaining lines of the display show the mappings of IP addresses (or IP aliases) to MAC addresses.

Use the *ip_addr* or the *hostname* options to specify an IP host when the ARP cache is large.

Examples

This example shows how to display the ARP table:

```
Console> (enable) show arp
ARP Aging time = 300 sec
+ - Permanent Arp Entries
* - Static Arp Entries
* 2.2.2.2                      at 00-08-cc-44-aa-18 on vlan 5
+ 1.1.1.1                      at 00-08-94-cc-02-aa on vlan 5
142.10.52.195                          at 00-10-07-3c-05-13 port 7/1-4 on vlan 5
192.70.31.126                          at 00-00-0c-00-ac-05 port 7/1-4 on vlan 5
121.23.79.121                          at 00-00-1c-03-00-40 port 7/1-4 on vlan 5
Console> (enable)
```

Related Commands

clear arp
set arp

show authentication

Use the **show authentication** command to display authentication information.

show authentication

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display authentication information:

```
Console> show authentication
                     Console Session   Telnet Session   Http Session
Login Authentication:
---------------------  ---------------  ---------------  -----------
tacacs                 disabled          disabled         disabled
radius                 disabled          disabled         enabled(*)
kerberos               disabled          disabled         disabled
local                  enabled(*)        enabled(*)       enabled
local                  enabled(primary)  enabled(primary)  enabled(primary)
attempt limit          3                 3                3
lockout timeout (sec)  disabled          disabled         disabled

Enable Authentication: Console Session   Telnet Session    Http Session
---------------------- ----------------- ----------------  ----------------
tacacs                 disabled          disabled          disabled
radius                 disabled          disabled          disabled
kerberos               disabled          disabled          disabled
local                  enabled(primary)  enabled(primary)  enabled(primary)
attempt limit          3                 3                 3
lockout timeout (sec)  disabled          disabled          disabled
Console>
```

Related Commands

set authentication enable
set authentication login

show authorization

Use the **show authorizaton** command to display authorization setup and configuration information on the switch.

show authorization

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display authorization setup and configuration information:

```
Console> (enable) show authorization
Telnet:
-------
            Primary   Fallback
            -------   --------
exec:       tacacs+    deny
enable:     tacacs+    deny
commands:
 config:    tacacs+    deny
 all:       -         -

Console:
--------
            Primary   Fallback
            -------   --------
exec:       tacacs+    deny
enable:     tacacs+    deny
commands:
 config:    tacacs+    deny
 all:       -         -

Console> (enable)
```

Related Commands

set authorization commands
set authorization enable
set authorization exec

show banner

Use the **show banner** command to view the MOTD and Catalyst 6500 series Switch Fabric Module LCD banner stored in NVRAM.

show banner

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the MOTD and Catalyst 6500 series Switch Fabric Module LCD banner stored in NVRAM:

```
Console> (enable) show banner
MOTD banner:

LCD config:
hello
there
Console> (enable)
```

Related Commands

set banner lcd
set banner motd

show boot

Use the **show boot** command to display the contents of the BOOT environment variables and the configuration register setting.

show boot [*mod*]

Syntax Description

mod	(Optional) Number of the supervisor engine containing the Flash device.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the BOOT environment variable:

```
Console> show boot
BOOT variable = bootflash:cat6000-sup.5-5-1.bin,1;slot0:cat6000-sup.5-4-1.bin,1;
CONFIG_FILE variable = slot0:switch.cfg

Configuration register is 0x800f
ignore-config: disabled
auto-config: non-recurring, overwrite, sync disabled
console baud: 9600
boot: image specified by the boot system commands
Console>
```

Related Commands

set boot auto-config
set boot config-register
set boot system flash

show boot device

Use the **show boot device** command to display the NAM boot string stored in NVRAM.

show boot device *mod*

Syntax Description

mod	Number of the module containing the Flash device.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This command is supported by the NAM module only.

Examples

This example shows how to display the boot device information for module 2:

```
Console> show boot device 2
Device BOOT variable = hdd:2
Console>
```

Related Commands

clear boot device
set boot device

show cam

Use the **show cam** command to display CAM table entries.

show cam {**dynamic** | **static** | **permanent** | **system**} [{*mod/port*} | *vlan*]

show cam *mac_addr* [*vlan*]

Syntax Description

dynamic	Keyword to display dynamic CAM entries.
static	Keyword to display static CAM entries.
permanent	Keyword to display permanent CAM entries.
system	Keyword to display system CAM entries.
mod/port	(Optional) Number of the module and the port on the module.
vlan	(Optional) Number of the VLAN; valid values are from **1** to **1005** and from **1025** to **4094**.
mac_addr	MAC address.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you specify a VLAN, then only those CAM entries matching the VLAN number are displayed.

If you do not specify a VLAN, all VLANs are displayed.

If the MAC address belongs to a router, it is shown by appending an "R" to the MAC address.

You can set the traffic filter for unicast addresses only; you cannot set the traffic filter for multicast addresses.

Examples

This example shows how to display dynamic CAM entries for all VLANs:

```
Console> show cam dynamic
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------    -----  -------------------------------------------
1     00-60-5c-86-5b-81     *    4/1 [ALL]
1     00-60-2f-35-48-17     *    4/1 [ALL]
1     00-80-24-f3-47-20     *    1/2 [ALL]
1     00-60-09-78-96-fb     *    4/1 [ALL]
1     00-80-24-1d-d9-ed     *    1/2 [ALL]
```

```
1     00-80-24-1d-da-01    *    1/2 [ALL]
1     08-00-20-7a-63-01    *    4/1 [ALL]

Total Matching CAM Entries Displayed = 7
Console>
```

This example shows how to display dynamic CAM entries for VLAN 1:

```
Console> show cam dynamic 1
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des  [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------  -----  -------------------------------------------
1     00-40-0b-60-d7-3c           2/1-2 [IP]
1     00-e0-34-8b-d3-ff           2/1-2 [IP]
1     00-e0-14-0f-df-ff           2/1-2 [IP]
1     00-00-0c-35-7f-42           2/1-2 [IP]
1     00-90-6f-a3-bb-ff           2/1-2 [IP]
1     00-e0-8f-63-7f-ff           2/1-2 [IP]
1     00-00-0c-35-7f-42           2/1-2 [GROUP]
.
. Display truncated
.
1     00-e0-f9-c8-33-ff           2/1-2 [IP]
Console>
```

This example shows routers listed as the CAM entries:

```
Console> show cam 00-00-81-01-23-45
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry
X = Port Security Entry

Router Watergate with IP address 172.25.55.1 has CAM entries:
VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------    -----  -------------------------------------------
1     00-00-81-01-23-45R    *    2/9 [IP]
2     00-00-81-01-23-45R    *    2/10 [IP]
Total Matching CAM Entries = 2
Console>

Console> (enable) show cam 00-00-81-01-23-45
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------    -----  -------------------------------------------
1     00-00-81-01-23-45R    *    FILTER
Console>
```

Related Commands

- **clear cam**
- **set cam**
- **show cam agingtime**
- **show config**

show cam agingtime

Use the **show cam agingtime** command to display CAM aging time information for all configured VLANs.

show cam agingtime [*vlan*]

Syntax Description

vlan	(Optional) Number of the VLAN or range of VLANs; valid values are from **1** to **1005** and from **1025** to **4094**.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display CAM aging time information:

```
Console> show cam agingtime
VLAN   1 aging time = 300 sec
VLAN   3 aging time = 300 sec
VLAN   5 aging time = 300 sec
VLAN   9 aging time = 300 sec
VLAN 100 aging time = 300 sec
VLAN 200 aging time = 300 sec
VLAN 201 aging time = 300 sec
VLAN 202 aging time = 300 sec
VLAN 203 aging time = 300 sec
Console>
```

This example shows how to display CAM aging time information for a specific VLAN:

```
Console> show cam agingtime 1005
VLAN 1005 aging time = 300 sec
Console>
```

Related Commands

clear cam
set cam
show cam

show cam count

Use the **show cam count** command to display the number of CAM entries only.

show cam count {**dynamic** | **static** | **permanent** | **system**} [*vlan*]

Syntax Description

dynamic	Keyword to display dynamic CAM entries.
static	Keyword to display static CAM entries.
permanent	Keyword to display permanent CAM entries.
system	Keyword to display system CAM entries.
vlan	(Optional) Number of the VLAN; valid values are from **1** to **1005** and from **1025** to **4094**.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a VLAN, all VLANs are displayed.

Examples

This example shows how to display the number of dynamic CAM entries:

```
Console> (enable) show cam count dynamic
Total Matching CAM Entries = 6
Console> (enable)
```

Related Commands

clear cam
set cam

show cam msfc

Use the **show cam msfc** command to display the router's MAC-VLAN entries.

show cam msfc {*mod*} [*vlan*]

Syntax Description

mod	Number of the module for which MSFC information is displayed.
vlan	(Optional) Number of the VLAN; valid values are from **1** to **1005** and from **1025** to **4094**.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you specify the VLAN, only CAM entries that belong to that VLAN are displayed.

Examples

This example shows how to display all CAM entries:

```
Console> (enable) show cam msfc
VLAN  Destination MAC      Destination-Ports or VCs        Xtag  Status
----  ------------------   ------------------------------  ----  ------
194   00-e0-f9-d1-2c-00R   7/1                             2     H
193   00-00-0c-07-ac-c1R   7/1                             2     H
193   00-00-0c-07-ac-5dR   7/1                             2     H
202   00-00-0c-07-ac-caR   7/1                             2     H
204   00-e0-f9-d1-2c-00R   7/1                             2     H
195   00-e0-f9-d1-2c-00R   7/1                             2     H
192   00-00-0c-07-ac-c0R   7/1                             2     H
192   00-e0-f9-d1-2c-00R   7/1                             2     H
204   00-00-0c-07-ac-ccR   7/1                             2     H
202   00-e0-f9-d1-2c-00R   7/1                             2     H
Total Matching CAM Entries Displayed = 14
Console> (enable)
```

This example shows how to display CAM entries for a specific VLAN:

```
Console> show cam msfc 15 192
VLAN  Destination MAC      Destination-Ports or VCs        Xtag  Status
----  ------------------   ------------------------------  ----  ------
192   00-00-0c-07-ac-c0R   7/1                             2     H
192   00-e0-f9-d1-2c-00R   7/1                             2     H
Console>
```

Related Commands

show cam

show cdp

Use the **show cdp** command to display CDP information.

show cdp

show cdp neighbors [*mod*[/*port*]] [**vlan** | **duplex** | **capabilities** | **detail**]

show cdp neighbors exlude ip-phone

show cdp port [*mod*[/*port*]]

Syntax Description

neighbors	Keyword to show CDP information for Cisco products connected to the switch.
[*mod*[/*port*]]	(Optional) Number of the module for which CDP information is displayed and optionally, the number of the port for which CDP information is displayed.
vlan	(Optional) Keyword to show the native VLAN number for the neighboring Cisco products.
duplex	(Optional) Keyword to show the duplex type of the neighboring Cisco products.
capabilities	(Optional) Keyword to show the capability codes for the neighboring Cisco products; valid values are **R**, **T**, **B**, **S**, **H**, **I**, and **r** (R = Router, T = Trans Bridge, B = Source Route Bridge, S = Switch, H = Host, I = IGMP, and r = Repeater).
detail	(Optional) Keyword to show detailed information about neighboring Cisco products.
exclude ip-phone	Keywords to exclude IP phone information from the display of neighboring Cisco products.
port	Keyword to show CDP port settings.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The per-port output of the **show cdp port** command is not displayed if you globally disable CDP. If you globally enable CDP, the per-port status is displayed.

If you enter the **show cdp neighbors** command for a device that supports earlier versions of CDP, "unknown" is displayed in the VTP Management Domain, Native VLAN, and Duplex fields.

If you do not specify a module number, CDP information for the entire switch is displayed.

Examples

This example shows how to display CDP information for the system:

```
Console> show cdp
CDP               :enabled
Message Interval  :60
Hold Time         :180
```

This example shows how to display detailed CDP neighbor information. The display varies depending on your network configuration at the time you run the command.

```
Console> show cdp neighbors 4 detail
Port (Our Port):4/4
Device-ID:69046406
Device Addresses:
  IP Address:172.20.25.161
Holdtime:150 sec
Capabilities:TRANSPARENT_BRIDGE SWITCH
Version:
  WS-C6009 Software, Version NmpSW: 5.4(1)CSX
  Copyright (c) 1995-1999 by Cisco Systems
Port-ID (Port on Device):4/8
Platform:WS-C6009
VTP Management Domain:unknown
Native VLAN:1
Duplex:half
Console>
```

This example shows how to display CDP information about neighboring systems:

```
Console> show cdp neighbors
* - indicates vlan mismatch.
# - indicates duplex mismatch.

Port     Device-ID                      Port-ID                   Platform
-------- ------------------------------ ------------------------- ------------
3/5      002267619                      3/6 *                     WS-C6000
3/6      002267619                      3/5                       WS-C6000
4/1      002267619                      4/2                       WS-C6000
4/2      002267619                      4/1 #                     WS-C6000
4/20     069000057                      8/5                       WS-C6000
5/1      005763872                      2/1                       WS-C6009
5/1      066506245                      2/1                       WS-C6009
5/1      066508595                      5/12 *#                   WS-C6009
5/1      066508596                      5/1                       WS-C6009
Console>
```

This example shows how to display duplex information about neighboring systems:

```
Console> show cdp neighbors duplex
* - indicates vlan mismatch.
# - indicates duplex mismatch.

Port     Device-ID                      Port-ID                   Duplex
-------- ------------------------------ ------------------------- ------
3/5      002267619                      3/6 *                     half
3/6      002267619                      3/5                       half
4/1      002267619                      4/2                       full
4/2      002267619                      4/1 #                     full
4/20     069000057                      8/5                       -
5/1      005763872                      2/1                       -
5/1      066506245                      2/1                       -
5/1      066508595                      5/12 *#                   half
5/1      066508596                      5/1                       half
Console>
```

This example shows how to display VLAN information about neighboring systems:

```
Console> show cdp vlan
* - indicates vlan mismatch.
# - indicates duplex mismatch.

Port     Device-ID                      Port-ID                  NativeVLAN
-------- ------------------------------ ------------------------ ----------
3/5      002267619                      3/6 *                    1
3/6      002267619                      3/5                      1
4/1      002267619                      4/2                      1
4/2      002267619                      4/1 #                    1
4/20     069000057                      8/5                      -
5/1      005763872                      2/1                      -
5/1      066506245                      2/1                      -
5/1      066508595                      5/12 *#                  1
5/1      066508596                      5/1                      1
Console>
```

This example shows how to display capability information about neighboring systems:

```
Console> show cdp neighbors capabilities
* - indicates vlan mismatch.
# - indicates duplex mismatch.

Port     Device-ID                      Port-ID                  Capabilities
-------- ------------------------------ ------------------------ ------------
3/5      002267619                      3/6 *                    T S
3/6      002267619                      3/5                      T S
4/1      002267619                      4/2                      T S
4/2      002267619                      4/1 #                    T S
4/20     069000057                      8/5                      T B S
5/1      005763872                      2/1                      T B S
5/1      066506245                      2/1                      T B S
5/1      066508595                      5/12 *#                  T B S
5/1      066508596                      5/1                      T B S
Console>
```

This example shows how to display CDP information for all ports:

```
Console> show cdp port
CDP               :enabled
Message Interval  :60
Hold Time         :180

Port      CDP Status
--------  ----------
 2/1      enabled
 2/2      enabled
 5/1      enabled
 5/2      enabled
 5/3      enabled
 5/4      enabled
 5/5      enabled
 5/6      enabled
 5/7      enabled
 5/8      enabled
Console>
```

Related Commands set cdp

show channel

Use the **show channel** command to display EtherChannel information for a channel.

show channel [*channel_id*] [**info** | **statistics** | **mac**]

show channel [*channel_id*] [**info** [*type*]]

show channel [*channel_id* | **all**] **protocol**

Syntax Description

channel_id	(Optional) Number of the channel.
info	(Optional) Keyword to display channel information.
statistics	(Optional) Keyword to display statistics about the port (PAgP packets sent and received).
mac	(Optional) Keyword to display MAC information about the channel.
type	(Optional) Keyword to display feature-related parameters; valid values are **spantree**, **trunk**, **protcol**, **gmrp**, **gvrp**, **qos**, **rsvp, cops, dot1qtunnel, auxiliaryvlan**, and **jumbo**.
all	(Optional) Keyword to display protocols of all channels.
protocol	Keyword to display channel protocol.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify *channel_id*, EtherChannel information is shown for all channels.

No information is displayed if the channel specified is not in use.

If you enter the optional **info** *type*, the specified feature-related parameters are displayed in the output.

To display protocols on all channels, enter the **show channel all protocol** command.

Examples

This example shows how to display channel information for a specific channel:

```
Console> show channel 865
Channel Ports                                            Status    Channel
id                                                                 Mode
------- ------------------------------------------------ --------- --------------
    865 4/1-2                                            connected desirable
                                                                   non-silent
Console>
```

This example shows how to display channel information for all channels:

```
Console> show channel
Channel Id   Ports
-----------  ------------------------------------------------
768          2/1-2
769          4/3-4
770          4/7-8
Console>
```

This example shows how to display port information for a specific channel:

```
Console> show channel 769
Chan Port  Port     Portfast Port    Port
id         priority          vlanpri vlanpri-vlans
---- ----- -------- -------- ------- ----------------------------------------
769  1/1        32  disabled       0
769  1/2        32  disabled       0

Chan Port  IP       IPX      Group
id
---- ----- -------- -------- --------
769  1/1  on       auto-on  auto-on
769  1/2  on       auto-on  auto-on

Chan Port  GMRP     GMRP         GMRP
id         status   registration forwardAll
---- ----- -------- ------------ ----------
769  1/1  enabled  normal       disabled
769  1/2  enabled  normal       disabled

Chan Port  GVRP     GVRP          GVRP
id         status   registeration applicant
---- ----- -------- ------------- ---------
 769  1/1  disabled normal        normal
 769  1/2  disabled normal        normal

Chan Port  Qos-Tx Qos-Rx Qos-Trust    Qos-DefCos Qos-Port-based
id
---- ----- ------ ------ ------------ ---------- --------------
 769  1/1  2q2t   1q4t   untrusted             0 false
 769  1/2  2q2t   1q4t   untrusted             0 false

Chan Port  ACL name                         Protocol
id
---- ----- -------------------------------- --------
 769  1/1                                   IP
                                            IPX
                                            MAC
 769  1/2                                   IP
                                            IPX
                                            MAC
Console>
```

This example shows how to display port information for all channels:

```
Console> show channel info
Chan Port  Status     Channel   Admin Speed Duplex Vlan PortSecurity/
id                   mode      group                   Dynamic Port
---- ----- ---------- --------- ----- ------ ------ ---- -------------
 769  1/1  notconnect on          195 1000   full      1 -
 769  1/2  notconnect on          195 1000   full      1 -
 865  4/1  notconnect on          194 100    half      1 -
 865  4/2  notconnect on          194 100    half      1 -
```

```
Chan Port  if-   Oper-group Neighbor   Chan  Oper-Distribution
id         Index            Oper-group cost  Method
---- ----- ----- ---------- ---------- ----- -----------------
 769  1/1  -              1               0 ip both
 769  1/2  -              1               0 ip both
 865  4/1  -              1               0 ip both
 865  4/2  -              1               0 ip both

Chan Port  Device-ID                      Port-ID                   Platform
id
---- ----- ------------------------------ ------------------------ ----------
 769  1/1
 769  1/2
 865  4/1
 865  4/2

Chan Port  Trunk-status Trunk-type    Trunk-vlans
id
----- ----- ------------ ------------ ----------------------------------------
 769  1/1   not-trunking negotiate     1-1005
 769  1/2   not-trunking negotiate     1-1005
 865  4/1   not-trunking negotiate     1-1005
 865  4/2   not-trunking negotiate     1-1005

.
.
.
Console>
```

This example shows how to display PAgP information for all channels:

```
Console> show channel statistics
Port  Channel PAgP Pkts   PAgP Pkts PAgP Pkts PAgP Pkts PAgP Pkts PAgP Pkts
       id      Transmitted Received  InFlush   RetnFlush OutFlush  InError
----- ------- ----------- --------- --------- --------- --------- ---------
 2/1      768           0         0         0         0         0         0
 2/2      768           0         0         0         0         0         0
 4/3      769           0         0         0         0         0         0
 4/4      769           0         0         0         0         0         0
 4/7      770           0         0         0         0         0         0
 4/8      770           0         0         0         0         0         0
Console>
```

This example shows how to display PAgP information for a specific channel:

```
Console> show channel 768 statistics
Port  Channel PAgP Pkts   PAgP Pkts PAgP Pkts PAgP Pkts PAgP Pkts PAgP Pkts
       id      Transmitted Received  InFlush   RetnFlush OutFlush  InError
----- ------- ----------- --------- --------- --------- --------- ---------
 2/1      768           0         0         0         0         0         0
 2/2      768           0         0         0         0         0         0
Console>
```

This example shows how to display statistics for a specific channel:

```
Console> show channel 768 mac
Channel  Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast
-------- -------------------- -------------------- --------------------
768                      525                  959                  827

Channel  Xmit-Unicast         Xmit-Multicast       Xmit-Broadcast
-------- -------------------- -------------------- --------------------
768                      384                   88                    1
Port     Rcv-Octet            Xmit-Octet
-------- -------------------- --------------------
```

```
768                   469263               48083

Channel  Dely-Exced MTU-Exced  In-Discard Lrn-Discrd In-Lost    Out-Lost
-------- ---------- ---------- ---------- ---------- ---------- ----------
768               0          0          0          0          0          0
Console>
```

This example shows how to display statistics for all channels:

```
Console> show channel mac
Channel  Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast
 -------- -------------------- -------------------- --------------------
 768                   532290                  163                   6
 769                        0                    0                   0
 771                        4                   64                   0

 Channel  Xmit-Unicast         Xmit-Multicast       Xmit-Broadcast
 -------- -------------------- -------------------- --------------------
 768                   602591                   77                   3
 769                        0                    0                   0
 771                   636086                  222                  12

 Port     Rcv-Octet            Xmit-Octet
 -------- -------------------- --------------------
 768                  44873880             45102132
 769                        0                    0
 771                    64153             64831844

 Channel  Dely-Exced MTU-Exced  In-Discard Lrn-Discrd In-Lost    Out-Lost
 -------- ---------- ---------- ---------- ---------- ---------- ----------
 768               0          0          0          0          0          0
 769               0          0          0          0          0          0
 771               0         18          0          0          0          0
Last-Time-Cleared
--------------------------
Wed Jun 10 1999, 20:31:13
Console>
```

These examples show how to display feature-specific parameter information:

```
Console> show channel 769 info trunk
Chan Port  Trunk-status Trunk-type    Trunk-vlans
id
----- ----- ------------ ------------ ----------------------------------------
769  1/1  not-trunking negotiate     1-1005
769  1/2  not-trunking negotiate     1-1005

Chan Port  Portvlancost-vlans
id
---- ----- ------------------------------------------------------------------
769  1/1
769  1/2
Console>
Console> show channel 769 info spantree
Chan Port  Port     Portfast Port    Port
id         priority          vlanpri vlanpri-vlans
---- ----- -------- -------- ------- ----------------------------------------
769  1/1        32 disabled       0
769  1/2        32 disabled       0
Console>

Console> show channel 769 info protcol
Chan Port  IP       IPX      Group
id
```

```
---- ----- -------- -------- --------
769  1/1  on       auto-on  auto-on
769  1/2  on       auto-on  auto-on
Console>

Console> show channel 769 info gmrp
Chan Port  GMRP     GMRP         GMRP
id         status   registration forwardAll
---- ----- -------- ------------ ----------
769  1/1  enabled  normal       disabled
769  1/2  enabled  normal       disabled
Console>

Console> show channel 769 info gvrp
Chan Port  GVRP     GVRP          GVRP
id         status   registeration applicant
---- ----- -------- ------------- ---------
769  1/1  disabled normal       normal
769  1/2  disabled normal       normal
Console>

Console> show channel 769 info qos
Chan Port  Qos-Tx   Qos-Rx   Qos-Trust    Qos-DefCos Qos-Interface
id         PortType PortType Type                    Type
---- ----- -------- -------- ------------ ---------- --------------
769  1/1   2q2t     1q4t     untrusted             0 port-based
769  1/2   2q2t     1q4t     untrusted             0 port-based

Chan Port  ACL name                          Type
id
---- ----- -------------------------------- ----
769  1/1                                    IP
                                            IPX
                                            MAC
769  1/2                                    IP
                                            IPX
                                            MAC
Console>
```

Related Commands

- show channel group
- show port channel

show channel group

Use the **show channel group** command to display EtherChannel group status information.

show channel group [*admin_group*] [**info** | **statistics**]

show channel group [*admin_group*] [**info** [*type*]]

Syntax Description

admin_group	(Optional) Number of the administrative group; valid values are from 1 to 1024.
info	(Optional) Keyword to display group information.
statistics	(Optional) Keyword to display statistics about the group.
type	(Optional) Keyword to display feature-related parameters; valid values are **spantree**, **trunk**, **protcol**, **gmrp**, **gvrp**, **qos**, **rsvp, cops, dot1qtunnel, auxiliaryvlan**, and **jumbo**.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify *admin_group*, EtherChannel information is shown for all admin groups.

If you enter the optional **info** *type*, the specified feature-related parameters are displayed in the output.

Examples

This example shows how to display Ethernet channeling information for all admin groups:

```
Console> show channel group
Admin Group  Ports
-----------  ----------------------------------------------
7            1/1-2
Console>
```

This example shows how to display Ethernet channeling information for a specific group:

```
Console> show channel group 154
Admin Port  Status     Channel   Channel
group                  Mode      id
----- ----- ---------- --------- --------
  154  1/1  notconnect on             769
  154  1/2  connected  on             769
```

```
Admin Port  Device-ID                      Port-ID                  Platform
group
----- ----- ------------------------------ ------------------------ ----------
 154  1/1
  154  1/2    066510644(cat26-lnf(NET25))        2/1                      WS-C5505
Console>
```

This example shows how to display group information:

```
Console>  show channel group 154 info
Admin Port  Status     Channel   Ch    Speed Duplex Vlan PortSecurity/
group                  mode      id                     Dynamic Port
----- ----- ---------- --------- ----- ----- ------ ---- -------------
  154  1/1  notconnect on          769 1000  full      1 - Dynamic port
  154  1/2  connected  on          769 1000  full      1 - Dynamic port

Admin Port  if-   Oper-group Neighbor   Chan  Oper-Distribution
group       Index            Oper-group cost  Method
----- ----- ----- ---------- ---------- ----- -----------------
  154  1/1  -              1               0 mac both
  154  1/2  868            1               0 mac both

Admin Port  Device-ID                      Port-ID                  Platform
group
----- ----- ------------------------------ ------------------------ ----------
  154  1/1
  154  1/2  066510644(cat26-lnf(NET25))    2/1                      WS-C5505

Admin Port  Trunk-status Trunk-type    Trunk-vlans
group
----- ----- ------------ ------------ ----------------------------------------
  154  1/1  not-trunking negotiate    1-1005
  154  1/2  not-trunking negotiate    1-1005

Admin Port  Portvlancost-vlans
group
----- ----- ------------------------------------------------------------------
  154  1/1
  154  1/2

Admin Port  Port     Portfast Port    Port
group       priority          vlanpri vlanpri-vlans
----- ----- -------- -------- ------- ----------------------------------------
  154  1/1        32 disabled       0
  154  1/2        32 disabled       0

Admin Port  IP       IPX      Group
group
----- ----- -------- -------- --------
  154  1/1  on       auto-on  auto-on
  154  1/2  on       auto-on  auto-on

Admin Port  GMRP     GMRP         GMRP
group       status   registration forwardAll
----- ----- -------- ------------ ----------
  154  1/1  enabled  normal       disabled
  154  1/2  enabled  normal       disabled

Admin Port  GVRP     GVRP          GVRP
group       status   registeration applicant
----- ----- -------- ------------ ---------
  154  1/1  disabled normal       normal
  154  1/2  disabled normal       normal
```

```
Admin Port  Qos-Tx Qos-Rx Qos-Trust    Qos-DefCos Qos-Port-based
group
----- ----- ------ ------ ------------ ---------- --------------
  154  1/1  2q2t   1q4t   untrusted             0 false
  154  1/2  2q2t   1q4t   untrusted             0 false

Admin Port  ACL name                          Protocol
group
----- ----- -------------------------------- --------
  154  1/1  ip_acl                           IP
            ipx_acl                          IPX
            mac_acl                          MAC
  154  1/2                                   IP
                                             IPX
                                             MAC
Console>
```

These examples show how to display feature-specific parameter information:

```
Console> show channel group 154 info trunk
Admin Port  Trunk-status Trunk-type    Trunk-vlans
group
----- ----- ------------ ------------ ----------------------------------------
  154  1/1  not-trunking negotiate     1-1005
  154  1/2  not-trunking negotiate     1-1005
Console>

Console> show channel group 154 info spantree
Admin Port  Portvlancost-vlans
group
----- ----- ------------------------------------------------------------------
  154  1/1
  154  1/2

Admin Port  Port     Portfast Port    Port
group       priority          vlanpri vlanpri-vlans
----- ----- -------- -------- ------- ----------------------------------------
  154  1/1        32 disabled       0
  154  1/2        32 disabled       0
Console>

Console> show channel group 154 info protcol
Admin Port  IP       IPX      Group
group
----- ----- -------- -------- --------
  154  1/1  on       auto-on  auto-on
  154  1/2  on       auto-on  auto-on
Console>

Console> show channel group 154 info gmrp
Admin Port  GMRP     GMRP         GMRP
group       status   registration forwardAll
----- ----- -------- ------------ ----------
  154  1/1  enabled  normal       disabled
  154  1/2  enabled  normal       disabled
Console>
```

```
Console> show channel group 154 info gvrp
Admin Port  GVRP     GVRP          GVRP
group       status   registeration applicant
----- ----- -------- ------------ ---------
  154  1/1  disabled normal       normal
  154  1/2  disabled normal       normal
Console>

Console> show channel group 769 info qos
Chan Port  Qos-Tx   Qos-Rx   Qos-Trust    Qos-DefCos Qos-Interface
id         PortType PortType Type                   Type
---- ----- -------- -------- ------------ ---------- --------------
769  1/1  2q2t     1q4t     untrusted             0 port-based
769  1/2  2q2t     1q4t     untrusted             0 port-based

Chan Port  ACL name                          Type
id
---- ----- -------------------------------- ----
769  1/1                                    IP
                                            IPX
                                            MAC
769  1/2                                    IP
                                            IPX
                                            MAC
Console>
```

Related Commands show channel
show port channel

show channel hash

Use the **show channel hash** command to display the channel port the traffic goes to based on the current channel distribution mode.

show channel hash *channel_id src_ip_addr* [*dest_ip_addr*]

show channel hash *channel_id dest_ip_addr*

show channel hash *channel_id src_mac_addr* [*dest_mac_addr*]

show channel hash *channel_id dest_mac_addr*

show channel hash *channel_id src_port dest_port*

show channel hash *channel_id dest_port*

Syntax Description

channel_id	Number of the channel.
src_ip_addr	Source IP address.
dest_ip_addr	(Optional) Destination IP address.
src_mac_addr	Source MAC address.
dest_mac_addr	(Optional) Destination MAC address.
src_port	Number of the source port; valid values are from **0** to **65535**.
dest_port	Number of the destination port; valid values are from **0** to **65535**.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify *channel_id*, EtherChannel information is shown for all channels.

No information is displayed if the channel specified is not in use.

Examples

This example shows how to display hash information in a channel:

```
Console> show channel hash 769 10.6.1.1 10.6.2.3
Selected channel port:1/2
Console>
```

show channel mac

Use the **show channel mac** command to display MAC information in the channel.

show channel mac

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display MAC information in a channel:

```
Console> (enable) show channel mac
Channel  Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast
-------- -------------------- -------------------- --------------------

Channel  Xmit-Unicast         Xmit-Multicast       Xmit-Broadcast
-------- -------------------- -------------------- --------------------

Channel  Rcv-Octet            Xmit-Octet
-------- -------------------- --------------------

Channel  Dely-Exced MTU-Exced  In-Discard Lrn-Discrd In-Lost    Out-Lost
-------- ---------- ---------- ---------- ---------- ---------- ----------
```

show channelprotocol

Use the **show channelprotocol** command to display the channeling protocol used by each module in the system.

show channelprotocol

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

PAgP and LACP manage channels differently. When all the ports in a channel get disabled, PAgP removes them from its internal channels list; **show** commands do not display the channel. With LACP, when all the ports in a channel get disabled, LACP does not remove the channel; **show** commands continue to display the channel even though all its ports are down. To determine if a channel is actively sending and receiving traffic with LACP, use the **show port** command to see if the link is up or down.

LACP does not support half-duplex links. If a port is in active/passive mode and becomes half duplex, the port is suspended (and a syslog message is generated). The port is shown as "connected" using the **show port** command and as "not connected" using the **show spantree** command. This discrepancy is because the port is physically connected but never joined spanning tree. To get the port to join spanning tree, either set the duplex to full or set the channel mode to off for that port.

For more information about PAgP and LACP, refer to the "Guidelines for Port Configuration" section of the "Configuring EtherChannel" chapter of the *Catalyst 6000 Family Software Configuration Guide*.

Examples

This example shows how to display the protocol used by each module in the system:

```
Console> show channelprotocol
        Channel
Module  Protocol
------  --------
1       LACP
2       LACP
3       PAGP
4       LACP
Console>
```

Related Commands

set channelprotocol

show channel traffic

Use the **show channel traffic** command to display channel port utilization based on MAC counters.

show channel traffic [*channel_id*]

Syntax Description

channel_id	(Optional) Number of the channel.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify *channel_id*, EtherChannel information is shown for all channels.

No information is displayed if the channel specified is not in use.

Examples

This example shows how to display traffic information in a channel:

```
Console> show channel traffic 769
ChanId Port  Rx-Ucst Tx-Ucst Rx-Mcst Tx-Mcst Rx-Bcst Tx-Bcst
------ ----- ------- ------- ------- ------- ------- -------
   769  1/1    0.00%   0.00%   0.00%   0.00%   0.00%   0.00%
   769  1/2  100.00% 100.00% 100.00% 100.00%   0.00%   0.00%
Console>
```

show config

Use the **show config** command to display the nondefault system or module configuration.

show config [**all**]

show config [**system** | *mod*] [**all**]

show config acl location

Syntax Description

all	(Optional) Keyword to specify all module and system configuration information, including the IP address.
system	(Optional) Keyword to display system configuration.
mod	(Optional) Keyword to display module configuration.
acl location	Keyword to display ACL configuration file location.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

To view specific information within the **show config** output, if you enter /*text* and press the **Return** key at the --More-- prompt, the display starts two lines above the line containing the *text* string. If the text string is not found, "Pattern Not Found" is displayed. You can also enter "**n**" at the --More-- prompt to search for the last entered *text* string.

Examples

This example shows how to display the nondefault system and module configuration:

```
Console> (enable) show config
This command shows non-default configurations only.
Use 'show config all' to show both default and non-default configurations.
........
..

begin
!
# ***** NON-DEFAULT CONFIGURATION *****
!
!
#time: Mon Apr 17 2000, 08:33:09
!
#version 5.5(1)
#System Web Interface Version 5.0(0.25)
!
set editing disable
```

```
!
#frame distribution method
set port channel all distribution mac unknown
!
#snmp
set snmp trap 0.0.0.0
set snmp trap 0.0.0.0
!
#kerberos
set kerberos server  0.0.0.0
set kerberos server  0.0.0.0
set kerberos realm
set kerberos realm
!
#vtp
set vtp domain Lab_Network
set vtp v2 enable
set vtp pruning enable
set vlan 1 name default type ethernet mtu 1500 said 100001 state active
set vlan 2 name VLAN0002 type ethernet mtu 1500 said 100002 state active
set vlan 6 name VLAN0006 type ethernet mtu 1500 said 100006 state active
set vlan 10 name VLAN0010 type ethernet mtu 1500 said 100010 state active
set vlan 20 name VLAN0020 type ethernet mtu 1500 said 100020 state active
set vlan 50 name VLAN0050 type ethernet mtu 1500 said 100050 state active
set vlan 100 name VLAN0100 type ethernet mtu 1500 said 100100 state active
set vlan 152 name VLAN0152 type ethernet mtu 1500 said 100152 state active
set vlan 200 name VLAN0200 type ethernet mtu 1500 said 100200 state active
set vlan 300 name VLAN0300 type ethernet mtu 1500 said 100300 state active
set vlan 303 name VLAN0303 type fddi mtu 1500 said 100303 state active
set vlan 400 name VLAN0400 type ethernet mtu 1500 said 100400 state active
set vlan 500 name VLAN0500 type ethernet mtu 1500 said 100500 state active
set vlan 521 name VLAN0521 type ethernet mtu 1500 said 100521 state active
set vlan 524 name VLAN0524 type ethernet mtu 1500 said 100524 state active
set vlan 570 name VLAN0570 type ethernet mtu 1500 said 100570 state active
set vlan 801 name VLAN0801 type trbrf mtu 4472 said 100801 state active bridge
set vlan 850 name VLAN0850 type ethernet mtu 1500 said 100850 state active
set vlan 917 name VLAN0917 type ethernet mtu 1500 said 100917 state active
set vlan 999 name VLAN0999 type ethernet mtu 1500 said 100999 state active
set vlan 1002 name fddi-default type fddi mtu 1500 said 101002 state active
set vlan 1004 name fddinet-default type fddinet mtu 1500 said 101004 state acti
set vlan 1005 name trbrf-default type trbrf mtu 4472 said 101005 state active b
set vlan 802 name VLAN0802 type trcrf mtu 4472 said 100802 state active parent
set vlan 1003 name trcrf-default type trcrf mtu 4472 said 101003 state active p
set vlan 3 translation 303 translation 0
set vlan 4 translation 304 translation 0
set vlan 5 translation 305 translation 0
set vlan 303 translation 3 translation 0
set vlan 304 translation 4 translation 0
set vlan 305 translation 5 translation 0
set vlan 351 translation 524 translation 0
set vlan 524 translation 351 translation 0
!
#ip
set interface sc0 1 1.10.11.212/255.255.255.0 1.10.11.255

set ip route 0.0.0.0/0.0.0.0         172.20.52.126
set ip route 0.0.0.0/0.0.0.0         172.20.52.125
set ip route 0.0.0.0/0.0.0.0         172.20.52.121
!
```

```
#rcp
set rcp username 1
!
#dns
set ip dns server 171.68.10.70 primary
set ip dns server 171.68.10.140
set ip dns enable
set ip dns domain cisco.com
!
#spantree
set spantree fwddelay 4     801
set spantree maxage   10    801
#portfast
set spantree portfast bpdu-guard enable
#vlan 802
set spantree fwddelay 4     802
set spantree maxage   10    802
set spantree portstate 802 block 801
#vlan 1003
set spantree fwddelay 4     1003
set spantree maxage   10    1003
set spantree portstate 1003 block 1005
!
#syslog
set logging server 172.20.101.182
!
#set boot command
set boot config-register 0x100
set boot system flash bootflash:cat6000-sup.5-5-1.bin
!
#HTTP commands
set ip http server enable
set ip http port 1922
!
# default port status is disable
!
#mls
set mls nde disable
!
#qos
set qos enable
set qos map 1q4t 1 1 cos 2
set qos map 1q4t 1 1 cos 3
set qos map 1q4t 1 1 cos 4
set qos map 1q4t 1 1 cos 5
set qos map 1q4t 1 1 cos 6
set qos map 1q4t 1 1 cos 7
!
#Accounting
set accounting commands enable config stop-only tacacs+
!
# default port status is enable
!
#module 1 : 2-port 1000BaseX Supervisor
!
#module 2 empty
!
#module 3 : 48-port 10/100BaseTX (RJ-45)
set spantree portfast   3/8 enable
!
```

```
#module 4 empty
!
#module 5 : 48-port 10/100BaseTX (RJ-45)
!
#module 6 empty
!
set vlan 100  6/1
set spantree portcost    6/1  200
!
#module 7 : 24-port 10/100BaseTX Ethernet
set vlan 5    7/5
set vlan 100  7/23
set vlan 200  7/9
set port disable    7/5

set port name       7/9  1528 Hub
set port security 7/10 enable
set port security 7/10 maximum 200
set port security 7/10 00-11-22-33-44-55
set port security 7/10 00-11-22-33-44-66
set port security 7/10 00-11-22-33-44-77
set port security 7/10 violation restrict
set port security 7/10 age 30
set trunk 7/1  desirable isl 1-1005
set trunk 7/2  desirable isl 1-1005
set trunk 7/3  desirable isl 1-1005
set trunk 7/4  desirable isl 1-1005
set trunk 7/10 off negotiate 1-1005
set trunk 7/23 on isl 1-1005
set spantree portcost    7/23  150
set spantree portvlancost 7/23 cost 50 100
!
#module 8 empty
!
#module 9 empty
!
#module 15 empty
!
#module 16 empty
end
Console>
```

This example shows how to display default and nondefault configuration information:

```
Console> (enable) show config all
begin
!
# ***** ALL (DEFAULT and NON-DEFAULT) CONFIGURATION *****
!
#Current time: Mon Apr 17 2000, 08:33:09
!
#version 5.51(1)
!
set password $1$FMFQ$HfZR5DUszVHIRhrz4h6V70
set enablepass $1$FMFQ$HfZR5DUszVHIRhrz4h6V70
set prompt Console>
set length 24 default
set logout 20
set banner motd ^C^C
!
```

```
#system
set system baud  9600
set system modem disable
set system name
set system location
set system contact
!
.
.
.
Console>
```

This example shows how to display nondefault system configuration information:

```
Console> (enable) show config system
begin
!
# ***** NON-DEFAULT CONFIGURATION *****
!
#time: Mon Apr 17 2000, 08:33:09
!
#version 5.5(1)
!
!
#set boot command
set boot config-register 0x2
set boot system flash bootflash:kk1
end
Console>
```

This example shows how to display all system default and nondefault configuration information:

```
Console> (enable) show config system all
begin
!
#system
set system baud  9600
set system modem disable
set system name
set system location
set system contact
!
end
Console>
```

This example shows how to display module nondefault configuration information:

```
Console> (enable) show config 1
..............
begin
!
# ***** NON-DEFAULT CONFIGURATION *****
!
!
#time: Mon Apr 17 2000, 08:33:09
!
#version 5.5(1)
!
!
#module 1 : 4-port 10/100BaseTX Supervisor
!
end
Console>
```

This example shows how to display the ACL configuration file location:

```
Console> (enable) show config acl location
ACL configuration is being saved in NVRAM.
Console> (enable)
```

Related Commands clear config
write

show config mode

Use the **show config mode** command to display the system configuration mode currently running on the switch.

show config mode

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to display the current system configuration mode when set to text:

```
Console> (enable) show config mode
System configuration mode set to text.
System configuration file = bootflash:switch.cfg
Console> (enable)
```

This example shows how to display the current system configuration mode when set to binary:

```
Console> (enable) show config mode
System configuration mode set to binary.
Console> (enable)
```

Related Commands

set config mode

show config qos acl

Use the **show config qos acl** command to display the committed access lists in a command line format.

show config qos acl {*acl_name* | **all**}

Syntax Description

acl_name	Unique name that identifies the list to which the entry belongs.
all	Keyword to specify all committed access lists.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display all committed access lists:

```
Console> show config qos acl all
#ipx1:
set qos acl ipx ipx1 dscp 1 any AA BB
set qos acl ipx ipx1 dscp 1 0 AA CC
#default-action:
set qos acl default-action ip dscp 0
set qos acl default-action ipx dscp 0
set qos acl default-action mac dscp 0
Console>
```

This example shows how to display a specific committed access list:

```
Console> show config qos acl my_ip_acl
#my_ip_acl:
set qos acl ip my_ip_acl trust-dscp microflow my-micro tcp 1.2.3.4/255.0.0.0 eq
port 21 172.20.20.1/255.255.255.0 tos 5
set qos acl ip my_ip_acl trust-dscp microflow my-micro aggregate agg tcp
173.22.3.4/255.0.0.0 eq port 19 173.22.20.1/255.255.255.0 tos 5
Console>
```

Related Commands

commit

show cops

Use the **show cops** command to display COPS information.

show cops info [**diff-serv** | **rsvp**] [**noalias**]

show cops roles

Syntax Description

info	Keyword to display COPS status and configuration information.
diff-serv	(Optional) Keyword to specify the differentiated services server table.
rsvp	(Optional) Keyword to specify the RSVP server table.
noalias	(Optional) Keyword to force the display to show only IP addresses, not IP aliases.
roles	Keyword to display the ports assigned to each role.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

A few minutes after a switchover occurs between active and redundant supervisor engines, if you enter the **show cops roles** command, the output may be incorrect. If this is the case, the following warning displays:

```
COPS High Availability Switch Over in progress, hardware may be
programmed differently than as suggested by the output of these
commands.
```

Examples

This example shows how to display COPS status and configuration information:

```
Console> show cops info
COPS general configuration
---------------------------
COPS domain name            : -
Connection retry intervals  : initial   = 30 seconds
                              increment = 30 seconds
                              max       = 300 seconds
COPS Diff-Serv client state
---------------------------
COPS connection state       :not-connected
Last active server          :172.20.25.3 [port:3288]
Primary configured server   :172.20.25.3 [port:3288]
Secondary configured server :-
COPS RSVP client state
-----------------------
```

```
COPS connection state       : connected
Last active server          : 171.21.34.56
Primary configured server   : 171.21.34.56 [3288]
Secondary configured server : 171.21.34.57 [3288]
Console>
```

This example shows how to display COPS RSVP status and configuration information:

```
Console> show cops info rsvp
COPS general configuration
--------------------------
COPS domain name            : -
Connection retry intervals  : initial   = 30 seconds
                              increment = 30 seconds
                              max       = 300 seconds

COPS RSVP client state
----------------------
COPS connection state       : connected
Last active server          : 171.21.34.56
Primary configured server   : 171.21.34.56 [3288]
Secondary configured server : 171.21.34.57 [3288]
Console>
```

This example shows how to display the ports assigned to each role:

```
Console> show cops roles
Admin Roles                    Mod/Ports
------------------------------ ----------------------------------------
access_port                    1/1-2,3/1-5,3/8
backbone_port                  1/1-2,3/8
branch_office_port             3/6-7,4/1-8
net_port                       -

Oper Roles                     Mod/Ports
------------------------------ ----------------------------------------
access_port                    1/1-2,3/1-5,3/8
backbone_port                  1/1-2,3/8
branch_office_port             3/6-7,4/1-8
Console>
```

This example shows how to display only IP addresses, not IP aliases:

```
Console> show cops noalias
COPS general configuration
--------------------------
COPS domain name            : -
Connection retry intervals  : initial   = 30 seconds
                              increment = 30 seconds
                              max       = 300 seconds

COPS Diff-Serv client state
---------------------------
COPS connection state       : not-connected
TCP  connection state       : not-connected
Last active server          : -
Primary configured server   : -
Secondary configured server : -
```

```
COPS RSVP client state
----------------------
COPS connection state       : not-connected
TCP  connection state       : not-connected
Last active server          : -
Primary configured server   : -
Secondary configured server : -
Console>
```

Related Commands

clear cops
set cops

show counters

Use the **show counters** command to display hardware counters for a port, all ports on a module, or a supervisor engine.

show counters {*mod* | *mod*/*port*}

show counters supervisor

Syntax Description

mod	Number of the module.
mod/port	Number of the module and the port.
supervisor	Keyword to display counters for the supervisor engine.

Defaults

This command has no default setting.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The "Last-Time-Cleared" timestamp at the end of the **show counters** {*mod* | *mod*/*port*} command output is either the last time the counters were cleared on the specified port or the last time that the module was inserted or the switch was reset, whichever happened last.

Examples

This example shows how to display the counters for module 2, port 1:

Note The counters displayed may change depending on the module type queried.

```
Console> show counters 2/1
Generic counters version 1
64 bit counters
0  rxHCTotalPkts                    =            2170558
1  txHCTotalPkts                    =            2588911
2  rxHCUnicastPkts                  =            2142669
3  txHCUnicastPkts                  =            2585457
4  rxHCMulticastPkts                =              19552
5  txHCMulticastPkts                =               1789
6  rxHCBroadcastPkts                =               8332
7  txHCBroadcastPkts                =               1665
8  rxHCOctets                       =          190513843
9  txHCOctets                       =          227423299
10 rxTxHCPkts64Octets               =              20996
11 rxTxHCPkts65to127Octets          =            4737279
12 rxTxHCPkts128to255Octets         =               1170
13 rxTxHCPkts256to511Octets         =                 16
14 rxTxHCpkts512to1023Octets        =                  8
```

```
15 rxTxHCpkts1024to1518Octets         =                   0
16 rxDropEvents                       =                   0
32 bit counters
0  rxCRCAlignErrors                   =          0
1  rxUndersizedPkts                   =          0
2  rxOversizedPkts                    =          0
3  rxFragmentPkts                     =          0
4  rxJabbers                          =          0
5  txCollisions                       =          0
6  ifInErrors                         =          0
7  ifOutErrors                        =          0
8  ifInDiscards                       =          0
9  ifInUnknownProtos                  =          0
10 ifOutDiscards                      =          0
11 txDelayExceededDiscards            =          0
12 txCRC                              =          0
13 linkChange                         =          2
Dot3 counters version 1
0  dot3StatsAlignmentErrors           =          0
1  dot3StatsFCSErrors                 =          0
2  dot3StatsSingleColFrames           =          0
3  dot3StatsMultiColFrames            =          0
4  dot3StatsSQETestErrors             =          0
5  dot3StatsDeferredTransmisions      =          0
6  dot3StatsLateCollisions            =          0
7  dot3StatsExcessiveCollisions       =          0
8  dot3StatsInternalMacTransmitErrors =          0
9  dot3StatsCarrierSenseErrors        =          0
10 dot3StatsFrameTooLongs             =          0
11 dot3StatsInternalMacReceiveErrors  =          0
Flowcontrol counters version 1
0  txPause                            =          0
1  rxPause                            =          0
Last-Time-Cleared
--------------------------
Tue Mar 21 2000, 19:19:03
Console>
```

This example shows how to display the counters for the supervisor engine:

```
Console> show counters supervisor
Acl Manager Error Stats Counter(s)
====================================
IP checksum errors   = 00000

Forwarding Engine Error Stats Counters
====================================
IP length errors     = 0
IP too short errors  = 0
IP checksum errors   = 0
IPX length errors    = 0
IPX too short errors = 0
Console>
```

Table 2-28 describes the possible fields in the **show counters** command output.

Table 2-28 show counters Command Output Fields

Field	Description
64-bit counters	
rxHCTotalPkts	Number of packets (including bad packets, broadcast packets, and multicast packets) received on a link.
txHCTotalPkts	Number of packets (including bad packets, broadcast packets, and multicast packets) transmitted on a link.
rxHCUnicastPkts	Number of packets, delivered by this sublayer to a higher (sub)layer, which were not addressed to a multicast or broadcast address at this sublayer.
txHCUnicastPkts	Number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sublayer, including those that were discarded or not sent.
rxHCMulticastPkts	Number of packets, delivered by this sublayer to a higher (sub)layer, which were addressed to a multicast address at this sublayer. For a MAC layer protocol, this includes both Group and Functional addresses.
txHCMulticastPkts	Number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sublayer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses.
rxHCBroadcastPkts	Number of packets, delivered by this sublayer to a higher (sub)layer, which were addressed to a broadcast address at this sublayer.
txHCBroadcastPkts	Number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sublayer, including those that were discarded or not sent.
rxHCOctets	Number of octets received on the interface, including framing characters.
txHCOctets	Number of octets transmitted out of the interface, including framing characters.
rxTxHCPkts64Octets	Number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
rxTxHCPkts65to127Octets	Number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
rxTxHCPkts128to255Octets	Number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
rxTxHCPkts256to511Octets	Number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
rxTxHCpkts512to1023Octets	Number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
rxTxHCpkts1024to1518Octets	Number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
rxDropEvents[1]	Number of events in which packets were dropped by the probe due to lack of resources.
32-bit counters	
rxCRCAlignErrors	Number of packets received that had a length (excluding framing bits, but including FCS octets) between 64 and 1518 octets, inclusive, and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

Table 2-28 show counters Command Output Fields (continued)

Field	Description
rxUndersizedPkts	Number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well-formed.
rxOversizedPkts	Number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well-formed.
rxFragmentPkts[2]	Number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
rxJabbers[3]	Number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
txCollisions[4]	The best estimate of the total number of collisions on this Ethernet segment. The value returned will depend on the location of the RMON probe. Section 8.2.1.3 (10Base5) and section 10.3.1.3 (10Base2) of IEEE standard 802.3 states that a station must detect a collision in the receive mode if three or more stations are transmitting simultaneously. A repeater port must detect a collision when two or more stations are transmitting simultaneously. Thus, a probe placed on a repeater port could record more collisions than a probe connected to a station on the same segment would. Probe location plays a much smaller role when considering 10BaseT.
ifInErrors	For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol.
ifOutErrors	Number of octets transmitted out of the interface, including framing characters.
ifInDiscards	Number of inbound packets that were chosen to be discarded even though no errors had been detected to prevent their delivery to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
ifInUnknownProtos	Number of inbound packets with unknown protocols.
ifOutDiscards	Number of inbound packets chosen to be discarded even though no errors had been detected to prevent their delivery to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
txDelayExceededDiscards	Number of frames discarded by this port due to excessive transmit delay.
txCRC	Number of CRC errors.
linkChange	Number of times the port toggled between a connect state to a non-connect state.
Dot3 counters version 1	
dot3StatsAlignmentErrors[5]	A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check.
dot3StatsFCSErrors[6]	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check.
dot3StatsSingleColFrames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the dot3StatsMultipleCollisionFrames object.

Table 2-28 show counters Command Output Fields (continued)

Field	Description
dot3Stats MultiColFrames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the dot3StatsSingleCollisionFrames object.
dot3StatsSQETestErrors	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface. The SQE TEST ERROR message is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985 and its generation is described in section 7.2.4.6 of the same document.
dot3StatsDeferredTransmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions.
dot3StatsLateCollisions[7]	Number of times that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet.
dot3StatsExcessiveCollisions	A count of frames for which transmission on a particular interface fails due to excessive collisions.
dot3StatsInternalMacTransmitErrors[8]	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsLateCollisions object, the dot3StatsExcessiveCollisions object, or the dot3StatsCarrierSenseErrors object.
dot3StatsCarrierSenseErrors	Number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface. The count represented by an instance of this object is incremented at most once per transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt.
dot3StatsFrameTooLongs	A count of frames received on a particular interface that exceeds the maximum permitted frame size. The count represented by an instance of this object is incremented when the frameTooLong status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtained are counted exclusively according to the error status presented to the LLC.
dot3StatsInternalMacReceiveErrors[9]	A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsFrameTooLongs object, the dot3StatsAlignmentErrors object, or the dot3StatsFCSErrors object.
Flowcontrol counters version 1	
txPause	Number of control frames transmitted at the gigabit level. This counter is valid only on a Gigabit Ethernet port.
rxPause	Number of control frames received at the gigabit level. This counter is valid only on a Gigabit Ethernet port.

1. This number is not necessarily the number of packets dropped; it is just the number of times this condition has been detected.
2. It is entirely normal for etherStatsFragments to increment because it counts both runts (which are normal occurrences due to collisions) and noise hits.
3. This definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2), which define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
4. An RMON probe inside a repeater should ideally report collisions between the repeater and one or more other hosts (transmit collisions as defined by IEEE 802.3k) plus receiver collisions observed on any coax segments to which the repeater is connected.
5. This number is incremented when the alignmentError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtained are counted exclusively according to the error status presented to the LLC.

6. This number is incremented when the frameCheckError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtained are counted exclusively according to the error status presented to the LLC.
7. 512 bit-times corresponds to 51.2 microseconds on a 10-Mbps system. A (late) collision represented by an instance of this object is also considered as a (generic) collision for other collision-related statistics.
8. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of transmission errors on a particular interface not otherwise counted.
9. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of receive errors on a particular interface not otherwise counted.

Related Commands

clear counters

show crypto key

Use the **show crypto key** command to display RSA key pair information.

show crypto key

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The **crypto** commands are supported on systems that run these image types only:

- supk9 image—for example, cat6000-supk9.6-1-3.bin
- supcvk9 image—for example, cat6000-supcvk9.6-1-3.bin

Examples

This example shows how to display key pair information:

```
Console> (enable) show crypto key
RSA keys was generated at: Tue Dec 14 1999, 14:22:48
1024 37 11205183948399013011667148538409950947450374566823948912494417799515437271871599996436830339109643861793422720443713266686928948984984257053159297897246076921045354720103938686487836695793386604820940927205149512376570286088608321628093701730900686518705893502418540282606318597410241155889469702560715486842 1
Console> (enable)
```

Related Commands

clear crypto key rsa
set crypto key rsa

show default

Use the **show default** command to check the status of the default port status setting.

show default

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The command shows whether the **set default portstatus** command is in disable or enable mode.

Examples

This example shows how to display the status of the default port status:

```
Console> (enable) show default
portstatus: disable
Console> (enable)
```

Related Commands

set default portstatus

show dot1q-all-tagged

Use the **show dot1q-all-tagged** command to display the dot1q tagging status.

show dot1q-all-tagged

Syntax Description This command has no keywords or arguments.

Defaults This command has no default settings.

Command Types Switch command.

Command Modes Privileged.

Examples This example shows how to display dot1q tagging status:

```
Console> (enable) show dot1q-all-tagged
Dot1q all tagged mode disabled
Console> (enable)
```

Related Commands **set dot1q-all-tagged**

show dot1x

Use the **show dot1x** command to display the system dot1x capabilities, protocol version, and timer values.

show dot1x

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the dot1x information for the system:

```
Console> show dot1x
PAE Capability             Authenticator Only
Protocol Version           1
system-auth-control        enabled
max-req                    2
quiet-period               60 seconds
re-authperiod              3600 seconds
server-timeout             30 seconds
supp-timeout               30 seconds
tx-period                  30 seconds

Console>
```

Related Commands

clear dot1x config
set dot1x

show dvlan statistics

Use the **show dvlan statistics** command to display dynamic VLAN statistics.

show dvlan statistics

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to display dynamic VLAN statistics:

```
Console> show dvlan statistics
VMPS Client Statistics
----------------------
VQP Queries:               0
VQP Responses:             0
Vmps Changes:              0
VQP Shutdowns:             0
VQP Denied:                0
VQP Wrong Domain:          0
VQP Wrong Version:         0
VQP Insufficient Resource: 0
Console>
```

Related Commands

reconfirm vmps

show environment

Use the **show environment** command to display environmental, temperature, and inline power status information.

show environment [**all** | **temperature** | {**power** [*mod*]}]

Syntax Description

all	(Optional) Keyword to display environmental status information (for example, power supply, fan status, and temperature information) and information about the power available to the system.
temperature	(Optional) Keyword to display temperature information.
power	(Optional) Keyword to display inline power status.
mod	(Optional) Number of the module to display inline power status

Defaults

If you do not enter a keyword, environmental status information (for example, power supply, fan status, and temperature information) only is displayed.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The **temperature** option is not supported by the NAM.

In the output of the **show environment all** command, environmental status and temperature information for the NAM module is not supported.

In the output of the **show environment temperature** and **show environment all** commands, you will notice three slot 1 displays. The first slot 1 is the actual supervisor engine. The second slot 1 is the switching engine, which is on the supervisor engine (slot 1) and has its own Intake, Exhaust, Device 1, and Device 2 temperature outputs. The third slot 1 is the MSFC, which is also on the supervisor engine, and has its own Intake, Exhaust, Device 1, and Device 2 temperature outputs.

If you see a partial-deny card status, this is an indication that some module ports are inline powered but not all the ports on the module are inline powered.

Examples

This example shows how to display environmental status information:

```
Console> show environment
Environmental Status (. = Pass, F = Fail, U = Unknown, N = Not Present)
  PS1:.     PS2:N     PS1 Fan:.     PS2 Fan:N
  Chassis-Ser-EEPROM:.     Fan:.
  Clock(A/B):A         Clock A:.     Clock B:.
  VTT1:.    VTT2:.    VTT3:.
Console>
```

This example shows how to display environmental status information and details about the power available to the system:

```
Console> show environment all
Environmental Status (. = Pass, F = Fail, U = Unknown, N = Not Present)
  PS1: .     PS2: N     PS1 Fan: .     PS2 Fan: N
  Chassis-Ser-EEPROM: .     Fan: .
  Clock(A/B): A         Clock A: .     Clock B: .
  VTT1: .    VTT2: .    VTT3: .

                  Intake        Exhaust       Device 1     Device 2
Slot             Temperature   Temperature   Temperature   Temperature
---------------  ------------  ------------  ------------  ------------
1                24C(50C,65C)  32C(60C,75C)  27C           32C
3                N/A           N/A           N/A           N/A
5                22C(50C,65C)  27C(60C,75C)  28C           28C
1  (Switch-Eng)  22C(50C,65C)  22C(60C,75C)  N/A           N/A
1  (MSFC)        26C(50C,65C)  30C(60C,75C)  N/A           N/A

Chassis Modules
------------------
VTT1: 25C(85C,100C)
VTT2: 24C(85C,100C)
VTT3: 25C(85C,100C)

PS1 Capacity: 1153.32 Watts (27.46 Amps @42V)
PS2 Capacity: none
PS Configuration : PS1 and PS2 in Redundant Configuration.
Total Power Available: 1153.32 Watts (27.46 Amps @42V)
Total Power Available for Line Card Usage: 1153.32 Watts (27.46 Amps @42V)
Total Power Drawn From the System: 453.18 Watts (10.79 Amps @42V)
Remaining Power in the System: 700.14 Watts (16.67 Amps @42V)
Default Inline Power allocation per port: 2.00 Watts (0.04 Amps @42V)

Slot power Requirement/Usage :

Slot Card Type           PowerRequested PowerAllocated CardStatus
                         Watts   A @42V Watts   A @42V
---- ------------------- ------- ------ ------- ------ ----------
1    WS-X6K-SUP1A-2GE    138.60   3.30  138.60   3.30  ok
2                          0.00   0.00  138.60   3.30  none
3    WS-X6380-NAM         63.00   1.50   63.00   1.50  ok
5    WS-X6248-RJ-45      112.98   2.69  112.98   2.69  ok
Console>
```

This example shows how to display temperature information:

```
Console> show environment temperature
                  Intake        Exhaust       Device 1     Device 2
Slot             Temperature   Temperature   Temperature   Temperature
---------------  ------------  ------------  ------------  ------------
1                25C(50C,65C)  34C(60C,75C)  27C           32C
3                N/A           N/A           N/A           N/A
5                24C(50C,65C)  27C(60C,75C)  28C           29C
1  (Switch-Eng)  22C(50C,65C)  22C(60C,75C)  N/A           N/A
1  (MSFC)        28C(50C,65C)  32C(60C,75C)  N/A           N/A

Chassis Modules
------------------
VTT1: 25C(85C,100C)
VTT2: 25C(85C,100C)
VTT3: 25C(85C,100C)
Console> (enable)
```

This example shows how to display the inline power for all modules:

```
Console> show environment power
PS1 Capacity: 1153.32 Watts (27.46 Amps @ 42V)
PS2 Capacity: none
PS Configuration : PS1 and PS2 in Redundant Configuration.
Total Power Available: 1153.32 Watts (27.46 Amps @ 42V)
Total Power Available for Line Card Usage: 1153.32 Watts (27.46 Amps @ 42V)
Total Power Drawn From the System: 289.80 Watts (6.90 Amps @ 42V)
Remaining Power in the System: 863.52 Watts (20.56 Amps @42V)
Default inline power allocation: 10.5 Watts/port (0.25 Amps @ 42V)

Slot power Requirement/Usage :

Slot  Card-Type            Power-Requested  Power-Allocated  Card-Status
                           Watts   A @ 42V  Watts   A @ 42V
----  -------------------  ------- -------  ------- -------  ------------
1                          0.00    0.00     126.42  3.01     none
2     WS-X6K-SUP1-2GE      138.60  3.30     138.60  3.30     ok
3     WS-X6348-RJ-45       114.24  2.72     151.20  3.60     ok
5     WS-X6348-RJ-45       109.20  2.60     100.88  2.40     partial-deny
Console>
```

This example shows how to display the inline power status for a specific module:

```
Console> show environment power 9
Module 9:
Default Inline Power allocation per port: 9.500 Watts (0.22 Amps @42V)
Total inline power drawn by module 9: 0 Watt

Slot power Requirement/Usage :

Slot Card Type           PowerRequested PowerAllocated CardStatus
                         Watts   A @42V Watts   A @42V
---- ------------------- ------- ------ ------- ------ ----------
9    WS-X6348            123.06   2.93  123.06   2.93  ok

Default Inline Power allocation per port: 9.500 Watts (0.22 Amps @42V)
Port      InlinePowered     PowerAllocated
      Admin Oper   Detected mWatt mA @42V
----- ----- ------ -------- ----- --------
 9/1  auto  off    no       0     0
 9/2  auto  off    no       0     0
 9/3  auto  off    no       0     0
 9/4  auto  off    no       0     0
 9/5  auto  off    no       0     0
.
.
.
Console>
```

Table 2-29 describes the fields in the **show environment** output.

Table 2-29 show environment Command Output Fields

Field	Description
Environmental Status[1]	
PS1: and PS2:	Power supply status.
PS1 Fan: and PS2 Fan:	Power supply fan status.
Chassis-Ser-EEPROM:	Chassis serial EEPROM status.

Table 2-29 show environment Command Output Fields (continued)

Field	Description
Fan:	Fan status.
Clock A: and Clock B:	Clock A and B status.
VTT1:, VTT2:, and VTT3:	VTT module status. VTT modules are power monitors for the chassis backplane. A minor system alarm is signalled when one of the three VTTs fails, and a major alarm is signalled when two or more VTTs fail.
Intake Temperature and Exhaust Temperature	Temperature of the air flow as it enters, goes over the modules, and exits the chassis. The current temperature is listed first, with the minor and major alarm temperatures listed in parentheses.
Device 1 Temperature and Device 2 Temperature	The devices are additional temperature sensors measuring the internal temperature on each module indicated. The current temperature is listed first, with the warning and critical alarm temperatures listed in parentheses.
Chassis Modules	
VTT1:, VTT2:, and VTT3:	Temperature of the VTT modules. The current temperature is listed first, with the minor and major alarm temperature settings listed in parentheses.
PS1 Capacity: and PS2 Capacity:	Power supply capacity.
PS Configuration:	Power supply configuration.
Total Power Available:	Total available power.
Total Power Available for Line Card Usage:	Total power available for module use.
Total Power Drawn From the System:	Total power drawn from the system.
Remaining Power in the System:	Remaining power in the system.
Default Inline Power allocation per port:	Default inline power allocation per port.
Slot power Requirement/Usage	
Power Requested	Module power requested.
Power Allocated	Module power allocation.
Card Status	Module status (no, ok, partial-deny[2], unknown, power-bad, and power-deny).
Total inline power drawn	Total inline power drawn from the system.
InlinePowered—Admin	Inline power management status—auto, on, and off.
InlinePowered—Oper	Inline power status—on indicates power is being supplied by that port, off indicates power is not being supplied by the port, denied indicates there is not have enough power available to provide to the port.
InlinePowered—Detected	Status of whether inline power is detected.

1. Environmental status indications are the following: . = Pass, F = Fail, U = Unknown, and N = Not Present.
2. The partial-deny state indicates that some ports but not all ports in the module are inline powered.

Related Commands

set inlinepower defaultallocation
show environment
show port inlinepower

show errdisable-timeout

Use the **show errdisable-timeout** command to display the errdisable timeout configuration and status.

show errdisable-timeout

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If your system is configured with a Supervisor Engine 2, the crossbar-fallback error may be displayed in the ErrDisable Reason field.

Examples

This example shows how to display the errdisable timeout configuration and status:

```
Console> (enable) show errdisable-timeout
ErrDisable Reason   Timeout Status
------------------- ------------
bpdu-guard          Enable
channel-misconfig   Disable
duplex-mismatch     Enable
udld                Enable
other               Disable

Interval: 300 seconds

Ports that will be enabled at the next timeout:
Port  ErrDisable Reason
----- -----------------
 3/1  udld
 3/8  bpdu-guard
 6/5  udld
 7/24 duplex-mismatch
Console> (enable)
```

Related Commands

set errdisable-timeout

show errordetection

Use the **show errordetection** command to display error detection settings.

show errordetection

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to display the error detection settings:

```
Console> (enable) show errordetection
Inband error detection:          disabled
Memory error detection:          enabled
Port counter error detection:    enabled
Console> (enable)
```

Related Commands

set errordetection

show fabric channel

Use the **show fabric channel** command to display Switch Fabric Module information.

show fabric channel counters [*mod*]

show fabric channel utilization

show fabric channel switchmode [*mod*]

Syntax Description

counters	Keyword to display fabric channel counter information.
mod	(Optional) Number of the Switch Fabric Module.
utilization	Keyword to display fabric channel utilization information.
switchmode	Keyword to display switch mode and fabric channel status.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

These commands are supported on systems configured with a Switch Fabric Module and the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) only.

In the **show fabric channel switchmode** command output, the Fab Chan field displays the module channel number and the correspondent fabric channel number in pairs. The first number is the fabric channel number associated with the module (valid value is 0) and the second number is the fabric channel number to the Catalyst 6500 series Switch Fabric Module (valid values are 0 to 17).

For the Switch Fabric Module, the Switch Mode and Channel Status fields will show “n/a.”

In the **show fabric channel switchmode** command output, the Switch Mode field displays one of the following modes:

- Flow-through mode—In this mode, data passes between the local bus and the supervisor engine bus.
- Truncated mode—In this mode, the truncated data is sent over the switch fabric channel if both the destination and the source modules are fabric-enabled modules. If either the source or destination module is not a fabric-enable module, the data goes through the switch fabric channel and the data bus. The Switch Fabric Module does not get involved when traffic is forwarded between nonfabric-enabled modules.
- Compact mode—In this mode, a compact version of the DBus header is forwarded over the switch fabric channel, delivering the best possible switching rate. Nonfabric-enabled modules do not support the compact mode and will generate CRC errors if they receive frames in compact mode.

Examples

This example shows how to display fabric channel counter information for a specific module:

```
Console> show fabric channel counters 2
Channel 0 counters:
0 rxErrors                          =                   0
1 txErrors                          =                   0
2 txDropped                         =                   0
Console>
```

This example shows how to display fabric channel utilization information:

```
Console> show fabric channel utilization
Fab Chan Input Output
-------- ----- ------
       0    0%     0%
       1    0%     0%
       2    0%     0%
       3    0%     0%
.
.
.
      15    0%     0%
      16    0%     0%
      17    0%     0%
Console>
```

This example shows how to display switch mode and fabric channel status:

```
Console> show fabric channel switchmode
Global switching mode: flow through
Module Num Fab Chan Fab Chan Switch Mode  Channel Status
------ ------------ -------- ------------ --------------
     2            1   0, 1   flow through ok
     3            0   n/a    n/a          n/a
     5           18   0, 0   n/a          unknown
     5           18   1, 1   n/a          ok
.
.
.
     5           18  15, 15  n/a          unknown
     5           18  16, 16  n/a          unknown
     5           18  17, 17  n/a          unknown
    16            0 n/a      n/a          n/a
Console>
```

Table 2-30 describes the fields in the **show fabric channel** output.

Table 2-30 show fabric channel Command Output Fields

Field	Description
rxErrors	Number of received errors.
txErrors	Number of transmitted errors.
txDropped	Number of dropped transmitted packets.
Input	Percentage of input traffic utilization.
Output	Percentage of output traffic utilization.
Num Fab Chan	Number of fabric channels associated with the module.
Global switching mode	Global switching mode of the switch (flow through, truncated, and compact).

Table 2-30 show fabric channel Command Output Fields (continued)

Field	Description
Fab Chan	Fabric channel number; see the "Usage Guidelines" section for additional information.
Switch Mode	Channel switch mode type (flow through, truncated, and compact).
Channel Status	Channel status (ok, sync error, CRC error, heartbeat error, buffer error, timeout error, or unknown).

Related Commands **switch fabric**

show file

Use the **show file** command to display the contents of a file that have been saved to Flash memory.

show file [*device***:**]*filename* [**dump**]

Syntax Description

*device***:**	(Optional) Device where the Flash memory resides.
filename	Name of the configuration file.
dump	(Optional) Keyword to show the hexadecimal dump of the file.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

A colon (:) is required after the specified device.

Examples

This example shows how to display the contents of the configuration file saved to Flash memory:

```
Console> (enable) show file slot0:cfgfile
begin
!
#version 5.4
!
set password $1$FMFQ$HfZR5DUszVHIRhrz4h6V70
set enablepass $1$FMFQ$HfZR5DUszVHIRhrz4h6V70
set prompt Console>
set length 24 default
!
#system
set system baud  9600
set system modem disable
...
Console> (enable)
```

This example shows how to display the hexadecimal dump from a file:

```
Console> (enable) show file slot:cfgfile dump
8099d140  0A626567 696E0A21 0A237665 7273696F   .begin.!.#versio
8099d150  6E20352E 3328302E 31312942 4F552D45   n 5.3(0.11)BOU-E
8099d160  6E670A21 0A736574 20706173 73776F72   ng.!.set passwor
8099d170  64202431 24464D46 51244866 5A523544   n $1$FMFQ$HfZR5D
8099d180  55737A56 48495268 727A3468 36563730   UszVHIRhrz4h6V70
8099d190  0A736574 20656E61 626C6570 61737320   .set enablepass
8099d1a0  24312446 4D465124 48665A52 35445573   $1$FMFQ$HfZR5DUs
8099d1b0  7A564849 5268727A 34683656 37300A73   zVHIRhrz4h6V70.s
...
```

show flash

Use the **show flash** command to list bootflash or Flash PC card information, including file code names, version numbers, volume ID, status, and sizes.

show flash devices

show flash [[*m*/]*device*:] [**all** | **chips** | **filesys**]

Syntax Description

m/	(Optional) Module number of the supervisor engine containing the Flash device.
*device***:**	(Optional) Valid devices are **bootflash** and **slot0**.
all	(Optional) Keyword to list deleted files, undeleted files, and files with errors on a Flash memory device.
chips	(Optional) Keyword to show information about the Flash chip.
filesys	(Optional) Keyword to show the Device Info Block, the Status Info, the Usage Info, and the volume ID.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

A colon (:) is required after the specified device.

Examples

This example shows how to list the Flash files:

```
Console> show flash devices
slot0, bootflash, tftp
Console>
```

These examples show how to list supervisor engine Flash information:

```
Console> show flash
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
  1 .. ffffffff fec05d7a  4b3a4c   25  4667849 Mar 03 2000 08:52:09 cat6000-sup.
5-3-4-CSX.bin
  2 .. ffffffff 4e5efc31  c0fadc   30  7716879 May 19 2000 06:50:55 cat6000-sup-
d.6-1-0-83-ORL.bin

3605796 bytes available (12384988 bytes used)
Console>
```

```
Console> show flash chips
******** Intel Series 2+ Status/Register Dump ********

ATTRIBUTE MEMORY REGISTERS:
  Config Option Reg (4000): 2
  Config Status Reg (4002): 0
  Card Status   Reg (4100): 1
  Write Protect Reg (4104): 4
  Voltage Cntrl Reg (410C): 0
  Rdy/Busy Mode Reg (4140): 2
COMMON MEMORY REGISTERS: Bank 0
  Intelligent ID Code  : 8989A0A0
  Compatible Status Reg: 8080
  Global     Status Reg: B0B0
  Block Status Regs:
    0  :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    8  :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    16 :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    24 :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0

COMMON MEMORY REGISTERS: Bank 1
  Intelligent ID Code  : 8989A0A0
  Compatible Status Reg: 8080
  Global     Status Reg: B0B0
  Block Status Regs:
    0  :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    8  :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    16 :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    24 :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0

COMMON MEMORY REGISTERS: Bank 2
  Intelligent ID Code  : FF00FF
    IID Not Intel -- assuming bank not populated

COMMON MEMORY REGISTERS: Bank 3
Console>

Console> show flash all
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
  1 .. ffffffff fec05d7a  4b3a4c   25  4667849 Mar 03 2000 08:52:09 cat6000-sup.
5-3-4-CSX.bin
  2 .. ffffffff 4e5efc31  c0fadc   30  7716879 May 19 2000 06:50:55 cat6000-sup-
d.6-1-0-83-ORL.bin

3605796 bytes available (12384988 bytes used)

-------- F I L E   S Y S T E M   S T A T U S --------
  Device Number = 0
DEVICE INFO BLOCK:
  Magic Number          = 6887635   File System Vers = 10000    (1.0)
  Length                = 800000    Sector Size      = 20000
  Programming Algorithm = 4         Erased State     = FFFFFFFF
  File System Offset    = 20000     Length = 7A0000
  MONLIB Offset         = 100       Length = C730
  Bad Sector Map Offset = 1FFF8     Length = 8
  Squeeze Log Offset    = 7C0000    Length = 20000
  Squeeze Buffer Offset = 7E0000    Length = 20000
  Num Spare Sectors     = 0
    Spares:
STATUS INFO:
  Writable
  NO File Open for Write
  Complete Stats
  No Unrecovered Errors
```

```
USAGE INFO:
  Bytes Used     = 201D9B  Bytes Available = 5FE265
  Bad Sectors    = 0       Spared Sectors  = 0
  OK Files       = 1       Bytes = 100FC0
  Deleted Files  = 1       Bytes = 100DDB
  Files w/Errors = 0       Bytes = 0

******** Intel Series 2+ Status/Register Dump ********

ATTRIBUTE MEMORY REGISTERS:
  Config Option Reg (4000): 2
  Config Status Reg (4002): 0
  Card Status   Reg (4100): 1
  Write Protect Reg (4104): 4
  Voltage Cntrl Reg (410C): 0
  Rdy/Busy Mode Reg (4140): 2

COMMON MEMORY REGISTERS: Bank 0
  Intelligent ID Code  : 8989A0A0
  Compatible Status Reg: 8080
  Global     Status Reg: B0B0
  Block Status Regs:
    0  :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    8  :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    16 :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    24 :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0

COMMON MEMORY REGISTERS: Bank 1
  Intelligent ID Code  : 8989A0A0
  Compatible Status Reg: 8080
  Global     Status Reg: B0B0
  Block Status Regs:
    0  :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    8  :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    16 :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    24 :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0

COMMON MEMORY REGISTERS: Bank 2
  Intelligent ID Code  : FF00FF
    IID Not Intel -- assuming bank not populated

COMMON MEMORY REGISTERS: Bank 3
  Intelligent ID Code  : FF00FF
    IID Not Intel -- assuming bank not populated

COMMON MEMORY REGISTERS: Bank 4
  Intelligent ID Code  : FF00FF
    IID Not Intel -- assuming bank not populated
Console>
```

Related Commands

download
reset—switch

show garp timer

Use the **show garp timer** command to display all the values of the GARP timers.

show garp timer

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

You must maintain the following *relationship* for the various timer values:

- Leave time must be greater than or equal to three times the join time.
- Leaveall time must be greater than the leave time.

Caution Set the same GARP application (for example, GMRP and GVRP) timer values on all Layer 2-connected devices. If the GARP timers are set differently on the Layer 2-connected devices, GARP applications will not operate successfully.

Note The modified timer values are applied to all GARP application (for example, GMRP and GVRP) timer values.

Examples

This example shows how to display all the values of the GARP timers:

```
Console> (enable) show garp timer
Timer     Timer Value (milliseconds)
--------  -------------------------
Join      200
Leave     600
LeaveAll  10000
Console> (enable)
```

Related Commands

set garp timer
set gmrp timer
set gvrp timer

show gmrp configuration

Use the **show gmrp configuration** command to display complete GMRP-related configuration information.

show gmrp configuration

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If the port list exceeds the available line spaces, the list wraps to the next line.

Examples

This example shows how to display GMRP-related configuration information:

```
Console> (enable) show gmrp configuration
Global GMRP Configuration:
GMRP Feature is currently enabled on this switch.
GMRP Timers (milliseconds):
Join = 200
Leave = 600
LeaveAll = 10000
Port based GMRP Configuration:
GMRP-Status Registration ForwardAll Port(s)
----------- ------------ ---------- ------------------------------------------
Enabled     Normal       Disabled   1/1-2
                                    2/1-48
                                    15/1
Console> (enable)
```

Related Commands

set gmrp registration

show gmrp statistics

Use the **show gmrp statistics** command to display all the GMRP-related statistics for a specified VLAN.

show gmrp statistics [*vlan*]

Syntax Description

vlan	(Optional) VLAN for which to show GMRP statistics; valid values are from **1** to **1005** and from **1025** to **4094**.

Defaults

The default is that if you do not specify a VLAN, statistics for VLAN 1 are shown.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display all the GMRP-related statistics for VLAN 23:

```
Console> show gmrp statistics 23
GMRP Statistics for vlan <23>:
Total valid GMRP Packets Received:                      500
Join Empties:                                           200
Join INs:                                               250
Leaves:                                                 10
Leave Alls:                                             35
Empties:                                                5
Fwd Alls:                                               0
Fwd Unregistered:                                       0
Total valid GMRP Packets Transmitted:                   600
Join Empties:                                           200
Join INs:                                               150
Leaves:                                                 45
Leave Alls:                                             200
Empties:                                                5
Fwd Alls:                                               0
Fwd Unregistered:                                       0
Total valid GMRP Packets Received:                      0
Total GMRP packets dropped:                             0
Total GMRP Registrations Failed:                        0
Console>
```

Related Commands

clear gmrp statistics
set gmrp

show gmrp timer

Use the **show gmrp timer** command to display all the values of the GMRP timers.

show gmrp timer

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display all the values of the GMRP timers:

```
Console> (enable) show gmrp timer
Timer               Timer Value(milliseconds)
-------------------------------------------
Join                200
Leave               600
Leave All           10000
Console> (enable)
```

Related Commands

set garp timer
set gmrp timer
set gvrp timer
show gmrp configuration

show gvrp configuration

Use the **show gvrp configuration** command to display GVRP configuration information, including timer values, whether GVRP and dynamic VLAN creation is enabled, and which ports are running GVRP.

show gvrp configuration

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If the port list exceeds the available line spaces, the list wraps to the next line.

If no ports are GVRP participants, the message output changes from:

```
GVRP Participants running on port_list
```

to:

```
GVRP Participants running on no ports.
```

Examples

This example shows how to display GVRP configuration information:

```
Console> show gvrp configuration

Global GVRP Configuration:
GVRP Feature is currently enabled on the switch.
GVRP dynamic VLAN creation is enabled.
GVRP Timers(milliseconds)
Join = 200
Leave = 600
LeaveAll = 10000

Port based GVRP Configuration:
GVRP-Status Registration Applicant Port(s)
----------- ------------ --------- -----------------------------------------
Enabled.    Normal       Normal    2/1
Enabled.    Normal       Active    4/4
Enabled.    Fixed        Normal    4/9
Enabled.    Fixed        Active    4/11
Enabled.    Forbidden    Normal    4/10
Enabled.    Forbidden    Active    4/5
Disabled    Normal       Normal    2/2
                                   4/12-24
                                   5/1-8
Disabled    Normal       Active    4/1,4/8
```

```
Disabled   Fixed       Normal   4/2
Disabled   Fixed       Active   4/7
Disbled    Forbidden   Normal   4/3
Disbled    Forbidden   Active   4/6

GVRP Participants running on no ports.
Console>
```

Related Commands

- clear gvrp statistics
- set gvrp
- set gvrp dynamic-vlan-creation
- set gvrp registration
- set gvrp timer
- show gvrp statistics

show gvrp statistics

Use the **show gvrp statistics** command to view GVRP statistics for a port.

show gvrp statistics [*mod/port*]

Syntax Description

mod/port	(Optional) Number of the module and port on the module.

Defaults

The default is, that if you do not specify a VLAN, statistics for VLAN 1 are shown.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display GVRP statistics for module 2, port 1:

```
Console> show gvrp statistics 2/1
GVRP enabled

GVRP statistics for port 2/1:
Total valid pkts rcvd:           18951
Total invalid pkts recvd         0
General Queries recvd            377
Group Specific Queries recvd     0
MAC-Based General Queries recvd  0
Leaves recvd                     14
Reports recvd                    16741
Queries  Xmitted                 0
GS Queries Xmitted               16
Reports Xmitted                  0
Leaves Xmitted                   0
Failures to add GDA to EARL      0
Topology Notifications rcvd      10
GVRP packets dropped             0
Console>
```

Table 2-31 describes the fields in the **show gvrp statistics** output.

Table 2-31 show gvrp statistics Command Output Fields

Field	Description
GVRP Enabled	Status of whether GVRP is enabled or disabled.
Total valid pkts rcvd	Total number of valid GVRP packets received.
Total invalid pkts recvd	Total number of invalid GVRP packets received.
General Queries recvd	Total number of GVRP general queries received.
Group Specific Queries recvd	Total number of GVRP group-specific queries received.

Table 2-31 show gvrp statistics Command Output Fields (continued)

Field	Description
MAC-Based General Queries recvd	Total number of MAC-based general queries received.
Leaves recvd	Total number of GVRP leaves received.
Reports recvd	Total number of GVRP reports received.
Queries Xmitted	Total number of GVRP general queries transmitted by the switch.
GS Queries Xmitted	Total number of GVRP group specific-equivalent queries transmitted by the switch.
Reports Xmitted	Total number of GVRP reports transmitted by the switch.
Leaves Xmitted	Total number of GVRP leaves transmitted by the switch.
Failures to add GDA to EARL	Total number of times the switch failed to add a multicast entry (GDA) to the EARL table.
Topology Notifications rcvd	Total number of topology change notifications received by the switch.
GVRP packets dropped	Total number of GVRP packets dropped by the switch.

Related Commands

clear gvrp statistics
set gvrp
set gvrp dynamic-vlan-creation
set gvrp registration
set gvrp timer
show gvrp configuration

show ifindex

Use the **show ifindex** command to display the information of the specific ifIndex.

show ifindex *number*

Syntax Description

number	Number of the ifIndex.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

You can designate multiple ifIndex numbers by separating each number with a comma. To specify a range of numbers, use a dash (-) between the low and high numbers.

Examples

This example shows how to display ifIndex information:

```
Console> show ifindex 1,2,3,4-15,40-45
 Ifindex 1 is mapped to interface sc0.
 Ifindex 2 is mapped to interface sl0.
 Ifindex 3 is mapped to port 1/1.
 Ifindex 4 is mapped to port 1/2.
 Ifindex 5 is mapped to port 1/3.
 Ifindex 6 is mapped to port 1/4.
 Ifindex 7 is mapped to vlan 1.
 Ifindex 8 is mapped to vlan 1002.
 Ifindex 9 is mapped to vlan 1004.
 Ifindex 10 is mapped to vlan 1005.
 Ifindex 11 is mapped to vlan 1003.
 Ifindex 12 is mapped to port 9/1.
 Ifindex 13 is mapped to port 9/2.
 Ifindex 14 is mapped to port 9/3.
 Ifindex 15 is mapped to port 9/4.
 Ifindex 40 is mapped to port 8/5.
 Ifindex 41 is mapped to port 8/6.
 Ifindex 42 is mapped to port 8/7.
 Ifindex 43 is mapped to port 8/8.
 Ifindex 44 is mapped to port 8/9.
 Ifindex 45 is mapped to FEC-1/1-2.
Console>
```

show igmp mode

Use the **show igmp mode** command to display the IGMP mode on the switch.

show igmp mode

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch.

Command Modes

Normal.

Usage Guidelines

The switch dynamically chooses either IGMP-only or IGMP-CGMP mode, depending on the traffic present on the network. IGMP-only mode is used in networks with no CGMP devices. IGMP-CGMP mode is used in networks with both IGMP and CGMP devices.

The **show igmp mode** command output includes three fields:

- IGMP Mode—Possible values are auto, igmp-only, and igmp-cgmp.
- IGMP-Operational-Mode—Possible values are igmp-only and igmp-cgmp.
- IGMP Address Aliasing Mode—Possible values are normal and fallback.

Examples

This example shows how to diplay the IGMP mode:

```
Console> show igmp mode
IGMP Mode:                  auto
IGMP Operational Mode:      igmp-only
IGMP Address Aliasing Mode: normal
Console>
```

Related Commands

set igmp mode

show igmp ratelimit-info

Use the **show igmp ratelimit** command to display the IGMP rate limit for general-query packets, IGMP snooping protocol packets, and Protocol Independent Multicasting version 2 (PIMv2) packets.

show igmp ratelimit-info

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The output of this command displays the number of IGMP rate limiting packets that are sent out every 30 seconds.

Examples

This example shows how to display IGMP rate limiting information:

```
Console> show igmp ratelimit-info
IGMP Ratelimiting is enabled
IGMP Ratelimiting: No of messages allowed in 30 seconds
-----------------------------------------------------
Igmp General Queries : 100
Dvmrp Probes         : 100
Mospf1 Hellos        : 100
Mospf2 Hellos        : 100
PimV2 Hellos         : 100
Console>
```

Related Commands

set igmp ratelimit

show igmp statistics

Use the **show igmp statistics** command to view IGMP statistics for a particular VLAN.

show igmp statistics [*vlan_id*]

Syntax Description

vlan_id	(Optional) VLAN for which to show IGMP statistics; valid values are from **1** to **1005** and from **1025** to **4094**.

Defaults

The default is that if you do not specify a VLAN, statistics for VLAN 1 are shown.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to view IGMP statistics for VLAN 1:

```
Console> show igmp statistics 1
IGMP enabled

IGMP statistics for vlan 1:
Total valid pkts rcvd:           18951
Total invalid pkts recvd         0
General Queries recvd            377
Group Specific Queries recvd     0
MAC-Based General Queries recvd  0
Leaves recvd                     14
Reports recvd                    16741
Queries  Xmitted                 0
GS Queries Xmitted               16
Reports Xmitted                  0
Leaves Xmitted                   0
Failures to add GDA to EARL      0
Topology Notifications rcvd      10
IGMP packets dropped             0
Console>
```

Table 2-32 describes the fields in the **show igmp statistics** output.

Table 2-32 show igmp statistics Command Output Fields

Field	Description
IGMP enabled	Status of whether IGMP snooping is enabled or disabled.
Total valid pkts rcvd	Number of valid IGMP packets received.
Total invalid pkts recvd	Number of invalid IGMP packets received.
General Queries recvd	Number of IGMP general queries received.

Table 2-32 show igmp statistics Command Output Fields (continued)

Field	Description
Group Specific Queries recvd	Number of IGMP group-specific queries received.
MAC-Based General Queries recvd	Number of MAC-based general queries received.
Leaves recvd	Number of IGMP leaves received.
Reports recvd	Number of IGMP reports received.
Queries Xmitted	Number of IGMP general queries transmitted by the switch.
GS Queries Xmitted	Number of IGMP group-specific equivalent queries transmitted by the switch.
Reports Xmitted	Number of IGMP reports transmitted by the switch.
Leaves Xmitted	Number of IGMP leaves transmitted by the switch.
Failures to add GDA to EARL	Number of times the switch failed to add a multicast entry (GDA) to the EARL table.
Topology Notifications rcvd	Number of topology change notifications received by the switch.
IGMP packets dropped	Number of IGMP packets dropped by the switch.

Related Commands

clear igmp statistics
clear multicast router
set igmp
set multicast router
show multicast group
show multicast router

show imagemib

Use the **show imagemib** command to display image information provided in the CISCO-IMAGE-MIB for a particular image.

show imagemib *filename*

Syntax Description

filename	Name of the Flash device on the supervisor engine.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display CISCO-IMAGE-MIB information for the Flash image:

```
Console> (enable) show imagemib bootflash:cat6000-sup.6-1-1.bin
show mib info for file bootflash:cn50
CW_BEGIN$cat6000-WS-X6K-SUP1$
CW_IMAGE$bootflash:at6000-sup.5-5-1.bin$
CW_FAMILY$Catalyst 6000 Switch$
CW_MODULE$Catalyst Supervisor Module$
CW_VERSION$5.5.1$
CW_MIN_DRAM$ 32 MB$
CW_MIN_BOOTFLASH$  8 MB$
CW_MIN_NVRAM$ 512 KB$
CW_BUILDTIME$  Mar 24 2000 00:32:33$
CW_SYSDESCR$Catalyst Operating System$
CW_END$cat6000-WS-X6K-SUP1$
Console>
```

show interface

Use the **show interface** command to display information on network interfaces.

show interface

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display sl0 and sc0:

```
Console> show interface
sl0: flags=51<UP,POINTOPOINT,RUNNING>
        slip 0.0.0.0 dest 0.0.0.0
sc0: flags=63<UP,BROADCAST,RUNNING>
        vlan 1 inet 174.44.67.8 netmask 255.255.0.0 broadcast 172.20.255.255
dhcp server: 174.44.67.201
Console>
```

Table 2-33 describes the fields in the **show interface** command output.

Table 2-33 show interface Command Output Fields

Field	Description
sl0	Information on the SLIP interface.
flags	Flags indicating the interface state (decoded in the subsequent field).
<UP,POINTOPOINT, RUNNING>	Interface state (UP, DOWN, BROADCAST, LOOPBACK, POINTOPOINT, or RUNNING).
slip	IP address of the SLIP interface.

Table 2-33 show interface Command Output Fields (continued)

Field	Description
dest	IP address of the host to which the console port will be connected.
sc0	Information on the in-band interface.
vlan	Number of the VLAN to which the sc0 interface has been assigned (known as the management VLAN).
inet	IP address of the interface.
netmask	Network mask for the interface.
broadcast	Broadcast address for the interface.
dhcp server	IP address of the DHCP server.

Related Commands **set interface**

show ip alias

Use the **show ip alias** command to show a listing of defined IP aliases.

show ip alias [*name*]

Syntax Description

name	(Optional) Alias for a specific host.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display a listing of all IP aliases:

```
Console> show ip alias
default         0.0.0.0
sparc20         192.168.10.69
cat6000-1       172.16.169.16
cat6000-2       172.16.169.20
Console>
```

Related Commands

clear ip alias
set ip alias

show ip dns

Use the **show ip dns** command to show the DNS name servers and the default DNS domain name.

show ip dns

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the DNS name servers and the default DNS domain name:

```
Console> show ip dns
DNS is currently enabled.
The default DNS domain name is: cisco.com

DNS name server            status
---------------            -------
172.16.30.32
192.168.2.132              primary
172.31.128.70
Console>
```

Table 2-34 describes the fields in the **show ip dns** command output.

Table 2-34 show ip dns Command Output Fields

Field	Description
DNS is currently enabled	Status of whether DNS is enabled or disabled.
default DNS domain name	Default DNS domain name.
DNS name server	IP addresses or IP aliases of the configured DNS servers.
status	Primary DNS server.

Related Commands

clear ip dns domain
clear ip dns server
set ip dns
set ip dns domain
set ip dns server

show ip http

Use the **show ip http** command to view the HTTP configuration and the switch web interface information.

show ip http

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the HTTP configuration and web interface information if the web interface is supported:

```
Console> show ip http
HTTP Configuration Information:
---------------
HTTP Server: enabled
HTTP port: 80
Web Interface: Supported

Switch Information:
-----------------
File:  applet.html
       size: 912 bytes
       version: 5.0(0.26)
       date: 10/9/99
File:  cvembopt.jar
       size: 3500000 bytes
       version: 5.0(0.26)
       date: 10/9/99

Active Web Interface Session: 1
----------------------------
Client IP Address: 192.20.20.45
Request Type: GET
Request URI: /all-engine.jar
Console>
```

This example shows the HTTP configuration and web interface information if the web interface is not supported:

```
Console> show ip http
HTTP Configuration Information:
---------------
HTTP Server: disabled
HTTP port: 80
Web Interface: Not Supported
Console>
```

Related Commands

set ip http port
set ip http server

show ip permit

Use the **show ip permit** command to display the IP permit list information.

show ip permit [**noalias**]

Syntax Description

noalias	(Optional) Keyword to force the display to show IP addresses, not IP aliases.

Defaults

This command has no default value.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the IP permit list information:

```
Console> (enable) show ip permit
Telnet permit list feature enabled.
Ssh permit list enabled.
Snmp permit list feature disabled.

Permit List          Mask              Access-Type
---------------      ---------------   ---------------
172.16.0.0         255.255.0.0         telnet
172.20.52.3                            snmp telnet
172.20.52.32       255.255.255.224     snmp

Denied IP Address   Last Accessed Time Type
-----------------   ------------------ ------
172.100.101.104     01/20/97,07:45:20  SNMP
172.187.206.222     01/21/97,14:23:05  Telnet

Console> (enable)
```

Table 2-35 describes the fields in the **show ip permit** command output.

Table 2-35 show ip permit Command Output Fields

Field	Description
IP permit list feature enabled	Status of whether the IP permit list feature is enabled or disabled.
Permit List	IP addresses and IP aliases that are allowed to access the switch.
Mask	Subnet masks of permitted IP addresses.
Denied IP Address	IP addresses and IP aliases that are not allowed to access the switch.

Table 2-35 show ip permit Command Output Fields (continued)

Field	Description
Last Accessed Time	Date and time of the last attempt to log in to the switch from the address.
Type	Login-attempt type.

Related Commands

clear ip permit
set ip permit
set snmp trap

show ip route

Use the **show ip route** command to display IP routing table entries.

show ip route [**noalias**]

Syntax Description

noalias	(Optional) Keyword to force the display to show IP addresses, not IP aliases.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the IP route table:

```
Console> show ip route
Fragmentation   Redirect   Unreachable
-------------   --------   -----------
enabled         enabled    enabled

Destination      Gateway          RouteMask    Flags   Use       Interface
---------------  ---------------  ----------   -----   --------  ---------
172.20.0.0       172.20.26.70     0xffff0000   U       8          sc0
default          default          0xff000000   UH      0          sl0
Console>
```

Table 2-36 describes the fields in the **show ip route** command output.

Table 2-36 show ip route Command Output Fields

Field	Description
Fragmentation	Current setting of IP fragmentation.
Redirect	Current setting of ICMP redirect.
Unreachable	Current setting of ICMP unreachable messages.
Destination	Destination address IP route mask.
Gateway	IP address or IP alias of the gateway router.
RouteMask	Determines which path is closer to the destination.
Flags	Route status; possible values are U=up, G=route to a Gateway, H=route to a Host, and D=Dynamically created by a redirect.
Use	Number of times a route entry was used to route packets.
Interface	Type of interface.

Related Commands clear ip route
set ip route

show kerberos

Use the **show kerberos** command to display the Kerberos configuration information.

show kerberos [**creds**]

Syntax Description

creds	(Optional) Keyword to display credential information only.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display Kerberos configuration information:

```
Console> (enable) show kerberos
Kerberos Local Realm:CISCO.COM
Kerberos server entries:
Realm:CISCO.COM,  Server:187.0.2.1,  Port:750

Kerberos Domain<->Realm entries:
Domain:cisco.com,  Realm:CISCO.COM

Kerberos Clients NOT Mandatory
Kerberos Credentials Forwarding Enabled
Kerberos Pre Authentication Method set to None
Kerberos config key:
Kerberos SRVTAB Entries
Srvtab Entry 1:host/niners.cisco.com@CISCO.COM 0 932423923 1 1 8 01;;8>00>50;0=0=0
Console> (enable)
```

Table 2-37 describes the fields in the **show kerberos** command output.

Table 2-37 show kerberos Command Output Fields

Field	Description
Kerberos Local Realm	Status of whether the local realm is configured.
Kerberos server entries	Status of servers entered into the switch.
Kerberos Domain<->Realm entries	Kerberos domain and realm entries.
Kerberos Clients NOT Mandatory	Status of whether Kerberos has been configured as mandatory on the clients.

Table 2-37 show kerberos Command Output Fields (continued)

Field	Description
Kerberos Credentials Forwarding Disabled	Status of whether credentials forwarding is enabled or disabled.
Kerberos Pre Authentication Method	Status of whether preauthentication is enabled or disabled.
Kerberos config key	Status of whether a 3DES key has been configured.
Kerberos SRVTAB entries	SRVTAB entries.

Related Commands

clear kerberos clients mandatory
clear kerberos credentials forward
clear kerberos realm
clear kerberos server
clear key config-key
set kerberos clients mandatory
set kerberos credentials forward
set kerberos local-realm
set kerberos realm
set kerberos srvtab entry
set kerberos srvtab remote
set key config-key
show kerberos

show lacp-channel

Use the **show lacp-channel** command to display information about the LACP channel.

show lacp-channel

show lacp-channel sys-id

show lacp-channel group [*admin-key*] [**info** [*type*] | **statistics**]

show lacp-channel [*channel_id*] [**info** [*type*] | **statistics** | **mac**]

show lacp-channel hash *channel_id* {{*src_ip_addr* [*dest_ip_addr*]} | *dest_ip_addr* | {*src_mac_addr* [*dest_mac_addr*]} | *dest_mac_addr* | {*src_port dest_port*} | *dest_port*}

show lacp-channel traffic [*channel_id*]

Syntax Description

sys-id	Keyword to display the system identifier adopted by LACP.
group	Keyword to display all the ports that belong to a channel.
admin-key	(Optional) Number of the administrative key; valid values are from **1** to **65535**.
info	(Optional) Keyword to display detailed LACP channel information.
type	(Optional) Name of the feature-related parameter; valid values are **auxiliaryvlan**, **cops**, **dot1qtunnel**, **gmrp**, **gvrp**, **jumbo**, **protocol**, **qos**, **rsvp**, **spantree**, **trunk**.
statistics	(Optional) Keyword to display LACP statistics.
channel_id	(Optional) Number of the channel; valid values are from **769** to **896**.
mac	(Optional) Keyword to specify MAC information about the channel.
hash	Keyword to display the outgoing port used in a channel for a specific address or Layer 4 port number.
src_ip_addr	Source IP address.
dest_ip_addr	(Optional) Destination IP address.
src_mac_addr	Source MAC address.
dest_mac_addr	(Optional) Destination MAC address.
src_port	Number of the source port; valid values are from **0** to **65535**.
dest_port	Number of the destination port; valid values are from **0** to **65535**.
traffic	Keyword to display traffic utilization on channel ports.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify *admin-key*, information about all LACP channels is displayed.

If you do not specify *channel_id*, information about all LACP channels is displayed.

For differences between PAgP and LACP, refer to the "Guidelines for Port Configuration" section of the "Configuring EtherChannel" chapter of the *Catalyst 6000 Family Software Configuration Guide*.

Examples

This example shows how to display information about all LACP channels:

```
Console> show lacp-channel group
Admin Key    Ports
-----------  ------
69           4/1-2
70           4/5-6
143          2/1-2
151          4/3-4
152          4/7-8
Console>
```

This example shows how to display limited information about ports that are assigned to administrative key 152:

```
Console> show lacp-channel group 152
Port  Channel   Admin Ch   Partner Oper                        Partner
      Mode      Key   id   Sys ID                              Port
----- --------- ----- ---- ---------------------------------- -------
 4/7   active     152   770  8000,AC-12-24-56-78-90            4/3
 4/8   active     152   770  8000,AC-12-24-56-78-90            4/4
Console>
```

This example shows how to display detailed information about ports that are assigned to administrative key 152:

```
Console> show lacp-channel group 152 info
I = Isolated Port.  C = Channeling Port.  N = Not Connected.
H = Hot Stand-by Port.  S = Suspended Port.

Port  LACP Port Port  Speed Duplex VLANs  Trunk status Port  STP Port PortSecurity/
      Priority  Status                                Cost  Priority Dynamic Port
----- --------- ----- ----- ------ ------ ------------ ----- -------- ------------
 4/7  130       C      1000  full   1-1005 not-trunking    4      32
 4/8  131       C      1000  full   1-1005 not-trunking    4      32

Port  Admin Channel if-   Partner Oper              Partner     Partner   Partner
       Key  id      Index Sys ID                   Port Prior  Port      Oper Key
----- ----- ------- ----- ------------------------ ----------  --------  ----------
 4/7  152   770     31    800,AC-12-24-56-78-90     248          4/3       15768
 4/8  152   770     31    800,AC-12-24-56-78-90     249          4/4       15768
Console>
```

This example shows how to display LACP Tx and Rx statistics for ports that are assigned to administrative key 152:

```
Console> show lacp-channel group 152 statistics
Port  Admin    LACP Pkts  LACP Pkts Marker Pkts Marker Pkts LACP Pkts
       Key    Transmitted Received  Transmitted   Received    Errors
----- ------- ----------- --------- ----------- ----------- ---------
 4/7    152           0        92         0         0         0
 4/8    152           0         0         0         0         0
Console>
```

This example shows how to display all ports that are assigned to an administrative key:

```
Console> show lacp-channel group info
I = Isolated Port.  C = Channeling Port.  N = Not Connected.
H = Hot Stand-by Port.  S = Suspended Port.

Port  LACP Port Port  Speed Duplex VLANs  Trunk status Port  STP Port PortSecurity/
      Priority  Status                                 Cost  Priority Dynamic Port
----- --------- ----- ----- ------ ------ ------------ ----- -------- ------------
 4/1  50        I     1000  full   1-1005 not-trunking     4       32
 4/2  51        I     1000  full   1-1005 not-trunking     4       32
 4/5  27        I     1000  full   1-1005 not-trunking     4       32
 4/6  28         I    1000  full   1-1005  not-trunking     4      32
 2/1  133       C     1000  full   1-1005 not-trunking     4       32
 2/2  134       C     1000  full   1-1005 not-trunking     4       32
 4/3  200       C     1000  full   1-1005 not-trunking     4       32
 4/4  201       C     1000  full   1-1005 not-trunking     4       32
 4/7  130       C     1000  full   1-1005 not-trunking     4       32
 4/8  131       C     1000  full   1-1005 not-trunking     4       32

Port  Admin   Channel if-   Partner Oper                Partner    Partner  Partner
       Key    id      Index Sys ID                      Port Prior Port     Oper Key
----- ------- ------- ----- -------------------------- ---------- ------- --------
 4/1  69      0       -     0,00-00-00-00-00-00        0          3/1     0
 4/2  69      0       -     0,00-00-00-00-00-00        0          4/5     0
 4/5  70      0       -     0,00-00-00-00-00-00        0          7/3     0
 4/6  70      0       -     0,00-00-00-00-00-00        0          7/4     0
 2/1  143     768     29    1276,45-12-24-AC-78-90     34         5/1     5658
 2/2  143     768     29    1276,45-12-24-AC-78-90     35         5/2     5658
 4/3  151     769     30    13459,89-BC-24-56-78-90    200        1/1     9768
 4/4  151     769     30    13459,89-BC-24-56-78-90    201        1/2     9768
 4/7  152     770     31    8000,AC-12-24-56-78-90     248        4/3     15678
 4/8  152     770     31    8000,AC-12-24-56-78-90     249        4/4     15768
Console>
```

This example shows how to display Tx and Rx statistics for all ports that are assigned to an administrative key:

```
Console> show lacp-channel group statistics
Port  Admin    LACP Pkts  LACP Pkts Marker Pkts Marker Pkts LACP Pkts
       Key    Transmitted Received  Transmitted   Received    Errors
----- ------- ----------- --------- ----------- ----------- ---------
 4/1       69           0         0           0           0         0
 4/2       69           0         0           0           0         0
 4/5       70           0         0           0           0         0
 4/6       70           0         0           0           0         0
 2/1      143           0         0           0           0         0
 2/2      143           0         0           0           0         0
 4/3      151           0         0           0           0         0
 4/4      151           0         0           0           0         0
 4/7      152           0        92           0           0         0
 4/8      152           0         0           0           0         0
Console>
```

This example shows how to display the outgoing port for the specified source and destination IP addresses:

```
Console> (enable) show lacp-channel hash 808 172.20.32.10 172.20.32.66
Selected channel port:2/17
Console> (enable)
```

This example shows how to display traffic utilization on channel ports:

```
Console> (enable) show lacp-channel traffic
ChanId Port  Rx-Ucst Tx-Ucst Rx-Mcst Tx-Mcst Rx-Bcst Tx-Bcst
------ ----- ------- ------- ------- ------- ------- -------
   808  2/16   0.00%   0.00%  50.00%  75.75%   0.00%   0.00%
   808  2/17   0.00%   0.00%  50.00%  25.25%   0.00%   0.00%
   816  2/31   0.00%   0.00%  25.25%  50.50%   0.00%   0.00%
   816  2/32   0.00%   0.00%  75.75%  50.50%   0.00%   0.00%
Console> (enable)
```

Related Commands

clear lacp-channel statistics
set channelprotocol
set lacp-channel system-priority
set port lacp-channel
set spantree channelcost
set spantree channelvlancost
show port lacp-channel

show lcperroraction

Use the **show lcperroraction** command to display how your system handles LCP errors when a module reports an ASIC problem to the NMP.

show lcperroraction

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to display the action that handles an LCP error:

```
Console> (enable) show lcperroraction
LCP action level is: system
Console> (enable)
```

Related Commands

set lcperroraction

show lda

Use the **show lda** command to display the ASLB configuration information.

show lda [**committed** | **uncommitted**]

show lda mls entry

show lda mls entry [**destination** *ip_addr_spec*] [**source** *ip_addr_spec*] [**protocol** *protocol*] [**src-port** *src_port*] [**dst-port** *dst_port*] [**short** | **long**]

show lda mls statistics count

show lda mls statistics entry

show lda mls statistics entry [**destination** *ip_addr_spec*] [**source** *ip_addr_spec*] [**protocol** *protocol*] [**src-port** *src_port*] [**dst-port** *dst_port*]

Syntax Description

committed	(Optional) Keyword to view committed configuration information.
uncommitted	(Optional) Keyword to view configuration information that has not been committed.
mls entry	Keywords to display the ASLB MLS entries.
destination *ip_addr_spec*	(Optional) Full destination IP address or a subnet address in these formats: *ip_addr*, *ip_addr/netmask*, or *ip_addr/maskbit*.
source *ip_addr_spec*	(Optional) Full source IP address or a subnet address in these formats: *ip_addr*, *ip_addr/netmask*, or *ip_addr/maskbit*.
protocol *protocol*	(Optional) Keyword and variable to specify additional flow information (protocol family and protocol port pair) to be matched; valid values include **tcp**, **udp**, **icmp**, or a decimal number for other protocol families.
src-port *src_port*	(Optional) Keyword and variable to specify the number of the TCP/UDP source port (decimal). Used with **dst-port** to specify the port pair if the protocol is **tcp** or **udp**. **0** indicates "do not care."
dst-port *dst_port*	(Optional) Keyword and variable to specify the number of the TCP/UDP destination port (decimal). Used with **src-port** to specify the port pair if the protocol is **tcp** or **udp**. **0** indicates "do not care."
short | **long**	(Optional) Keyword to specify the width of the display.
count	Keyword to display the number of active ASLB MLS entries.
mls statistics entry	Keywords to display statistics information.

Defaults

The default displays MLS entry information in long format.

Command Types

Switch command.

Command Modes Normal.

Usage Guidelines This command is supported only on switches configured with the Supervisor Engine 1 with Layer 3 Switching Engine WS-F6K-PFC (Policy Feature Card).

Entering the **destination** keyword specifies the entries matching the destination IP address specification, entering the **source** keyword specifies the entries matching the source IP address specification, and entering an *ip_addr_spec* can specify a full IP address or a subnet address. If you do not specify a keyword, it is treated as a wildcard, and all entries are displayed.

When entering the *ip_addr_spec*, use the full IP address or a subnet address in one of the following formats: *ip_addr*, *ip_addr/netmask*, or *ip_addr/maskbit*.

Entering the **destination** keyword specifies the entries matching the destination IP address specification, entering the **source** keyword specifies the entries matching the source IP address specification, and entering an *ip_addr_spec* can specify a full IP address or a subnet address. If you do not specify a keyword, it is treated as a wildcard, and all entries are displayed.

Use the following syntax to specify an IP subnet address:

- *ip_subnet_addr*—This is the 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 with a length of 8, 16, or 24 bits.
- *ip_addr/subnet_mask*—This is the 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* is allowed to be a full host address, such as 172.22.253.1/255.255.252.00.
- *ip_addr/maskbits*—This is the 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* is allowed to be a full host address, such as 172.22.254.1/22, which has the same subnet address as 172.22.252.00/72.

If you have disabled the ASLB feature, you can view the last configuration using the **show lda uncommitted** command.

The **short** | **long** options give the flexibility to display the output in regular (80 characters in width) or wide screen.

If you enter the **show lda mls entry** or the **show lda mls statistics entry** command with no keywords or variables, all entries are displayed.

Examples This example shows how to display committed ASLB information:

```
Console> (enable) show lda committed
Status:Committed

Local Director Flow:10.0.0.8/ (TCP port 8)
Router MAC:
00-02-03-04-05-06
00-04-56-67-04-05
00-03-32-02-03-03

LD MAC:00-02-03-04-05-06
```

```
LD Router Side:
---------------
Router and LD are on VLAN 110
LD is connected to switch port 4/26 on VLAN 110

LD Server Side:
---------------
Server(s) and LD are on VLAN 105
LD is connected to switch port 4/40 on VLAN 105
Console> (enable)
```

This example shows how to display uncommitted ASLB information:

```
Console> (enable) show lda uncommitted
Status:Not Committed.

Router MAC:
00-02-03-04-05-06
00-04-56-67-04-05
00-03-32-02-03-03

LD MAC:00-02-03-04-05-06

LD Router Side:
----------------

LD Server Side:
----------------
Console> (enable)
```

Note The examples shown for the **show lda mls entry** commands are displayed in short format. The display in the long form exceeds the page width and cannot be shown.

This example shows how to display ASLB MLS entries in short format:

```
Console> (enable) show lda mls entry short
Destination-IP  Source-IP       Prot  DstPrt SrcPrt Destination-Mac   Vlan
--------------- --------------- ----- ------ ------ ----------------- ----
EDst ESrc DPort  SPort  Stat-Pkts  Stat-Bytes  Uptime   Age
---- ---- ------ ------ ---------- ----------- -------- --------
10.0.0.8        172.20.20.10    TCP  8      64     00-33-66-99-22-44 105
ARPA ARPA -      4/25   0          0           00:00:02 00:00:05

10.0.0.8        172.20.20.11    TCP  8      64     00-33-66-99-22-44 105
ARPA ARPA -      4/25   0          0           00:00:05 00:00:08
Console> (enable)
```

This example shows how to display ASLB information for the source IP address in short format:

```
Console> (enable) show lda mls entry source 172.20.20.11 short
Destination-IP  Source-IP       Prot  DstPrt SrcPrt Destination-Mac   Vlan
--------------- --------------- ----- ------ ------ ----------------- ----
EDst ESrc DPort  SPort  Stat-Pkts  Stat-Bytes  Uptime   Age
---- ---- ------ ------ ---------- ----------- -------- --------
10.0.0.8        172.20.20.11    TCP  8      64     00-33-66-99-22-44 105
ARPA ARPA -      4/25   0          0           00:00:05 00:00:08
Console> (enable)
```

This example shows how to display the number of active ASLB MLS entries:

```
Console> (enable) show lda mls statistics count
LDA active shortcuts:20
Console> (enable)
```

This example shows how to display all ASLB MLS entry statistics:

```
Console> (enable) show lda mls statistics entry
                                 Last    Used
Destination IP  Source IP       Prot DstPrt SrcPrt Stat-Pkts  Stat-Bytes
--------------- --------------- ---- ------ ------ ---------- ---------------
10.0.0.8        172.20.20.10    TCP  WWW    64     636        29256
10.0.0.8        172.20.22.10    TCP  WWW    64     0          0
Console> (enable)
```

This example shows how to display the statistics for a specific destination IP address:

```
Console> (enable) show lda mls statistics entry destination 172.20.22.14
                Last Used         Last    Used
Destination IP  Source IP       Prot DstPrt SrcPrt Stat-Pkts  Stat-Bytes
--------------- --------------- ---- ------ ------ ---------- ---------------
172.20.22.14    172.20.25.10    6    50648  80     3152       347854
Console> (enable)
```

Related Commands

- **clear lda**
- **commit lda**
- **set lda**

show log

Use the **show log** command to display the error log for the system or a specific module.

show log [*mod*]

show log dump [*-count*]

Syntax Description

mod	(Optional) Number of the module for which the log is displayed.
dump	Keyword to display dump log information.
-count	(Optional) Number of dump log entries to display.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

To display the contents of ASIC error messages as soon as they are received from SLCP/LCP, see the **set logging server** command.

You can use the **dump** keyword to display log dump information generated when certain events occur, such as memory corruption.

Examples

This example shows a partial display of the output from the **show log** command:

```
Console> show log

Network Management Processor (ACTIVE NMP) Log:
  Reset count:   10
  Re-boot History:   Mar 22 2000 10:34:09 0, Mar 17 2000 15:35:11 0
                     Mar 13 2000 17:40:16 0, Mar 13 2000 13:14:08 0
                     Mar 13 2000 11:57:30 0, Feb 24 2000 10:04:18 0
  Bootrom Checksum Failures:      0   UART Failures:                  0
  Flash Checksum Failures:        0   Flash Program Failures:         0
  Power Supply 1 Failures:        0   Power Supply 2 Failures:        0
  Swapped to CLKA:                0   Swapped to CLKB:                0
  Swapped to Processor 1:         0   Swapped to Processor 2:         0
  DRAM Failures:                  0

  Exceptions:                     0

  Last software reset by user: 3/13/2000,17:39:00

  EOBC Exceptions/Hang:            0

Heap Memory Log:
Corrupted Block = none
```

```
NVRAM log:

01. 1/25/2000,17:39:10: convertCiscoMIB:PreSac(0) checksum failed: 0xFFFF(0xE507
)

Module 3 Log:
  Reset Count:   14
  Reset History: Wed Mar 22 2000, 10:35:54
                 Fri Mar 17 2000, 15:36:57
                 Wed Mar 15 2000, 16:54:59
                 Tue Mar 14 2000, 16:02:19

<<<<output truncated >>>>
```

This example shows how to display dump log information:

```
Console> (enable) show log dump
Total logs: 1
Console> (enable)
```

Table 2-38 describes the possible fields in the output from the **show log** command.

Table 2-38 show log Command Output Fields

Field	Description
Network Management Processor (ACTIVE NMP) Log	Log that applies to the NMP on the supervisor engine.
Reset Count	Number of times the system has reset.
Re-boot History	Date and times the system has rebooted.
Bootrom Checksum Failures	Number of bootrom checksum failures.
UART Failures	Number of times the UART has failed.
Flash Checksum Failures	Number of times the Flash Checksum has failed.
Flash Program Failures	Number of times the Flash Program has failed.
Power Supply 1 Failures	Number of times Power Supply 1 has failed.
Power Supply 2 Failures	Number of times Power Supply 2 has failed.
Swapped to CLKA	Number of times a switchover to clock A has occurred.
Swapped to CLKB	Number of times a switchover to clock B has occurred.
Swapped to Processor 1	Number of times a switchover to processor 1 has occurred.
Swapped to Processor 2	Number of times a switchover to processor 2 has occurred.
DRAM Failures	Number of times the DRAM has failed.
Exceptions:	Exceptions log.
Last software reset by user	Date of the last time the software was reset.
NVRAM log	Number of times NVRAM errors have occurred.
Reset Count	Number of times the system has reset.
Reset History	Date and times the system has reset.
Total log	Number of entries.

Related Commands **clear log**

show log command

Use the **show log command** command to display the command log entries.

show log command [*mod*]

Syntax Description

mod	(Optional) Number of the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The command log entry table is a history log of commands input to the switch from the console or Telnet.

Examples

This example shows how to display the command log for a specific module:

```
Console> (enable) show log command 1
 Active Command log:

001. Oct 04 09:44:35 Pid = 86 show mod
002. Oct 04 09:44:55 Pid = 86 clear log command 3
003. Oct 04 10:09:07 Pid = 86 show port membership
004. Oct 04 10:10:15 Pid = 86 en
005. Oct 04 10:10:19 Pid = 86 clear port help
006. Oct 04 10:10:47 Pid = 86 clear spantree help
007. Oct 04 10:12:42 Pid = 86 show
008. Oct 04 10:12:57 Pid = 86 show qos help
009. Oct 04 10:14:46 Pid = 86 show log 5
010. Oct 04 10:14:53 Pid = 86 show log 1
011. Oct 04 10:15:04 Pid = 86 show log command 5
012. Oct 04 10:15:08 Pid = 86 show log command 1

Console> (enable)
```

Related Commands

clear log command

show logging

Use the **show logging** command to display the system message log information.

show logging [**noalias**]

Syntax Description

noalias	(Optional) Keyword to force the display to show IP addresses, not IP aliases.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the default system message log configuration:

```
Console> show logging

Logging buffer size:         500
        timestamp option:    enabled
Logging history size:        1
Logging console:             enabled
Logging telnet:              enabled
Logging server:              disabled
        server facility:     LOCAL7
        server severity:     warnings(4)


Facility            Default Severity         Current Session Severity
-------------       ----------------------   ------------------------
acl                 7                        7
cdp                 6                        6
cops                7                        7
dtp                 7                        7
dvlan               7                        7
earl                7                        7
ethc                7                        7
filesys             7                        7
gvrp                7                        7
ip                  7                        7
kernel              7                        7
ld                  7                        7
mcast               7                        7
mgmt                7                        7
mls                 7                        7
protfilt            7                        7
pruning             7                        7
privatevlan         7                        7
qos                 7                        7
radius              7                        7
rsvp                7                        7
```

```
security            7                    7
snmp                7                    7
spantree            7                    7
sys                 7                    7
tac                 7                    7
tcp                 7                    7
telnet              7                    7
tftp                7                    7
udld                7                    7
vmps                7                    7
vtp                 7                    7


0(emergencies)      1(alerts)            2(critical)
3(errors)           4(warnings)          5(notifications)
6(information)      7(debugging)
Console> (enable)
```

Table 2-39 describes the fields in the **show logging** command output.

Table 2-39 show logging Command Output Fields

Field	Description
Logging buffered size	Size of the logging buffer.
timestamp option	Status of whether the timestamp option is enabled or disabled.
Logging history size	Size of the logging history buffer.
Logging console	Status of whether logging to the console is enabled or disabled.
Logging telnet	Status of whether logging to the Telnet session is enabled or disabled.
Logging server	Status of whether logging to the logging server is enabled or disabled.
Facility	Name of the facility to be logged.
Server/Severity	Severity level at which point an error from that facility is logged.
Current Session Severity	Severity level at which point an error from that facility is logged during the current session.
0 (emergencies), 1 (alerts)...	Key to the numeric severity level codes.

Related Commands

clear logging server
set logging console
set logging history
set logging level
set logging server
set logging session
show logging buffer

show logging buffer

Use the **show logging buffer** command to display system messages from the internal buffer.

show logging buffer [**–**] [*number_of_messages*]

Syntax Description

–	(Optional) Keyword to force the display to show system messages starting from the end of the buffer.
number_of_messages	(Optional) Number of system messages to be displayed; valid values are from **1** to **1023**.

Defaults

The default is –20 messages.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not enter the **–** keyword, system messages are displayed from the beginning of the buffer. If you do not specify the *number_of_messages*, all messages in the buffer are displayed.

Examples

This example shows how to display the first four system messages from the internal buffer:

```
Console> (enable) show logging buffer 4

1999 Dec 28 15:18:21 %SYS-1-SYS_NORMPWRMGMT:System in normal power management on
1999 Dec 28 15:18:24 %SYS-5-MOD_PWRON:Module 2 powered up
1999 Dec 28 15:18:31 %MLS-5-NDEDISABLED:Netflow Data Export disabled
1999 Dec 28 15:18:32 %MLS-5-MCAST_STATUS:IP Multicast Multilayer Switching is ed
Console> (enable)
```

This example shows how to display the last four system messages from the internal buffer:

```
Console> (enable) show logging buffer -4
1999 Dec 28 15:18:32 %MLS-5-MCAST_STATUS:IP Multicast Multilayer Switching is ed
1999 Dec 28 15:18:32 %SYS-5-MOD_OK:Module 1 is online
1999 Dec 28 15:19:07 %SYS-5-MOD_OK:Module 2 is online
1999 Dec 28 15:19:27 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1
Console> (enable)
```

Related Commands

clear logging buffer
set logging buffer

show mac

Use the **show mac** command to display MAC counters.

show mac [**utilization**] [*mod*[/*port*]]

Syntax Description

utilization	(Optional) Keyword to display approximated packet and byte rates.
mod/[/*port*]	(Optional) Number of the module and optionally, the number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The **utilization** keyword is not supported on ATM ports.

If you do not specify a module number, all modules are shown. If you do not specify a port number, all ports are shown.

The Out-Discards field displays the number of outbound packets chosen to be discarded even though no errors had been detected to prevent being transmitted. For example, an outbound link is overwhelmed by switch traffic. Packets dropped are the ones destined for that port, but the port could not accept those packets due to XMT buffer overflow.

The Xmit-Packet-Rate, Xmit-Octet-Rate, Rcv-Packet-Rate, and Rcv-Octet-Rate fields display approximated average utilization rates rather than exact values. The approximated average is based on the previous approximation values, the last counter values read from hardware, the load time interval (fixed at 5 minutes), and the polling interval.

Examples

This example shows how to display MAC information for port 1 on module 3:

```
Console> show mac 3/1

Port     Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast
-------- -------------------- -------------------- --------------------
 3/1                        0                22636                    1

Port     Xmit-Unicast         Xmit-Multicast       Xmit-Broadcast
-------- -------------------- -------------------- --------------------
 3/1                     3690              1888064               305202

Port     Rcv-Octet            Xmit-Octet
-------- -------------------- --------------------
 3/1                  9310072            162180717

MAC      Dely-Exced MTU-Exced  In-Discard Out-Discard
```

```
-------- ---------- ---------- ---------- -----------
 3/1              0          0          0           0

Port  Last-Time-Cleared
----- -------------------------
 3/1  Wed Jan 14 2004, 07:59:35
Console>
```

This command shows how to display approximated packet and byte rates:

```
Console> (enable) show mac utilization 1
5 min input/output port rates:

Port  Xmit-Packet-Rate     Xmit-Octet-Rate
----- -------------------- --------------------
1/1                  1343               123432
1/2                  2342               232343
Port  Rcv-Packet-Rate      Rcv-Octet-Rate
----- -------------------- --------------------
1/1                  1324               143253
1/2                  2234               253234
Console> (enable)
```

Table 2-40 describes the possible fields in the **show mac** command output.

Table 2-40 show mac Command Output Fields

Field	Description
MAC	Module and port.
Rcv-Frms	Frames received on the port.
Xmit-Frms	Frames transmitted on the port.
Rcv-Broad	Broadcast frames received on the port.
Xmit-Broad	Broadcast frames transmitted on the port.
Dely-Exced	Total transmit frames aborted due to excessive deferral.
MTU-Exced	Frames for which the MTU size was exceeded.
In-Discard	Incoming frames that were discarded because the frame did not need to be switched.
Out-Discard	Number of outbound packets chosen to be discarded even though no errors had been detected to prevent their being transmitted.
Curr-Path	Current path used (primary or secondary).
TVX	Value of the valid transmission timer.
Upstream-Nbr	MAC address of the current upstream neighbor.
Downstream-Nbr	MAC address of the current downstream neighbor.
Old-Upstrm-Nbr	MAC address of the previous upstream neighbor.
Old-Downstrm-Nbr	MAC address of the previous downstream neighbor.
Rcv-Smt	Number of SMT frames received by the port.
Xmit-Smt	Number of SMT frames transmitted by the port.
Rcv-llc	Number of NLLC frames received by the port.
Xmit-llc	Number of LLC frames transmitted by the port.

Table 2-40 show mac Command Output Fields (continued)

Field	Description
Rcv-Octet	Number of octet frames received on the port.
Xmit-Octet	Number of octet frames transmitted on the port.
Rcv-Unicast	Number of unicast frames received on the port.
Rcv-Broadcast	Number of broadcast frames received on the port.
Xmit-Unicast	Number of unicast frames transmitted on the port.
Xmit-Broadcast	Number of broadcast frames transmitted on the port.
Tvx-Exp-Ct	Number of times the TVX timer expired.
MAC Last-Time-Cleared	Module and port number and the date and time of the last time the software counters are cleared on this MAC.
Xmit-Packet-Rate	Number of packets transmitted.
Xmit-Octet-Rate	Number of bytes transmitted.
Rcv-Packet-Rate	Number of packets received.
Rcv-Octet-Rate	Number of bytes received.

show microcode

Use the **show microcode** command to display the version of the microcode and the module version information.

show microcode

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the **show microcode** output for a supervisor engine:

```
Console> show microcode
Bundled Images  Version              Size    Built
--------------- -------------------- ------- -----------------
LCP SLCP        4.2(0.24)VAI58        302506 12/03/98 03:51:46
LCP LX1000      4.2(0.24)VAI58        288508 12/03/98 03:53:12
LCP LX10100     4.2(0.24)VAI58        379810 12/03/98 03:52:33
```

Table 2-41 describes possible fields in the **show microcode** command output.

Table 2-41 show microcode Command Output Fields

Field	Description
Bundled Images	Name of the bundled image.
Version	Version of the image.
Size	Size of the image.
Built	Date image was built.

show mls

Use the **show mls** command to display MLS Layer 3 packet information in the MLS-based Catalyst 6000 family switches.

show mls [**ip** | **ipx**] [*mod*]

Syntax Description

ip	(Optional) Keyword to specify IP MLS.
ipx	(Optional) Keyword to specify IPX MLS.
mod	(Optional) Number of the MSFC; valid values are **15** and **16**.

Defaults

The default displays both IP and IPX MLS information.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you enter any of the **show mls** commands on Catalyst 6000 family switches without IP or IPX MLS, one of these warning messages display:

```
Multilayer switching not supported on feature card.
```

or

```
IPX Multilayer switching not supported on feature card.
```

If you place the MSFC on a supervisor engine installed in slot 1, then the MSFC is recognized as module 15. If you install the supervisor engine in slot 2, the MSFC is recognized as module 16.

This command is not supported on switches configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2).

Examples

These examples show the display if you enter the **show mls** commands on a switch configured with the Supervisor Engine 1 with Layer 3 Switching Engine WS-F6K-PFC:

```
Console> (enable) show mls
Total Active MLS entries = 0
Total packets switched = 0
IP Multilayer switching enabled
IP Multilayer switching aging time = 256 seconds
IP Multilayer switching fast aging time = 0 seconds, packet threshold = 0
IP Flow mask: Full Flow
Configured flow mask is Destination flow
Active IP MLS entries = 0
Netflow Data Export version: 8
Netflow Data Export disabled
Netflow Data Export port/host is not configured
Total packets exported = 0
```

```
MSFC ID         Module XTAG MAC               Vlans
--------------- ------ ---- ----------------- --------------------
52.0.03         15     1    01-10-29-8a-0c-00 1,10,123,434,121
                                              222,666,959
IPX Multilayer switching enabled
IPX Multilayer switching aging time = 256 seconds
IPX Flow mask: Full Flow
Active IPX MLS entries = 0

MSFC ID         Module XTAG MAC               Vlans
--------------- ------ ---- ----------------- --------------------
52.0.0.3        16     1    00-10-29-8a-0c-00 1,10

Console> (enable)

Console> (enable) show mls ipx
IPX Multilayer switching disabled
IPX Multilayer switching aging time = 256 seconds
IPX flow mask is Destination flow
IPX max hop is 16
Active IPX MLS entries = 0

IPX MLS-RP IP    MLS-RP ID    XTAG MLS-RP MAC-Vlans
---------------- ------------ ---- --------------------------------
22.1.0.55        00906dfc5800    5 00-10-07-38-29-17  2-15,66,77,88,99
                                   00-90-6d-fc-58-00  20-21
MSFC ID         Module XTAG MAC               Vlans
--------------- ------ ---- ----------------- --------------------
52.0.0.3        16     1    00-10-29-8a-0c-00 1,10

Console> (enable)
```

Related Commands

- clear mls statistics entry
- set mls agingtime
- set mls cef load-balance
- set mls exclude protocol
- set mls nde
- set mls statistics protocol

show mls acl-route

Use the **show mls acl-route** command to display summaries from ACL for routing in the MLS-based Catalyst 6000 family switches.

show mls acl-route

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This command is supported on Catalyst 6000 family switches configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) only.

If you enter any of the **show mls** commands on Catalyst 6000 family switches without IP or IPX MLS, one of these warning messages display:

```
Multilayer switching not supported on feature card.
```

or

```
IPX Multilayer switching not supported on feature card.
```

Examples

This example shows how to display summaries from ACL for routing:

```
Console> show mls acl-route
Total L3 packets forwarded      0
Total L3 octets forwarded       0
Total routed VLANs              0
Total used adjacency entries    0
Console>
```

Related Commands

show mls

show mls cef interface

Use the **show mls cef interface** command to display MSFC VLAN information.

show mls cef interface [*vlan*]

Syntax Description

vlan	(Optional) Number of the VLAN; valid values are from **1** to **4094**.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This command is supported on Catalyst 6000 family switches configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) only.

Examples

This example shows how to display CEF interfaces:

```
Console> (enable) show mls cef interface
Module 16: vlan 1, IP Address 21.0.0.194, Netmask 255.0.0.0
  MTU = 1500, State = up, ICMP-Unreach = enabled, ICMP-Redirect = enabled
  Unicast RPF = disabled
Module 16: vlan 43, IP Address 43.0.0.99, Netmask 255.0.0.0
  MTU = 1500, State = down, ICMP-Unreach = disabled, ICMP-Redirect = disabled
  Unicast RPF = disabled
Module 16: vlan 44, IP Address 44.0.0.99, Netmask 255.0.0.0
  MTU = 1500, State = down, ICMP-Unreach = disabled, ICMP-Redirect = disabled
  Unicast RPF = disabled
Module 16: vlan 45, IP Address 45.0.0.99, Netmask 255.0.0.0
  MTU = 1500, State = up, ICMP-Unreach = enabled, ICMP-Redirect = enabled
  Unicast RPF = disabled
Module 16: vlan 46, IP Address 46.0.0.99, Netmask 255.0.0.0
  MTU = 1500, State = up, ICMP-Unreach = enabled, ICMP-Redirect = enabled
  Unicast RPF = disabled
Module 16: vlan 47, IP Address 47.0.0.99, Netmask 255.0.0.0
  MTU = 1500, State = down, ICMP-Unreach = disabled, ICMP-Redirect = disabled
  Unicast RPF = disabled
Module 16: vlan 48, IP Address 48.0.0.99, Netmask 255.0.0.0
  MTU = 1500, State = down, ICMP-Unreach = disabled, ICMP-Redirect = disabled
  Unicast RPF = disabled
Module 16: vlan 49, IP Address 0.0.0.0, Netmask 0.0.0.0
  MTU = 1500, State = down, ICMP-Unreach = disabled, ICMP-Redirect = disabled
  Unicast RPF = disabled

Console> (enable)
```

This example show how to display information for a specific CEF VLAN:

```
Console> (enable) show mls cef interface 46
Module 16: vlan 46, IP Address 46.0.0.99, Netmask 255.0.0.0
  MTU = 1500, State = up, ICMP-Unreach = enabled, ICMP-Redirect = enabled
  Unicast RPF = disabled

Console> (enable)
```

Table 2-42 describes the possible fields in the **show mls cef interface** command output.

Table 2-42 show mls cef interface Command Output Fields

Field	Description
Vlan	VLAN associated with the interface.
IP Address	IP address associated with the interface.
Netmask	IP network mask associated with the interface.
MTU	IP MTU associated with the interface.
State	Interface state (up or down).
ICMP-Unreach	Status of whether denied Layer 3 packets will be bridged to MSFC to generate ICMP unreachable.
ICMP-Redirect	Status of whether Layer 3 packets whose destination VLAN is equal to the source VLAN should be redirected to the MSFC to generate ICMP redirect.
Unicast RPF	Unicast RPF enable/disable.

Related Commands

clear mls cef
show mls cef mac
show mls cef summary
show mls entry cef

show mls cef mac

Use the **show mls cef mac** command to display BIA physical MAC and HSRP active virtual MACs associated with the designated MSFC2.

show mls cef mac

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This command is supported on Catalyst 6000 family switches configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) only.

If the MSFC2 has any HSRP MAC addresses configured on one or more VLANs and these interfaces are HSRP ACTIVE (for example, not standby), these will also be displayed in the command output. For example:

```
Console> show mls cef mac
Module 16:Physical MAC-Address 00-01-97-34-2b-fd
Vlan Virtual MAC-Address(es)
---- ------------------------
   1 00-00-0c-07-ac-00
  20 00-00-0c-07-ac-00
```

You will only see the virtual MAC addresses if those interfaces on the designated MSFC2 that have HSRP configured are HSRP ACTIVE and not STANDBY.

Examples

This example shows how to display the MAC address associated with the designated MSFC2:

```
Console> (enable) show mls cef mac
Module 16: Physical MAC-Address 00-01-97-36-1b-fd

Console> (enable)
```

Related Commands

clear mls cef
show mls cef interface
show mls cef summary
show mls entry cef

show mls cef summary

Use the **show mls cef summary** command to display a summary of CEF table information.

show mls cef summary

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This command is supported on Catalyst 6000 family switches configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) only.

Examples

This example shows how to display CEF information:

```
Console> (enable) show mls cef summary
Total L3 packets switched:                    0
Total L3 octets switched:                     0
Total route entries:                         10
   IP route entries:                          9
   IPX route entries:                         1
   IPM route entries:                         0
IP load sharing entries:                      0
IPX load sharing entries:                     0
Forwarding entries:                           1
Bridge entries:                               6
Drop entries:                                 3
Console> (enable)
```

Table 2-43 describes the possible fields in the **show mls cef summary** command output.

Table 2-43 show mls cef summary Command Output Fields

Field	Description
Total L3 packets forwarded	Number of Layer 3 packets forwarded by the CEF engine.
Total L3 octets forwarded	Number of Layer 3 octets forwarded by the CEF engine.
Total route entries	Number of route entries.
IP route entries	Number of IP route entries.

Table 2-43 show mls cef summary Command Output Fields (continued)

Field	Description
IPX route entries	Number of IPX route entries.
IP load sharing entries	Number of load-sharing entries.
IPX load sharing entries	Number of load-sharing entries.
Forwarding entries	Number of forwarding entries.
Bridge entries	Number of bridge entries.
Drop entries	Number of incomplete entries (no adjacency information).

Related Commands

clear mls cef
show mls cef interface
show mls cef mac
show mls entry cef

show mls entry

Use the **show mls entry** command to display state information in the MLS-based Catalyst 6000 family switches.

show mls entry [*mod*] [**short** | **long**]

show mls entry ip [*mod*] [**destination** *ip_addr_spec*] [**source** *ip_addr_spec*] [**protocol** *protocol*] [**src-port** *src_port*] [**dst-port** *dst_port*] [**short** | **long**]

show mls entry ipx [*mod*] [**destination** *ipx_addr_spec*] [**short** | **long**]

show mls entry qos

Syntax Description

mod	(Optional) MSFC module number; valid values are **15** or **16**.
short	(Optional) Keyword to display the output with carriage returns.
long	(Optional) Keyword to display the output on one line.
ip	Keyword to specify IP MLS.
destination	(Optional) Keyword to specify the destination IP or IPX address.
ip_addr_spec	(Optional) Full IP address or a subnet address.
source	(Optional) Keyword to specify the source IP or IPX address.
protocol	(Optional) Keyword to specify the protocol type.
protocol	(Optional) Protocol type; valid values can be **0**, **tcp**, **udp**, **icmp**, or a decimal number for other protocol families. **0** indicates "do not care."
src-port *src_port*	(Optional) Keyword and variable to specify the number of the TCP/UDP source port (decimal). Used with **dst-port** to specify the port pair if the protocol is **tcp** or **udp**. **0** indicates "do not care."
dst-port *dst_port*	(Optional) Keyword and variable to specify the number of the TCP/UDP destination port (decimal). Used with **src-port** to specify the port pair if the protocol is **tcp** or **udp**. **0** indicates "do not care."
ipx	Keyword to specify IPX MLS.
ipx_addr_spec	(Optional) Full IPX address or a subnet address.
qos	Keyword to specify QoS.

Defaults

The default displays MLS information in long format.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

On switches configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2), the display contains summaries derived from three forwarding sources: FIB for routing, the NetFlow table for statistics, and ACL TCAM for policy-based routing.

The *mod* variable and the **ip**, **ipx**, **long**, and **short** keywords are not supported on switches configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2).

If you use the **ip** keyword, you are specifying a command for IP MLS. If you use the **ipx** keyword, you are specifying a command for IPX MLS.

When entering the *ip_addr_spec*, use the full IP address or a subnet address in one of the following formats: *ip_addr*, *ip_addr/netmask,* or *ip_addr/maskbit*.

When entering the *ipx_addr_spec*, use the full IP address or a subnet address in one of the following formats: *src_net/*[*mask*], *dest_net.dest_node*, or *dest_net/mask*.

If you enter any **show mls** command on Catalyst 6000 family switches without IP MLS, this warning message displays:

```
Multilayer switching not supported on feature card.
```

If you enter any **show mls** command on Catalyst 6000 family switches without IPX MLS, this warning message displays:

```
IPX Multilayer switching not supported on feature card.
```

If you enter the **show mls** command with no arguments, general IP MLS information and all IP MLS-RP information displays.

A value 0 for *src_port* and *dst_port* means "don't care."

Entering the **destination** keyword specifies the entries matching the destination IP address specification, entering the **source** keyword specifies the entries matching the source IP address specification, and entering an *ip_addr_spec* can specify a full IP address or a subnet address. If you do not specify a keyword, it is treated as a wildcard, and all entries are displayed.

Use the following syntax to specify an IP subnet address:

- *ip_subnet_addr*—This is the 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 with a length of 8, 16, or 24 bits.
- *ip_addr/subnet_mask*—This is the 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* is allowed to be a full host address, such as 172.22.253.1/255.255.252.00.
- *ip_addr/maskbits*—This is the 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* is allowed to be a full host address, such as 172.22.254.1/22, which has the same subnet address as 172.22.252.00/72.

The [**long** | **short**] option gives the flexibility to display the output in regular (80 characters in width) or wide screen.

Dashes may be displayed for some fields if the fields are not applicable to the type of flow mask.

If you place the MSFC on a supervisor engine installed in slot 1, then the MSFC is recognized as module 15. If you install the supervisor engine in slot 2, the MSFC is recognized as module 16.

Examples

Note The examples shown for the **show mls entry** commands are displayed in short format. The display in the long form exceeds the page width and cannot be shown.

These examples show the display if you enter the **show mls entry** commands on a switch configured with the Supervisor Engine 1 with Layer 3 Switching Engine WS-F6K-PFC:

```
Console> (enable) show mls entry short
Destination-IP  Source-IP       Prot  DstPrt SrcPrt Destination-Mac   Vlan ---------------
--------------- ----- ------ ------ ----------------- ----
 ESrc EDst SPort DPort Stat-Pkts Stat-Byte   Uptime   Age
 ---- ---- ----- ----- ---------- --------- --------
171.69.200.234  171.69.192.41   TCP*  6000   59181  00-60-70-6c-fc-22 4
 ARPA SNAP 5/8   11/1  3152      347854       09:01:19 09:08:20
171.69.1.133    171.69.192.42   UDP   2049   41636  00-60-70-6c-fc-23 2
 SNAP ARPA 5/8   1/1   2345      123456       09:03:32 09:08:12

Total IP entries: 2

Destination-IPX           Source-IPX-net Destination-Mac   Vlan Port
------------------------- -------------- ----------------- ---- -----
 Stat-Pkts Stat-Bytes
 --------- -----------
BABE.0000.0000.0001       -              00-a0-c9-0a-89-1d 211  13/37 30230     1510775
201.00A0.2451.7423        -               00-a0-24-51-74-23 201  14/33
 30256     31795084
501.0000.3100.0501        -               31-00-05-01-00-00 501  9/37
 12121     323232
401.0000.0000.0401        -               00-00-04-01-00-00 401  3/1
 4633      38676

Total IPX entries: 4
Console> (enable)
```

For full flow:

```
Console> (enable) show mls entry ip short
Destination-IP  Source-IP       Prot  DstPrt SrcPrt Destination-Mac
Vlan --------------- --------------- ----- ------ ------
----------------- ----
EDst ESrc DPort SPort Stat-Pkts Stat-Byte   Uptime   Age
---- ---- ----- ----- ---------- --------- --------
MSFC 127.0.0.24 (module 16):
171.69.200.234  171.69.192.41   TCP*  6000   59181  00-60-70-6c-fc-22 4
ARPA SNAP 5/8   11/1  3152 347854       09:01:19 09:08:20
171.69.1.133    171.69.192.42   UDP   2049   41636  00-60-70-6c-fc-23 2
SNAP ARPA 5/8   1/1   2345 123456       09:03:32 09:08:12

Total Entries:2
* indicates TCP flow has ended
Console> (enable)
```

For destination-only flow:

```
Console> (enable) show mls entry ip short
Destination-IP  Source-IP       Prot  DstPrt SrcPrt Destination-Mac   Vlan ---------------
--------------- ----- ------ ------ ----------------- ----
 ESrc EDst SPort DPort Stat-Pkts Stat-Byte   Uptime   Age
 ---- ---- ----- ----- ---------- --------- --------
MSFC 127.0.0.24 (module 16):
171.69.200.234  -               -     -      -      00-60-70-6c-fc-22 4
```

```
 ARPA SNAP 5/8   11/1  3152 347854       09:01:19 09:08:20
171.69.1.133    -               -     -       -      00-60-70-6c-fc-23 2
 SNAP ARPA 5/8   1/1   2345 123456       09:03:32 09:08:12

Total Entries: 2
* indicates TCP flow has ended
Console> (enable)
```

For destination-source flow:

```
Console> (enable) show mls entry ip 16 short
Destination-IP  Source-IP       Prot  DstPrt SrcPrt Destination-Mac   Vlan ESrc EDst
Destination-IP  Source-IP      Prot  DstPrt SrcPrt Destination-Mac   Vlan ---------------
--------------- ----- ------ ------ ----------------- ----
 ESrc EDst SPort DPort Stat-Pkts Stat-Byte   Uptime   Age
 ---- ---- ----- ----- --------------------- -------- --------
MSFC 127.0.0.24 (module 16):
171.69.200.234  171.69.192.41   -     -       -      00-60-70-6c-fc-22 4
 ARPA SNAP 5/8   11/1  3152      347854       09:01:19 09:08:20
171.69.1.133    171.69.192.42   -     -       -      00-60-70-6c-fc-23 2
 SNAP ARPA 5/8   1/1   2345      123456       09:03:32 09:08:12

Total Entries: 2
* indicates TCP flow has ended
Console> (enable)
```

For destination-source:

```
Console> (enable) show mls entry ipx short
Destination-IPX           Source-IPX-net Destination-Mac   Vlan Port
------------------------- -------------- ----------------- ---- -----
 Stat-Pkts Stat-Bytes
 --------- -----------
MSFC 127.0.0.22 (Module 15):
201.00A0.2451.7423        1.0002         00-a0-24-51-74-23 201  14/33
 30256     31795084
501.0000.3100.0501        1.0003         31-00-05-01-00-00 501  9/37
 12121     323232

Total entries: 0
Console> (enable)
```

Destination-only flow:

```
Console> (enable) show mls entry ipx short
Destination-IPX           Source-IPX-net Destination-Mac   Vlan Port
------------------------- -------------- ----------------- ---- -----
 Stat-Pkts Stat-Bytes
 --------- -----------
MSFC 127.0.0.24 (module 16):
BABE.0000.0000.0001       -              00-a0-c9-0a-89-1d 211  13/37
 30230     1510775
201.00A0.2451.7423        -              00-a0-24-51-74-23 201  14/33
 30256     31795084
501.0000.3100.0501        -              31-00-05-01-00-00 501  9/37
 12121     323232
401.0000.0000.0401        -              00-00-04-01-00-00 401  3/1
 4633      38676

Total entries: 4
Console> (enable)
```

```
Console> (enable) show mls entry ipx 16 short
Destination-IPX           Source-IPX-net Destination-Mac   Vlan Port
------------------------ -------------- ----------------- ---- -----
 Stat-Pkts Stat-Bytes
 --------- -----------
MSFC 127.0.0.22 (Module 16):
501.0000.3100.0501        -              31-00-05-01-00-00 501  9/37
 12121     323232
401.0000.0000.0401        -              00-00-04-01-00-00 401  3/1
 4633      38676
Console> (enable)
```

These examples show the display if you enter the **show mls entry** commands on a switch configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2):

```
Console> (enable) show mls entry
Mod FIB-Type  Destination-IP  Destination-Mask NextHop-IP      Weight
--- --------- --------------- ---------------- --------------- ------
 15 receive   0.0.0.0         255.255.255.255
 15 receive   255.255.255.255 255.255.255.255
 15 receive   127.0.0.12      255.255.255.255
 16 receive   127.0.0.0       255.255.255.255
 16 receive   127.255.255.255 255.255.255.255
 15 resolved  127.0.0.11      255.255.255.255  127.0.0.11           1
 15 receive   21.2.0.4        255.255.255.255
 16 receive   21.0.0.0        255.255.255.255
 16 receive   21.255.255.255  255.255.255.255
 15 receive   44.0.0.1        255.255.255.255
 16 receive   44.0.0.0        255.255.255.255
 16 receive   44.255.255.255  255.255.255.255
 15 receive   42.0.0.1        255.255.255.255
 16 receive   42.0.0.0        255.255.255.255
 16 receive   42.255.255.255  255.255.255.255
 15 receive   43.0.0.99       255.255.255.255
 15 receive   43.0.0.0        255.255.255.255
 15 receive   43.255.255.255  255.255.255.255
 15 receive   192.20.20.20    255.255.255.255
 16 receive   21.2.0.5        255.255.255.255
 16 receive   42.0.0.20       255.255.255.255
 15 connected 43.0.0.0        255.0.0.0
 15 drop      224.0.0.0       240.0.0.0
 15 wildcard  0.0.0.0         0.0.0.0

Mod FIB-Type  Dest-IPX-net NextHop-IPX               Weight
--- --------- ------------ ------------------------ ------
 15 connected 21
 15 connected 44
 15 connected 42
 15 resolved  450          42.0050.3EA9.ABFD              1
 15 resolved  480          42.0050.3EA9.ABFD              1
 15 wildcard  0

Destination-IP  Source-IP      Prot  DstPrt SrcPrt Destination-Mac   Vlan EDst Stat-Pkts  Stat-Bytes  Uptime
Age      TcpDltSeq TcpDltAck
--------------- --------------- ----- ------ ------ ----------------- ---- ---- ---------- -----------
-------- -------- --------- ---------
0.0.0.5         0.0.0.5         5     204    104    cc-cc-cc-cc-cc-cc 5    ARPA 0          0
01:03:18 01:00:51 cccccccc  cccccccc
0.0.0.2         0.0.0.2         2     201    101    cc-cc-cc-cc-cc-cc 2    ARPA 0          0
01:03:21 01:00:51 cccccccc  cccccccc
0.0.0.4         0.0.0.4         4     203    X      cc-cc-cc-cc-cc-cc 4    ARPA 0          0
01:03:19 01:00:51 cccccccc  cccccccc
0.0.0.1         0.0.0.1         ICMP  200    100    cc-cc-cc-cc-cc-cc 1    ARPA 0          0
01:03:25 01:00:52 cccccccc  cccccccc
```

```
0.0.0.3         0.0.0.3         3     202    102    cc-cc-cc-cc-cc-cc 3    ARPA 0          0
01:03:20 01:00:52 cccccccc  cccccccc
0.0.0.6         0.0.0.6         TCP   205    105    cc-cc-cc-cc-cc-cc 6    ARPA 0          0
01:03:18 01:00:52 cccccccc  cccccccc
Console> (enable)

Console> (enable) show mls entry qos
Warning: QoS is disabled.
Destination-IP  Source-IP       Prot  DstPrt SrcPrt Stat-Pkts  Stat-Bytes  Excd-
Pkts  Stat-Bkts  Uptime   Age
--------------- --------------- ----- ------ ------ ---------- ----------- -----
----- ---------- -------- --------
MSFC 0.0.0.0 (Module 16):

Console> (enable)
```

Related Commands clear mls statistics entry

show mls entry cef

Use the **show mls entry cef** command to display CEF and adjacency entries (and Tx statistics) for IP resolved entries and IPX resolved or connected entries.

show mls entry cef [**adjacency**]

show mls entry cef [**short** | **long**]

show mls entry cef ip [[*ip_addr*/]*mask_len*] [**adjacency**]

show mls entry cef ipx [[*ipx_addr*/]*mask_len*] [**adjacency**]

Syntax Description

adjacency	(Optional) Keyword to display adjacency information.
short	(Optional) Keyword to display the output with carriage returns.
long	(Optional) Keyword to display the output on one line.
ip	Keyword to specify IP entries.
ipx	Keyword to specify IPX entries.
ip_addr	(Optional) IP address of the entry.
mask_len	(Optional) Mask length associated with the IP or IPX address of the entry; valid values are from **0** to **32**.
ipx_addr	(Optional) IPX address of the entry.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This command is supported on Catalyst 6000 family switches configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) only.

In the NextHop-IP field, the ouput may actually be set to “point2point” if the next hop is a point-to-point WAN interface.

When you enter the **show mls entry cef adjacency** command, only adjacency information for those IP or IPX CEF entries that are of type resolved, wildcard, or default are displayed.

Examples

This example shows how to display information for all CEF entries:

```
Console> (enable) show mls entry cef
Mod FIB-Type  Destination-IP  Destination-Mask NextHop-IP      Weight
--- --------- --------------- ---------------- --------------- ------
 16 receive   0.0.0.0         255.255.255.255
 16 receive   255.255.255.255 255.255.255.255
 16 resolved  127.0.0.21      255.255.255.255  127.0.0.21           1
 16 receive   21.0.0.194      255.255.255.255
 16 receive   45.0.0.99       255.255.255.255
 16 receive   46.0.0.99       255.255.255.255
 16 resolved  46.0.0.10       255.255.255.255  46.0.0.10            1
 16 resolved  46.0.0.9        255.255.255.255  46.0.0.9             1
 16 resolved  46.0.0.4        255.255.255.255  46.0.0.4             1
 16 resolved  46.0.0.1        255.255.255.255  46.0.0.1             1
 16 resolved  46.0.0.2        255.255.255.255  46.0.0.2             1
 16 resolved  46.0.0.3        255.255.255.255  46.0.0.3             1
 16 resolved  46.0.0.5        255.255.255.255  46.0.0.5             1
 16 resolved  46.0.0.6        255.255.255.255  46.0.0.6             1
 16 resolved  46.0.0.7        255.255.255.255  46.0.0.7             1
 16 resolved  46.0.0.8        255.255.255.255  46.0.0.8             1
 16 receive   224.0.0.0       255.255.255.0
 16 connected 21.0.0.0        255.0.0.0
 16 connected 45.0.0.0        255.0.0.0
 16 connected 46.0.0.0        255.0.0.0
 16 drop      224.0.0.0       240.0.0.0
 16 wildcard  0.0.0.0         0.0.0.0

Mod FIB-Type  Dest-IPX-net NextHop-IPX               Weight
--- --------- ------------ ------------------------ ------
 16 connected abcd
 16 connected defa
 16 resolved  fade         defa.000A.0203.0405           1
 16 wildcard  0
Console> (enable)
```

These examples show how to display information for a specific entry type:

```
Console> (enable) show mls entry cef ip
Mod FIB-Type  Destination-IP  Destination-Mask NextHop-IP      Weight
--- --------- --------------- ---------------- --------------- ------
 16 receive   0.0.0.0         255.255.255.255
 16 receive   255.255.255.255 255.255.255.255
 16 receive   127.0.0.22      255.255.255.255
 16 receive   127.0.0.0       255.255.255.255
 16 receive   127.255.255.255 255.255.255.255
 16 resolved  21.0.0.1        255.255.255.255  21.0.0.1             1
 16 receive   21.0.0.194      255.255.255.255
 16 receive   21.0.0.0        255.255.255.255
 16 receive   21.255.255.255  255.255.255.255
 16 resolved  127.0.0.21      255.255.255.255  127.0.0.21           1
 16 receive   224.0.0.0       255.255.255.0
.
.
.
Console> (enable) show mls entry cef ipx
Mod FIB-Type  Dest-IPX-net NextHop-IPX               Weight
--- --------- ------------ ------------------------ ------
 16 connected fadeface
 16 resolved  abcd         fadeface.0001.0203.0405       1
 16 wildcard  0
```

This example shows how to display adjacency information:

```
Console> (enable) show mls entry cef ip adjacency
Mod:                16
Destination-IP:     127.0.0.21         Destination-Mask:   255.255.255.255
FIB-Type:           resolved

AdjType  NextHop-IP      NextHop-Mac       Vlan Encp Tx-Packets   Tx-Octets
-------- --------------- ----------------- ---- ---- ------------ -------------
connect  127.0.0.21      00-00-12-00-00-00    0 ARPA            0             0

Mod:                16
Destination-IP:     46.0.0.10          Destination-Mask:   255.255.255.255
FIB-Type:           resolved

AdjType  NextHop-IP      NextHop-Mac       Vlan Encp Tx-Packets   Tx-Octets
-------- --------------- ----------------- ---- ---- ------------ -------------
connect  46.0.0.10       00-00-0c-42-00-0a   46 ARPA      4889030     224895380
Console> (enable)
```

Table 2-44 describes the possible fields in the **show mls entry cef** command output.

Table 2-44 show mls entry cef Command Output Fields

Field	Description
Mod	MSFC module number
Destination-IP Destination-IPX	Destination address (IP address or IPX network)
Destination-Mask	Destination mask
FIB-Type	FIB entry types are as follows: • receive—Prefix associated with an MSFC interface • connected—Prefix associated with a connected network • resolved—Prefix associated with a valid next-hop address • drop—Drop packets associated with this prefix • wildcard—Match-all entry (drop or MSFC redirect) • default—Default route (wildcard will point to default route)
NextHop-IP NextHop-IPX	Next-hop address (IP address or IPX network)
Weight	Next-hop load-sharing weight
AdjType	Adjacency types are as follows: • connect—Complete rewrite information • drop, null, loopbk—Drop adjacency • frc drp—Drop adjacency due to ARP throttling • punt—Redirect to MSFC for further processing • no r/w—Redirect to MSFC because rewrite is incomplete
NextHop-Mac	Next-hop destination MAC address
Vlan	Next-hop destination VLAN

Table 2-44 show mls entry cef Command Output Fields (continued)

Field	Description
Encp	Next-hop destination encapsulation type (ARPA, RAW, SAP, and SNAP)
Tx-Packets	Number of packets transmitted to this adjacency
Tx-Octets	Number of bytes transmitted to this adjacency

Related Commands

clear mls cef
clear mls entry cef adjacency
show mls cef interface
show mls cef mac
show mls cef summary

show mls entry netflow-route

Use the **show mls entry netflow-route** command to display shortcut information in the MLS-based Catalyst 6000 family switches.

show mls entry netflow-route [**short** | **long**]

show mls entry netflow-route ip [**destination** *ip_addr_spec*] [**source** *ip_addr_spec*] [**protocol** *protocol*] [**src-port** *src_port*] [**dst-port** *dst_port*] [**short** | **long**]

Syntax Description

short	(Optional) Keyword to display the output with carriage returns.
long	(Optional) Keyword to display the output on one line.
ip	Keyword to specify IP MLS.
destination	(Optional) Keyword to specify the destination IP or IPX address.
ip_addr_spec	(Optional) Full IP address or a subnet address.
source	(Optional) Keyword to specify the source IP or IPX address.
protocol	(Optional) Keyword to specify the protocol type.
protocol	(Optional) Protocol type; valid values can be **0**, **tcp**, **udp**, **icmp**, or a decimal number for other protocol families. **0** indicates "do not care."
src-port *src_port*	(Optional) Keyword and variable to specify the number of the TCP/UDP source port (decimal). Used with **dst-port** to specify the port pair if the protocol is **tcp** or **udp**. **0** indicates "do not care."
dst-port *dst_port*	(Optional) Keyword and variable to specify the number of the TCP/UDP destination port (decimal). Used with **src-port** to specify the port pair if the protocol is **tcp** or **udp**. **0** indicates "do not care."

Defaults

The default displays MLS information in long format.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This command is supported on Catalyst 6000 family switches configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) only.

The **show mls entry netflow-route** command output displays software-installed NetFlow forwarding entries (these are used for features such as TCP intercept or reflexive ACL), but does not display flow statistics for flows that are switched via CEF entries.

If you use the **ip** keyword, you are specifying a command for IP MLS.

When entering the *ip_addr_spec*, use the full IP address or a subnet address in one of the following formats: *ip_addr*, *ip_addr/netmask*, or *ip_addr/maskbit*.

Entering the **destination** keyword specifies the entries matching the destination IP address specification, entering the **source** keyword specifies the entries matching the source IP address specification, and entering an *ip_addr_spec* can specify a full IP address or a subnet address. If you do not specify a keyword, it is treated as a wildcard, and all entries are displayed.

Use the following syntax to specify an IP subnet address:

- *ip_subnet_addr*—This is the 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 with a length of 8, 16, or 24 bits.
- *ip_addr/subnet_mask*—This is the 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* is allowed to be a full host address, such as 172.22.253.1/255.255.252.00.
- *ip_addr/maskbits*—This is the 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* is allowed to be a full host address, such as 172.22.254.1/22, which has the same subnet address as 172.22.252.00/72.

The [**long** | **short**] option gives the flexibility to display the output in regular (80 characters in width) or wide screen.

Dashes may be displayed for some fields if the fields are not applicable to the type of flow mask.

If you place the MSFC on a supervisor engine installed in slot 1, then the MSFC is recognized as module 15. If you install the supervisor engine in slot 2, the MSFC is recognized as module 16.

Examples

Note The example below is displayed in short format. The display in the long form exceeds the page width and cannot be shown.

```
Console> show mls entry netflow-route short
Destination-IP  Source-IP       Prot  DstPrt SrcPrt Destination-Mac   Vlan
--------------- --------------- ----- ------ ------ ----------------- ----
 EDst Stat-Pkts  Stat-Bytes  Uptime   Age      TcpDltSeq TcpDltAck

 ---- ---------- ----------- -------- -------- --------- ---------
0.0.0.8         0.0.0.8         8     207    107    cc-cc-cc-cc-cc-cc 8
 ARPA 0          0           00:07:07 00:21:08 cccccccc  cccccccc
0.0.0.7         0.0.0.7         7     206    106    cc-cc-cc-cc-cc-cc 7
 ARPA 0          0           00:07:09 00:21:08 cccccccc  cccccccc
0.0.0.10        0.0.0.10        10    209    109    cc-cc-cc-cc-cc-cc 10
 ARPA 0          0           00:07:06 00:21:08 cccccccc  cccccccc
0.0.0.9         0.0.0.9         9     208    108    cc-cc-cc-cc-cc-cc 9
 ARPA 0          0           00:07:07 00:21:08 cccccccc  cccccccc
0.0.0.6         0.0.0.6         TCP   205    105    cc-cc-cc-cc-cc-cc 6
 ARPA 0          0           00:07:12 00:21:08 cccccccc  cccccccc

Total entries displayed:5
Console>
```

show mls exclude protocol

Use the **show mls exclude protocol** command to display excluded protocols on TCP or UDP from being shortcuts.

show mls exclude protocol

Syntax Description

This command has no arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you enter the **show mls exclude protocol** command on a switch configured with the Supervisor Engine 1 with Layer 3 Switching Engine WS-F6K-PFC, MLS exclusion only works in full-flow mode.

These guidelines apply to switches configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2):

- The **show mls exclude protocol** displays the Layer 4 protocols that will not cause a NetFlow entry to be created automatically but can still be forwarded if a FIB hit occurs.
- MLS exclusion works regardless of the configured flow mask.

Examples

This example shows how to display excluded protocols on TCP or UDP from being shortcuts:

```
Console> (enable) show mls exclude protocol
Protocol-Port Excluded-From
------------- -------------
89            TCP UDP
5             TCP
10            TCP UDP
122           UDP
Note: MLS exclusion only works in full flow mode.
Console> (enable)
```

Related Commands

clear mls multicast statistics
set mls exclude protocol

show mls multicast

Use the **show mls multicast** command to display IP multicast MLS information.

show mls multicast

show mls multicast entry {[*mod*] [**vlan** *vlan_id*] [**group** *ip_addr*]} [**source** *ip_addr*] [**long** | **short**]

show mls multicast entry {[**all**] [**short** | **long**]}

show mls multicast statistics {*mod*}

Syntax Description

entry	Keyword to specify the IP multicast MLS packet entry.
mod	(Optional) Number of the MSFC; valid values are **15** and **16**.
vlan *vlan_id*	(Optional) Keyword and variable to specify a VLAN.
group *ip_addr*	(Optional) Keyword and variable to specify a multicast group address.
source *ip_addr*	(Optional) Keyword and variable to specify a multicast traffic source.
all	(Optional) Keyword to specify all IP multicast MLS entries on the switch.
long	(Optional) Keyword to specify an output appropriate for terminals that support output 80-characters wide.
short	(Optional) Keyword to specify an output appropriate for terminals that support output less than 80-characters wide.
statistics	Keyword to display statistics for an MSFC.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you enter the **show mls multicast** commands on Catalyst 6000 family switches without MLS, this warning message displays:

```
This feature is not supported on this device.
```

If you enter the **show mls multicast entry** command with no arguments, all the MLS entries for multicast displays. Each row in the **show mls multicast entry** command corresponds to a flow.

These guidelines apply to switches configured with the Supervisor 2 with Layer 3 Switching Engine II (PFC2):

- If you enter the **show mls multicast entry** command and an asterisk appears in the Source IP column, this indicates that any source is used.
- If you specify source 0, all * (asterisk) entries are displayed.

If you disable DNS, no name can be specified or shown.

A warning message is displayed if you disable the Layer 2 multicast protocol when the MMLS feature is running.

If you place the MSFC on a supervisor engine installed in slot 1, then the MSFC is recognized as module 15. If you install the supervisor engine in slot 2, the MSFC is recognized as module 16.

Examples

This example shows how to display global information about the IP MMLS entries on a switch configured with the Supervisor Engine 1 with Layer 3 Switching Engine WS-F6K-PFC:

```
Console> (enable) show mls multicast
Admin Status: Enabled
Operational Status: Inactive
Configured flow mask is {Source-Destination-Vlan} flow
Active Entries = 0
MSFC (Module 15): 0.0.0.0
Console> (enable)
```

This example shows how to display global information about the IP MMLS entries on a switch configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2):

```
Console> (enable) show mls multicast
Admin Status       : Enabled
 Operational Status : Active
 Total Entries      : 104
 MSFC (Module 15)   :
     IP Address     : 1.1.1.1
     Complete Flows : 30
     Partial Flows  : 10
 MSFC (Module 16)   :
     IP Address     : 2.2.2.2
     Complete Flows : 50
     Partial Flows  : 14
Console> (enable)
```

Table 2-45 describes the fields in the **show mls multicast** command output.

Table 2-45 show mls multicast Command Output Fields

Field	Description
Admin Status	Status of whether MMLS feature has been administratively enabled or not.
Operational Status	Actual operational status of the MMLS feature.
Total Entries	Number of shortcut entries that are currently installed.
MSFC	Information about the internal RP connected to the supervisor engine.
IP Address	IP address of the RP.
Complete Flows	Total number of complete flows installed by this RP.
Partial Flows	Total number of partial flows installed by this RP.

This example shows how to display statistical information on a switch configured with the Supervisor Engine 1 with Layer 3 Switching Engine WS-F6K-PFC:

```
Console> (enable) show mls multicast statistics
Router IP          Router Name        Router MAC
---------------    ------------------ -----------------
0.0.0.0            default            00-00-00-00-00-00

Transmit:
                     Feature Notifications: 0
            Feature Notification Responses: 0
           Shortcut Notification Responses: 0
                      Delete Notifications: 0
                           Acknowledgements: 0
                            Flow Statistics: 0
                   Total Transmit Failures: 0

Receive:
                     Feature Notifications: 0
                         Shortcut Messages: 0
               Duplicate Shortcut Messages: 0
                        Shortcut Install TLV: 0
                        Selective Delete TLV: 0
                            Group Delete TLV: 0
                                  Update TLV: 0
                      Input VLAN Delete TLV: 0
                     Output VLAN Delete TLV: 0
                          Global Delete TLV: 0
                            MFD Install TLV: 0
                           MFD Delete TLV: 0
                     Global MFD Delete TLV: 0
                              Invalid TLV: 0
Console> (enable)
```

This example shows how to display statistical information on a switch configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2):

```
Console> (enable) show mls multicast statistics
Router IP          Router Name        Router MAC
---------------    ------------------ -----------------
0.0.0.0            default            00-00-00-00-00-00

Transmit:
                     Feature Notifications: 0
            Feature Notification Responses: 0
           Shortcut Notification Responses: 0
                      Delete Notifications: 0
                           Acknowledgements: 0
                            Flow Statistics: 0
                   Total Transmit Failures: 0

Receive:
                     Feature Notifications: 0
                         Shortcut Messages: 0
               Duplicate Shortcut Messages: 0
                        Shortcut Install TLV: 0
                        Selective Delete TLV: 0
                            Group Delete TLV: 0
                                  Update TLV: 0
                      Input VLAN Delete TLV: 0
                     Output VLAN Delete TLV: 0
                          Global Delete TLV: 0
                            MFD Install TLV: 0
```

```
                                    MFD Delete TLV: 0
                                Global MFD Delete TLV: 0
                                   Invalid TLV: 0
Console> (enable)
```

This example shows how to display IP MMLS entry information on a switch configured with the Supervisor Engine 1 with Layer 3 Switching Engine WS-F6K-PFC:

```
Console> (enable) show mls multicast entry
Router IP       Dest IP         Source IP       Pkts       Bytes       InVlan  OutVlans
--------------- --------------- --------------- ---------- ----------- ------- --------
1.1.5.252       224.1.1.1       1.1.11.1        15870      2761380     20
1.1.9.254       224.1.1.1       1.1.12.3        473220     82340280    12
1.1.5.252       224.1.1.1       1.1.12.3        15759      2742066     20
1.1.9.254       224.1.1.1       1.1.11.1        473670     82418580    11
1.1.5.252       224.1.1.1       1.1.11.3        15810      2750940     20
1.1.9.254       224.1.1.1       1.1.12.1        473220     82340280    12
1.1.5.252       224.1.1.1       1.1.13.1        15840      2756160     20
Total Entries: 7
Console> (enable)
```

Note The display for the **show mls multicast entry** command has been modified to fit the page.

This example shows how to display IP MMLS entry information on a switch configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2):

```
Console> (enable) show mls multicast entry
 Router-IP       Dest-IP         Source-IP       Pkts               Bytes              InVlan Type
OutVlans
 --------------- --------------- --------------- ------------------ ------------------ ------ ----
----------
 33.0.33.26      224.2.2.3       10.0.0.1        595                59500              50      C    13,
12
 33.0.33.26      224.2.2.3       *               2                  200                50      P    13,
12

 Total Entries: 2 (1 of which type 'C' = Complete Flow/s, 'P' = Partial Flow/s)
Console> (enable)
```

Table 2-46 describes the fields in the **show mls multicast entry** command output.

Table 2-46 show mls multicast entry Command Output Fields

Field	Description
Router-IP	IP address of the RP that installed the flow.
Dest-IP	Multicast destination IP address for this flow.
Source-IP	IP address of the source that corresponds to this flow.
Pkts	Number of packets switched using this flow.
Bytes	Number of bytes switched using this flow.
InVlan	RPF interface for the packets corresponding to this flow.
Type	Shortcut Type (C = a complete shortcut and P = a partial shortcut).
OutVlans	Output VLANs on which the packets are replicated for this flow.
Total Entries	Number of shortcut entries currently installed.

Related Commands clear mls multicast statistics

show mls nde

Use the **show mls nde** command to display NetFlow Data Export information.

show mls nde

Syntax Description

This command has no arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display NetFlow Data Export information:

```
Console> show mls nde
Netflow Data Export version: 7
Netflow Data Export disabled
Netflow Data Export port/host is not configured.
Total packets exported = 0
Console>
```

show mls netflow-route

Use the **show mls netflow-route** command to display summaries from NetFlow for routing in the MLS-based Catalyst 6000 family switches.

show mls netflow-route [**ip** | **ipx**]

Syntax Description

ip	(Optional) Keyword to specify IP MLS.
ipx	(Optional) Keyword to specify IPX MLS.

Defaults

The default displays both IP and IPX MLS information.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This command is supported on Catalyst 6000 family switches configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) only.

Examples

This example shows how to display summaries from NetFlow for routing:

```
Console> show mls netflow-route
Total packets switched = 0
Total bytes switched = 0

Software installed aging time = 0
IP flows aging time = 256 seconds
IP flows fast aging time = 0 seconds, packet threshold = 0
IP Current flow mask is Full flow
Total netflow forwarding entries = 4
Netflow Data Export version:7
Netflow Data Export disabled
Netflow Data Export port/host is not configured.
Total packets exported = 0


IPX flows aging time = 256 seconds
IPX flow mask is Destination flow
IPX max hop is 15
Console>
```

show mls statistics

Use the **show mls statistics** command to display MLS statistics information in the MLS-based Catalyst 6000 family switches.

show mls statistics protocol

show mls statistics entry [*mod*]

show mls statistics entry ip [*mod*] [**destination** *ip_addr_spec*] [**source** *ip_addr_spec*] [**protocol** *protocol* [**src-port** *src_port*] [**dst-port** *dst_port*]]

show mls statistics entry ipx [*mod*] [**destination** *ipx_addr_spec*] [**source** *ipx_addr_spec*]

Syntax Description

protocol	Keyword to specify a route processor.
entry	Keyword to specify the entry type.
mod	(Optional) Number of the MSFC; valid values are **15** or **16**.
entry	Keyword to display statistics based on the specified option.
ip	Keyword to specify IP MLS.
destination	(Optional) Keyword to specify the destination IP address.
ip_addr_spec	(Optional) Full IP address or a subnet address in the following formats: ip_addr, ip_addr/netmask, or ip_addr/maskbit.
source	(Optional) Keyword to specify the source IP address.
protocol *protocol*	(Optional) Keyword and variable to specify additional flow information (protocol family and protocol port pair) to be matched; valid values are from **1** to **255**, **ip**, **ipinip**, **icmp**, **igmp**, **tcp**, and **udp**.
src-port *src_port*	(Optional) Keyword and variable to specify the source port IP address.
dst-port *dst_port*	(Optional) Keyword and variable to specify the destination port IP address.
ipx	Keyword to specify IPX MLS.
ipx_addr_spec	(Optional) Full IPX address or a subnet address in one of the following formats: *src_net/*[*mask*], *dest_net.dest_node*, or *dest_net/mask*.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If your system is configured with the Supervisor Engine 2 with Switching Engine II (PFC2), the **show mls statistics entry** command output displays per flow statistics as per the configured flow mask. You can enter this command to display per-flow statistics for flows that are CEF switched (in hardware) or switched through software-installed shortcuts in the NetFlow table.

You can enter the **show mls statistics entry** command to display NetFlow forwarding entries on systems configured with a Supervisor Engine 2. If your system is configured with a Supervisor Engine 1, enter the **show mls entry** command.

When specifying the **ip** | **ipx** keyword, if you specify **ip** or do not enter a keyword, this means that the command is for IP MLS. If you specify **ipx**, this means the command is for IPX only.

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

- IPX net 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)

If you enter any of the **show mls statistics protocol** commands on a Catalyst 6000 family switch without MLS, this warning message displays:

```
Feature not supported in hardware.
```

If you enter the **show mls statistics protocol** command, the statistics in the protocol category, such as Telnet, FTP, or WWW are displayed. Note that this applies for "full flowmask" only. In flowmasks other than full flow, inapplicable fields will have a dash (similar to **show mls entry** outputs).

A value 0 for *src_port* and *dst_port* means "don't care." Note that this applies for "full flowmask" only.

Use the following syntax to specify an IP subnet address:

- *ip_subnet_addr*—This is the short subnet address format. The trailing decimal number "00" in an IP address YY.YY.YY.YY specifies the boundary for an IP subnet address. For example, 172.22.36.00 indicates a 24-bit subnet address (subnet mask 255.255.255.0), and 173.24.00.00 indicates a 16-bit subnet address (subnet mask 255.255.0.0). However, this format can identify only a subnet address with a length of 8, 16, or 24 bits.
- *ip_addr/subnet_mask*—This is the 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* is allowed to be a full host address, such as 172.22.253.1/255.255.252.00, which has the same subnet address as *ip_subnet_addr*.
- *ip_addr/maskbits*—This is the 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* is allowed to be a full host address, such as 172.22.254.1/22, which has the same subnet address as 172.22.252.00/72.

If you place the MSFC on a supervisor engine installed in slot 1, then the MSFC is recognized as module 15. If you install the supervisor engine in slot 2, the MSFC is recognized as module 16.

Examples

This example shows how to display the statistics for all protocol categories:

```
Console> (enable) show mls statistics protocol
Protocol  TotalFlows  TotalPackets    Total Bytes
-------   ----------  --------------  ------------
Telnet    900         630             4298
FTP       688         2190            3105
WWW       389         42679           623686
SMTP      802         4966            92873
X         142         2487            36870
DNS       1580        52              1046
Others    82          1               73
Total     6583        53005           801951
Console> (enable)
```

This example shows how to display the statistics for all protocol categories:

```
Console> (enable) show mls statistics
                                    Last    Used
Destination IP  Source IP       Prot DstPrt SrcPrt Stat-Pkts  Stat-Bytes
--------------- --------------- ---- ------ ------ ---------- ---------------
172.20.22.14    172.20.25.10    6    50648  80     3152       347854
172.20.22.43    172.20.32.43    44   2323   324    23232      232323

Destination IPX           Source IPX net Stat-Pkts  Stat-Bytes
------------------------- -------------- ---------- ----------
201.00A0.2451.7423        1.0002         30256      31795084
501.0000.3100.0501        1.0003         12121      323232
Console> (enable)
```

Note The following commands are output from switches configured with the Supervisor Engine 1 with Layer 3 Switching Engine WS-F6K-PFC. The output from switches configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) are slightly different.

This example shows how to display IP MLS statistics for MSFC 15 in a system configured with the Supervisor Engine 1 with Layer 3 Switching Engine WS-F6K-PFC:

```
Console> show mls statistics entry ip 15 destination 172.20.22.14
MSFC 127.0.0.12 (Module 15):
                                    Last    Used
Destination IP  Source IP       Prot DstPrt SrcPrt Stat-Pkts Stat-Bytes
--------------- --------------- ---- ------ ------ --------- ---------------
172.20.22.14    172.20.25.10    6    50648  80     3152      347854
Console>
```

This example shows how to display the statistics for a specific destination IP address:

```
Console> show mls statistics entry ip destination 172.20.22.14
                Last Used         Last    Used
Destination IP  Source IP       Prot DstPrt SrcPrt Stat-Pkts  Stat-Bytes
--------------- --------------- ---- ------ ------ ---------- ---------------
172.20.22.14    172.20.25.10    6    50648  80     3152       347854
Console>
```

This example shows how to display the statistics for a specific destination IPX address:

```
Console> show mls statistics entry ipx destination 1.0002.00e0.fefc.6000
Destination IPX           Source IPX net Stat-Pkts  Stat-Bytes
------------------------- -------------- ---------- ----------
MLS-RP 10.20.26.64:
1.0002.00e0.fefc.6000     1.0003         11         521
Console>
```

Related Commands

- clear mls statistics entry
- set mls statistics protocol

show mls verify

To display the Layer 3 error checking configuration, use the **show mls verify** command.

show mls verify

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the Layer 3 error checking configuration:

```
Console> show mls verify
 IP checksum verification disabled
 IP minimum length verification enabled
 IP inconsistant length verification disabled
 IPX minimum length verification enabled
 IPX inconsistant length verification disabled
Console>
```

Table 2-47 describes the fields in the **show mls verify** command output.

Table 2-47 show mls verify Command Output Fields

Field	Description
IP checksum verification	Status of whether IP checksum verification is enabled or disabled.
IP minimum length verification	Status of whether the verification of IP minimum packet length is enabled or disabled.
IP inconsistent length verification	Status of whether the verification of IP length consistency is enabled or disabled.
IPX minimum length verification	Status of whether the verification of IPX minimum packet length is enabled or disabled.
IPX consistent length verification	Status of whether the verification of IPX length consistency is enabled or disabled.

Related Commands

set mls verify

show module

Use the **show module** command to display module status and information. For supervisor engines, the **show module** command displays the supervisor engine number but appends the uplink daughter card's module type and information.

show module [*mod*]

Syntax Description

mod	(Optional) Number of the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a module number, all modules are shown.

The MAC addresses for the supervisor engine are displayed in three lines of output. The first line lists the two MAC addresses for inband ports, the second line lists the two MAC addresses for the two gigabit-uplink ports, and the third line lists the allocated 0x3ff MAC address for the chassis backplane.

If you place the MSFC on a supervisor engine installed in slot 1, then the MSFC is recognized as module 15. If you install the supervisor engine in slot 2, the MSFC is recognized as module 16.

The slot field in the **show module** command display is required because submodules, such as the MSM, reside in the same slot as the supervisor engine module, but are treated as a separate module.

The MSM is referenced by the module number in all other CLI commands and is treated like any other module.

Examples

This example shows how to display status and information for all modules:

```
Console> show module
Mod Slot Ports Module-Type               Model               Sub Status
--- ---- ----- ------------------------- ------------------- --- --------
1   1    2     1000BaseX Supervisor      WS-X6K-SUP1A-2GE    yes ok
15  1    1     Multilayer Switch Feature WS-F6K-MSFC         no  ok
8   8    48    10/100BaseTX Ethernet     WS-X6248-RJ-45      no  ok
9   9    48    10/100BaseTX Ethernet     WS-X6348-RJ-45      yes ok

Mod Module-Name         Serial-Num
--- ------------------- -----------
1                       SAD03436055
15                      SAD03432597
9                       SAD03414268

Mod MAC-Address(es)                         Hw     Fw          Sw
--- --------------------------------------- ------ ----------- --------------
```

```
1   00-30-80-f7-a5-06 to 00-30-80-f7-a5-07 1.0    5.2(1)     6.1(0.12)
    00-30-80-f7-a5-04 to 00-30-80-f7-a5-05
    00-30-a3-4a-a0-00 to 00-30-a3-4a-a3-ff
15  00-d0-bc-ee-d0-dc to 00-d0-bc-ee-d1-1b 1.2    12.0(3)XE1 12.0(3)XE1
8   00-d0-c0-c8-83-ac to 00-d0-c0-c8-83-db 1.1    4.2(0.24)V 6.1(0.37)FTL
9   00-50-3e-7c-43-00 to 00-50-3e-7c-43-2f 0.201  5.3(1)

Mod Sub-Type                Sub-Model           Sub-Serial  Sub-Hw
--- ----------------------- ------------------- ----------- ------
1   L3 Switching Engine     WS-F6K-PFC          SAD03451187 1.0
9   Inline Power Module     WS-F6K-VPWR                     1.0
Console>
```

This example shows the display for a 48-port 10/100BASE-TX switching services-configured module:

```
Console> show module 5
Mod Slot Ports Module-Type               Model               Status
--- ---- ----- ------------------------- ------------------- --------
5   5    48    10/100BaseTX (RJ-45)      WS-X6248-RJ-45      ok

Mod Module-Name         Serial-Num
--- ------------------- -----------
5                       SAD03181291

Mod MAC-Address(es)                       Hw     Fw         Sw
--- ------------------------------------- ------ ---------- -----------------
5   00-50-f0-ac-30-54 to 00-50-f0-ac-30-83 1.0    4.2(0.24)V 6.1(0.12)
Console>
```

This example shows the display for an 8-port T1/E1 ISDN PRI services-configured module:

```
Console> (enable) show module 3
Mod Slot Ports Module-Type               Model               Status
--- ---- ----- ------------------------- ------------------- --------
3   3    8     T1 PSTN                   WS-X6608-T1         ok

Mod Module-Name         Serial-Num
--- ------------------- -----------
3   T1                  SAD02440056

Mod MAC-Address(es)                       Hw     Fw         Sw
--- ------------------------------------- ------ ---------- -----------------
3   00-50-0f-08-bc-a0 to 00-50-0f-08-bc-cf 0.1    5.1(1)     5.4(1)
Console>
```

This example shows the display for a 24-port FXS analog station interface services-configured module:

```
Console> show module 3
Mod Slot Ports Module-Type               Model               Status
--- ---- ----- ------------------------- ------------------- --------
3   3    24    FXS                       WS-X6624-FXS        ok

Mod Module-Name         Serial-Num
--- ------------------- -----------
3   Elvis-S             SAD02440056

Mod MAC-Address(es)                       Hw     Fw         Sw
--- ------------------------------------- ------ ---------- -----------------
3   00-50-0f-08-bc-a0 to 00-50-0f-08-bc-a0 0.1    5.1(1)     5.4(1)
Console>
```

Table 2-48 describes the possible fields in the **show module** command output.

Table 2-48 show module Command Output Fields

Field	Description
Mod	Module number.
Slot	Number of the slot where the module or submodule resides.
Ports	Number of ports on the module.
Module-Type	Module (such as 100BASE-X Ethernet).
Model	Model number of the module.
Sub	Status of whether a submodule is installed.
Status	Status of the module. Possible status strings are ok, disable, faulty, other, standby, error, pwr-down, and pwr-deny states[1].
Module-Name	Name of the module.
Serial-Num	Serial number of the module.
MAC-Address(es)	MAC address or MAC address range for the module.
Hw[2]	Hardware version of the module.
Fw[3]	Firmware version of the module.
Sw	Software version on the module.
Sub-Type[4]	Submodule type.
Sub-Model[4]	Model number of the submodule.
Sub-Serial[4]	Serial number of the submodule.
Sub-Hw[4]	Hardware version of the submodule.

1. The pwr-down and pwr-deny states are supported by the power management feature.
2. Hw for the supervisor engine displays the supervisor engine's EARL hardware version.
3. Fw for the supervisor engine displays the supervisor engine's boot version.
4. This field displays EARL information.

show moduleinit

Use the **show moduleinit** command to display contents of the information stored in the system module initiation log.

show moduleinit [*mod*] [**log** *lognum* | *-logcount*]

Syntax Description

mod	(Optional) Number of the module.
log	(Optional) Keyword to specify a specific log.
lognum	(Optional) Number of the log to display.
-logcount	(Optional) Number of previous logs to display.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a module number, contents for all modules are shown.

Examples

This example shows how to show the last two log entries for module 1:

```
Console> show moduleinit 1 log -2
Module 1:   Number of Logs: 3
Log #2:
State 1: Entry/Exit/Elapse Time: 14721/14721/0
  Success_Exit
State 2: Entry/Exit/Elapse Time: 14721/14721/0
  Success
State 3: Entry/Exit/Elapse Time: 14721/32223/17502
  Success_Exit

Log #3:
State 1: Entry/Exit/Elapse Time: 38302/38302/0
  P_PortConfigTokenRingFeatures()
  ConfigModule()
State 2: Entry/Exit/Elapse Time: 38302/38302/0
  Success
State 3: Entry/Exit/Elapse Time: 38302/38310/8
  Success_Exit
Console>
```

This example shows how to display the contents of a specific log for module 1:

```
Console> show moduleinit 1 log 2
Module 1:   Number of Logs: 3
Log #2:
State 1: Entry/Exit/Elapse Time: 14721/14721/0
```

```
  Success_Exit
State 2: Entry/Exit/Elapse Time: 14721/14721/0
  Success
State 3: Entry/Exit/Elapse Time: 14721/32223/17502

Console>
```

Table 2-49 describes the possible fields in the **show moduleinit** command output.

Table 2-49 show moduleinit Command Output Fields

Field	Description
Log #	Number of the log.
State #	Number of the module initiation states. Output includes the entry time into and exit time from all the module initiation states, along with the elapsed time, in milliseconds.

show msfcautostate

Use the **show msfcautostate** command to display the MSFC-derived interface state.

show msfcautostate

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to display the MSFC auto state status:

```
Console> (enable) show msfcautostate
MSFC Auto port state: enabled
Console> (enable)
```

Related Commands

set msfcautostate

show msmautostate

Use the **show msmautostate** command to display the current status of the line protocol state determination of the MSM(s) due to Catalyst 6000 family switch port state changes.

show msmautostate *mod*

Syntax Description

mod	Number of the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the current status of MSM line protocol state determination:

```
Console> show msmautostate
MSM Auto port state: enabled
Console>
```

Related Commands

set msmautostate

show multicast group

Use the **show multicast group** command to display the multicast group configuration.

show multicast group [*mac_addr*] [*vlan_id*]

Syntax Description

mac_addr	(Optional) Destination MAC address.
vlan_id	(Optional) Number of the VLAN.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the multicast group configuration for VLAN 1:

```
Console> show multicast group 1
VLAN  Dest MAC/Route Des    [CoS]   Destination Ports or VCs / [Protocol Type]
---- ----------------- ----- ---------------------------------
1    01-00-5e-00-01-28*      3/1,12/9
1    01-00-5e-63-7f-6f*      3/1,12/5,12/9
Total Number of Entries = 2
Console>
```

This example shows how to display the multicast group configuration for a specific MAC address on VLAN 5:

```
Console> show multicast group 01-00-5E-00-00-5C 5
VLAN  Dest MAC/Route Des    [CoS]   Destination Ports or VCs / [Protocol Type]
---- ----------------- ----- ---------------------------------
5    01-00-5E-00-00-5C       3/1, 3/9
Total Number of Entries = 1
Console>
```

Table 2-50 describes the fields in the **show multicast group** command output.

Table 2-50 show multicast group Command Output Fields

Field	Description
IGMP enabled/disabled	Status of whether IGMP is enabled or disabled.
GMRP enabled/disabled	Status of whether GMRP is enabled or disabled.
VLAN	VLAN number.
Dest MAC/Route Des	Group destination MAC address.
*	Status of whether the port was configured manually as a multicast router port.

Table 2-50 show multicast group Command Output Fields (continued)

Field	Description
CoS	CoS value.
Destination Ports or VCs	List of all the ports that belong to this multicast group. Traffic destined to this group address will be forwarded on all these ports.
Protocol Type	Type of protocol.
Total Number of Entries	Total number of entries in the multicast group table that match the criteria specified by the command.

Related Commands

clear multicast router
set multicast router
show multicast router

show multicast group count

Use the **show multicast group count** command to show the total count of multicast addresses (groups) in a VLAN.

show multicast group count [*vlan_id*]

Syntax Description

vlan_id	(Optional) Number of the VLAN.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

An asterisk in the **show multicast group count** command output indicates the port was configured manually.

Examples

This example shows how to display the total count of multicast groups in VLAN 5:

```
Console> show multicast group count 5

Total Number of Entries = 2
Console>
```

Related Commands

clear multicast router
set multicast router
show multicast router

show multicast protocols status

Use the **show multicast protocols status** command to display the status of Layer 2 multicast protocols on the switch.

show multicast protocols status

Syntax Description

This command has no arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the Layer 2 multicast protocol status:

```
Console> show multicast protocols status
IGMP disabled
IGMP fastleave enabled
RGMP enabled
GMRP disabled
Console>
```

Related Commands

set gmrp
set igmp

show multicast router

Use the **show multicast router** command to display the ports that have IGMP or RGMP-capable routers assigned to them.

show multicast router {**igmp** | **rgmp**} [*mod/port*] [*vlan_id*]

Syntax Description

igmp	Keyword to specify IGMP-capable routers.
rgmp	Keyword to specify RGMP-capable routers.
mod/port	(Optional) Number of the module and the port on the module.
vlan_id	(Optional) Number of the VLAN.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the ports that have IGMP-multicast routers assigned to them:

```
Console> show multicast router igmp
Port    Vlan
------  ------
5/15    1
Total Number of Entries = 1
'*' - Configured
'+' - RGMP-capable
Console>
```

This example shows how to display the ports that have RGMP-multicast routers assigned to them:

```
Console> show multicast router rgmp
Port    Vlan
------  ------
5/1 +   1
5/14 +  2
Total Number of Entries = 2
'*' - Configured
'+' - RGMP-capable
Console>
```

Table 2-51 describes the fields in the **show multicast router** command output.

Table 2-51 show multicast router Command Output Fields

Field	Description
Port	Port through which a multicast router can be reached.
*	Status of whether the port was configured manually or not.
+	Status of whether the router is RGMP capable or not.
VLAN	VLAN associated with the port.
Total Number of Entries	Total number of entries in the table that match the criteria specified by the command.

Related Commands

set igmp
set multicast router
set rgmp
show multicast group
show multicast group count

show netstat

Use the **show netstat** command to display the currently active network connections and to list statistics for the various protocols in the TCP/IP.

show netstat [**tcp** | **udp** | **ip** | **icmp** | **routes** | **stats** | **interface**]

Syntax Description

tcp	(Optional) Keyword to show TCP statistics.
udp	(Optional) Keyword to show UDP statistics.
ip	(Optional) Keyword to show IP statistics.
icmp	(Optional) Keyword to show ICMP statistics.
routes	(Optional) Keyword to show the IP routing table.
stats	(Optional) Keyword to show all statistics for TCP, UDP, IP, and ICMP.
interface	(Optional) Keyword to show interface statistics.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the current active network connections:

```
Console> show netstat
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp        0    128  172.20.25.142.23       171.68.10.75.44720     ESTABLISHED
tcp        0      0  *.7161                 *.*                    LISTEN
tcp        0      0  *.23                   *.*                    LISTEN
udp        0      0  *.*                    *.*
udp        0      0  *.161                  *.*
udp        0      0  *.123                  *.*
Console>
```

This example shows how to display TCP statistics:

```
Console> show netstat tcp
tcp:
        5122 packets sent
                4642 data packets (102292 bytes)
                28 data packets (6148 bytes) retransmitted
                434 ack-only packets (412 delayed)
                0 URG only packets
                0 window probe packets
                1 window update packet
                17 control packets
        7621 packets received
                4639 acks (for 103883 bytes)
```

```
                69 duplicate acks
                0 acks for unsent data
                3468 packets (15367 bytes) received in-sequence
                12 completely duplicate packets (20 bytes)
                0 packets with some dup. data (0 bytes duped)
                4 out-of-order packets (0 bytes)
                0 packets (0 bytes) of data after window
                0 window probes
                0 window update packets
                0 packets received after close
                0 discarded for bad checksums
                0 discarded for bad header offset fields
                0 discarded because packet too short
        6 connection requests
        6 connection accepts
        10 connections established (including accepts)
        11 connections closed (including 1 drop)
        2 embryonic connections dropped
        4581 segments updated rtt (of 4600 attempts)
        28 retransmit timeouts
                0 connections dropped by rexmit timeout
        0 persist timeouts
        66 keepalive timeouts
                63 keepalive probes sent
                3 connections dropped by keepalive
Console>
```

Table 2-52 describes the fields in the **show netstat tcp** command output.

Table 2-52 show netstat tcp Command Output Fields

Field	Description
packets sent	Total number of TCP packets sent.
data packets (bytes)	Number of TCP data packets sent and the size of those packets in bytes.
data packets (bytes) retransmitted	Number of TCP data packets retransmitted and the size of those packets in bytes.
ack-only packets (delayed)	Number of TCP acknowledgment-only packets sent and the number of those packets delayed.
URG only packets	Number of URG packets.
window probe packets	Number of window probe packets.
window update packet	Number of window update packets.
packets received	Total number of TCP packets received.
acks (for *x* bytes)	Number of TCP acknowledgments received and the total bytes acknowledged.
duplicate acks	Number of duplicate TCP acknowledgments received.
acks for unsent data	Number of TCP acknowledgments received for data that was not sent.

Table 2-52 show netstat tcp Command Output Fields (continued)

Field	Description
packets (bytes) received in-sequence	Number of TCP packets (and the size in bytes) received in sequence.
completely duplicate packets (bytes)	Number of duplicate TCP packets (and the size in bytes) received.
packets with some dup. data (bytes duped)	Number of TCP packets received with duplicate data (and the number of bytes of duplicated data).
out-of-order packets (bytes)	Number of out-of-order TCP packets (and the size in bytes) received.
packets (bytes) of data after window	Number of TCP packets (and the size in bytes) received outside of the specified data window.
discarded for bad checksums	Number of TCP packets received and discarded that failed the checksum.
discarded because packet too short	Number of TCP packets received and discarded that were truncated.
connection requests	Total number of TCP connection requests sent.
connection accepts	Total number of TCP connection accepts sent.
connections established (including accepts)	Total number of TCP connections established, including those for which a connection accept was sent.
connections closed (including *x* drops)	Total number of TCP connections closed, including dropped connections.
retransmit timeouts	Number of timeouts that occurred when a retransmission was attempted.
connections dropped by rexmit timeout	Number of connections dropped due to retransmission timeouts.
keepalive timeouts	Number of keepalive timeouts that occurred.
keepalive probes sent	Number of TCP keepalive probes sent.
connections dropped by keepalive	Number of connections dropped.

This example shows how to display UDP statistics:

```
Console> show netstat udp
udp:
        0 incomplete headers
        0 bad data length fields
        0 bad checksums
        0 socket overflows
        1116 no such ports
Console>
```

Table 2-53 describes the fields in the **show netstat udp** command output.

Table 2-53 show netstat udp Command Output Fields

Field	Description
incomplete headers	Number of UDP packets received with incomplete packet headers.
bad data length fields	Number of UDP packets received with a data length field that did not match the actual length of the packet payload.
bad checksums	Number of UDP packets received that failed the checksum.
socket overflows	Number of socket overflows.
no such ports	Number of UDP packets received destined for nonexistent ports.

This example shows how to display IP statistics:

```
Console> show netstat ip
ip:
        76894 total packets received
        0 bad header checksums
        0 with size smaller than minimum
        0 with data size < data length
        0 with header length < data size
        0 with data length < header length
        0 fragments received
        0 fragments dropped (dup or out of space)
        0 fragments dropped after timeout
        0 packets forwarded
        0 packets not forwardable
        0 redirects sent
Console>
```

Table 2-54 describes the fields in the **show netstat ip** command output.

Table 2-54 show netstat ip Command Output Fields

Field	Description
total packets received	Total number of IP packets received.
bad header checksums	Number of received IP packets that failed the checksum.
with size smaller than minimum	Number of received IP packets that were smaller than the minimum IP packet size.
with data size < data length	Number of packets in which the data size was less than the data length.
with header length < data size	Number of packets in which the header length was less than the data size.
with data length < header length	Number of packets in which the data length was less than the minimum header length.
fragments received	Number of IP packet fragments received.

Table 2-54 show netstat ip Command Output Fields (continued)

Field	Description
fragments dropped (dup or out of space)	Number of received IP packet fragments that were dropped because of duplicate data or buffer overflow.
fragments dropped after timeout	Number of received IP packet fragments that were dropped.
packets forwarded	Number of forwarded IP packets.
packets not forwardable	Number of IP packets that the switch did not forward.
redirects sent	Number of IP packets that the switch redirected.

This example shows how to display ICMP statistics:

```
Console> show netstat icmp
icmp:
        Redirect enabled
        0 calls to icmp_error
        0 errors not generated 'cuz old message was icmp
        Output histogram:
                echo reply: 1001
        1 message with bad code fields
        0 messages < minimum length
        0 bad checksums
        0 messages with bad length
        Input histogram:
                echo reply: 12
                destination unreachable: 3961
                echo: 1001
        1001 message responses generated
Console>
```

Table 2-55 describes the fields in the **show netstat icmp** command output.

Table 2-55 show netstat icmp Command Output Fields

Field	Description
Redirect enabled	Status of whether ICMP redirection is enabled or disabled.
Output histogram	Frequency distribution statistics for output ICMP packets.
echo reply	Number of output echo reply ICMP packets.
messages with bad code fields	Number of ICMP packets with an invalid code field.
messages < minimum length	Number of ICMP packets with less than the minimum packet length.
bad checksums	Number of ICMP packets that failed the checksum.
messages with bad length	Number of ICMP packets with an invalid length.

Table 2-55 show netstat icmp Command Output Fields (continued)

Field	Description
Input histogram	Frequency distribution statistics for input ICMP packets.
echo reply	Number of input echo-reply ICMP packets.
destination unreachable	Number of input destination-unreachable ICMP packets.
echo	Number of input-echo ICMP packets.
message responses generated	Number of ICMP message responses the system generated.

This example shows how to display the IP routing table:

```
Console> show netstat routes
DESTINATION     GATEWAY         FLAGS   USE             INTERFACE
default         172.16.1.201    UG      6186            sc0
172.16.0.0      172.16.25.142   U       6383            sc0
default         default         UH      0               sl0
Console>
```

Table 2-56 describes the fields in the **show netstat routes** command output.

Table 2-56 show netstat routes Command Output Fields

Field	Description
DESTINATION	Destination IP address or network.
GATEWAY	Next hop to the destination.
FLAGS	Flags indicating the interface state.
USE	Number of times this route was used.
INTERFACE	Interface out of which packets to the destination should be forwarded.

This example shows how to display interface statistics:

```
Console> show netstat interface
Interface          InPackets InErrors OutPackets OutErrors
sl0                        0        0          0         0
sc0                   368996        0      12624         0
Console>
Interface Rcv-Octet            Xmit-Octet
--------- -------------------- --------------------
sc0       182786               0
sl0       0                    0
Interface Rcv-Unicast          Xmit-Unicast
--------- -------------------- --------------------
sc0       3002                 1314
sl0       0                    0
Console>
```

Table 2-57 describes the fields in the **show netstat interface** command output.

Table 2-57 show netstat interface Command Output Fields

Field	Description
Interface	Interface number (sl0 is the SLIP interface; sc0 is the in-band interface).
InPackets	Number of input packets on the interface.
InErrors	Number of input errors on the interface.
OutPackets	Number of output packets on the interface.
OutErrors	Number of output errors on the interface.
Rcv-Octet	Number of octet frames received on the port.
Xmit-Octet	Number of octet frames transmitted on the port.
Rcv-Unicast	Number of unicast frames received on the port.
Xmit-Unicast	Number of unicast frames transmitted on the port.

Related Commands

set interface
set ip route

show ntp

Use the **show ntp** command to display the current NTP status.

show ntp

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the current NTP status:

```
Console> show ntp
Current time: Tue Mar 28 2000, 11:19:03 pst
Timezone: 'pst', offset from UTC is -8 hours
Summertime: 'pst', enabled
Last NTP update:
Broadcast client mode: enabled
Broadcast delay: 3000 microseconds
Client mode: disabled

NTP-Server
--------------------------------------
time_server.cisco.com
Console>
```

Table 2-58 describes the fields in the **show ntp** command output.

Table 2-58 show ntp Command Output Fields

Field	Description
Current time	Current system time.
Timezone	Time zone and the offset in hours from UTC.
Summertime	Time zone for daylight saving time and whether the daylight saving time adjustment is enabled or disabled.
Last NTP update	Time of the last NTP update.
Broadcast client mode	Status of whether NTP broadcast-client mode is enabled or disabled.
Broadcast delay	Configured NTP broadcast delay.
Client mode	Status of whether NTP client mode is enabled or disabled.
NTP-Server	List of configured NTP servers.

Related Commands

- clear ntp server
- set ntp broadcastclient
- set ntp broadcastdelay
- set ntp client
- set ntp server

show pbf

Use the **show pbf** command to display PBF-related information.

show pbf [{**adjacency** | **statistics** | **map**} [*adj_name*]]

Syntax Description

adjacency	(Optional) Keyword to display PBF adjacency information.
statistics	(Optional) Keyword to display PBF statistics.
map	(Optional) Keyword to display PBF adjacency map.
adj_name	(Optional) Name of the adjacency.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

To display MAC address information, enter the **show pbf** command with no options.

The **show adjacency map** command displays all the ACLs that use a specific adjacency.

Refer to the "Configuring Policy-Based Forwarding" section of Chapter 16, "Configuring Access Control," in the *Catalyst 6000 Family Software Configuration Guide* for detailed information about PBF.

Examples

This example shows how to display the MAC address for PFC2:

```
Console> show pbf
Pbf status    Mac address
-----------   ------------------
ok            00-01-64-61-39-c2
Console>
```

This example shows how to display adjacency information for PFC2:

```
Console> show pbf adjacency
Index    DstVlan   DstMac             SrcMac             Name
-------------------------------------------------------------------
1         2      0a-0a-0a-0a-0a-0a  00-11-22-33-44-55     a_1
2         2      0a-0a-0a-0a-0a-0b  00-11-22-33-44-55     a_2
3         2      0a-0a-0a-0a-0a-0c  00-11-22-33-44-55     a_3
4         2      0a-0a-0a-0a-0a-0d  00-11-22-33-44-55     a_4
5         1      20-20-20-20-20-20  00-11-22-33-44-55     b_1
6         1      20-20-20-20-20-21  00-11-22-33-44-55     b_2
7         1      20-20-20-20-20-22  00-11-22-33-44-55     b_3
8         1      20-20-20-20-20-23  00-11-22-33-44-55     b_4
Console>
```

This example shows how to display adjacency information for adjacency **a_1**:

```
Console> show pbf adj a_1
Index    DstVlan   DstMac             SrcMac             Name
-------------------------------------------------------------------
1          2      00-0a-0a-0a-0a-0a  00-11-22-33-44-55     a_1
Console>
```

This example shows how to display statistics for PFC2:

```
Console> show pbf statistics
Index    DstVlan   DstMac             SrcMac          HitCount(hex)  Name
-------------------------------------------------------------------------
1         2      0a-0a-0a-0a-0a-0a  00-11-22-33-44-55  0x00011eb4    a_1
2         2      0a-0a-0a-0a-0a-0b  00-11-22-33-44-55  0x00011ebc    a_2
3         2      0a-0a-0a-0a-0a-0c  00-11-22-33-44-55  0x00011ec3    a_3
4         2      0a-0a-0a-0a-0a-0d  00-11-22-33-44-55  0x00011eca    a_4
5         1      20-20-20-20-20-20  00-11-22-33-44-55  0x00011ed1    b_1
6         1      20-20-20-20-20-21  00-11-22-33-44-55  0x00011ed8    b_2
7         1      20-20-20-20-20-22  00-11-22-33-44-55  0x00011edf    b_3
8         1      20-20-20-20-20-23  00-11-22-33-44-55  0x00011ee6    b_4
Console>
```

This example shows how to display statistics for adjacency **a_1**:

```
Console> show pbf statistics a_1
Index    DstVlan   DstMac             SrcMac          HitCount(hex)  Name

-------------------------------------------------------------------------

1          2      00-0a-0a-0a-0a-0a  00-11-22-33-44-55  0x0038cd58    a_1
Console>
```

This example shows how to display the adjacency map for PFC2:

```
Console> show pbf map
Adjacency            ACL
------------------  --------------------
a_1                  ip1

a_2                  ip1

a_3                  ip1

a_4                  ip1

b_1                  ip2

b_2                  ip2

b_3                  ip2

b_4                  ip2
Console>
```

This example shows how to display the adjacency map for adjacency **a_1**:

```
Console> show pbf map a_1
Adjacency            ACL
------------------  --------------------
a_1                  ip1
Console>
```

Related Commands clear pbf
set pbf

show port

Use the **show port** command to display port status information.

show port [*mod*[*/port*]]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a *mod*, the ports on all modules are shown.

If you do not specify a *port*, all the ports on the module are shown.

The output for an 8-port T1/E1 PSTN interface module configured for transcoding and/or conferencing displays a transcoding port type as “mtp” (media termination point) or a conference port type as “conf bridge.”

The output for an 8-port T1/E1 PSTN interface module displays a transcoding port type as “transcoding” or a conference port type as “conferencing.”

The PAgP channel protocol and the LACP channel protocol manage channels differently. When all the ports in a channel get disabled, PAgP removes them from its internal channels list; **show** commands do not display the channel. With LACP, when all the ports in a channel get disabled, LACP does not remove the channel; **show** commands continue to display the channel even though all its ports are down. To determine if a channel is actively sending and receiving traffic with LACP, use the **show port** command to see if the link is up or down.

LACP does not support half-duplex links. If a port is in active/passive mode and becomes half duplex, the port is suspended (and a syslog message is generated). The port is shown as “connected” using the **show port** command and as “not connected” using the **show spantree** command. This discrepancy is because the port is physically connected but never joined spanning tree. To get the port to join spanning tree, either set the duplex to full or set the channel mode to off for that port.

For more information about PAgP and LACP, refer to the “Configuring EtherChannel” chapter of the *Catalyst 6000 Family Software Configuration Guide*.

Examples This example shows how to display the status and counters for a specific module and port:

```
Console> show port 1/1
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 1/1                     notconnect 1            full  1000 No GBIC


Port  Security Violation Shutdown-Time Age-Time Max-Addr Trap     IfIndex
----- -------- --------- ------------- -------- -------- -------- -------
 1/1  disabled  shutdown             0        0        1 disabled       3

Port  Num-Addr Secure-Src-Addr   Age-Left Last-Src-Addr     Shutdown/Time-Left
----- -------- ----------------- -------- ----------------- ------------------
 1/1         0                 -        -                 -        -         -

Port     Broadcast-Limit Broadcast-Drop
-------- --------------- --------------------
 1/1                   -                    0

Port   Send FlowControl    Receive FlowControl   RxPause TxPause Unsupported
       admin    oper       admin    oper                       opcodes
-----  -------- --------   -------- --------     ------- ------- -----------
 1/1   desired  off        off      off          0       0       0

Port  Status     Channel              Admin Ch
                 Mode                 Group Id
----- ---------- -------------------- ----- -----
 1/1  notconnect auto silent            112     0

Port  Align-Err  FCS-Err    Xmit-Err   Rcv-Err    UnderSize
----- ---------- ---------- ---------- ---------- ---------
 1/1           0          0          0          0         0

Port  Single-Col Multi-Coll Late-Coll  Excess-Col Carri-Sen Runts     Giants
----- ---------- ---------- ---------- ---------- --------- --------- ---------
 1/1           0          0          0          0         0         0         0

Last-Time-Cleared
--------------------------
Thu Feb 24 2000, 10:04:20
Console>
```

This example shows port information on a 48-port 10/100BASE-TX module with inline power:

```
Console> show port 9/5
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 9/5                     notconnect 1            auto  auto 10/100BaseTX

Port  AuxiliaryVlan AuxVlan-Status     InlinePowered     PowerAllocated
                                  Admin Oper   Detected mWatt mA @42V
----- ------------- -------------- ----- ------ -------- ----- --------
 9/5  none          none           auto  off    no       0     0


Port  Security Violation Shutdown-Time Age-Time Max-Addr Trap     IfIndex
----- -------- --------- ------------- -------- -------- -------- -------
 9/5  disabled  shutdown             0        0        1 disabled     126

Port  Num-Addr Secure-Src-Addr   Age-Left Last-Src-Addr     Shutdown/Time-Left
----- -------- ----------------- -------- ----------------- ------------------
 9/5         0                 -        -                 -        -         -
```

```
Port     Broadcast-Limit Broadcast-Drop
-------- --------------- --------------------
 9/5                   -                    0

Port   Send FlowControl    Receive FlowControl   RxPause TxPause Unsupported
       admin    oper       admin    oper                        opcodes
-----  -------- --------   -------- --------     ------- ------- -----------
 9/5   off      off        off      off          0       0       0

Port  Status     Channel              Admin Ch
                 Mode                 Group Id
----- ---------- -------------------- ----- -----
 9/5  notconnect auto silent            546     0

Port  Align-Err  FCS-Err    Xmit-Err   Rcv-Err    UnderSize
----- ---------- ---------- ---------- ---------- ---------
 9/5           0          0          0          0         0

Port  Single-Col Multi-Coll Late-Coll  Excess-Col Carri-Sen Runts     Giants
----- ---------- ---------- ---------- ---------- --------- --------- ---------
 9/5           0          0          0          0         0         0         0

Last-Time-Cleared
--------------------------
Wed Mar 15 2000, 21:57:31
Console>
```

This example shows the port information on an 8-port T1/E1 PSTN interface module configured for transcoding and conferencing:

```
Console> show port 7
----- ------------------ ---------- ---------- ------ ----- ------------
 7/1                     connected  123        full   1.544 T1
 7/2                     connected  2          full   1.544 T1
 7/3                     disable    1          full   1.544 T1
 7/4                     connected  11         full   1.544 T1
 7/5                     connected  123        full   1.544 T1
 7/6                     connected  1          full   1.544 T1
 7/7                     faulty     2          full   1.544 conf bridge
 7/8                     faulty     2          full   1.544 mtp

Port     DHCP    MAC-Address       IP-Address      Subnet-Mask
-------- ------- ----------------- --------------- ---------------
 7/1     enable  00-10-7b-00-0a-58 172.20.34.68    255.255.255.0
 7/2     enable  00-10-7b-00-0a-59 172.20.34.70    255.255.255.0
 7/3     enable  00-10-7b-00-0a-5a 172.20.34.64    255.255.255.0
 7/4     enable  00-10-7b-00-0a-5b 172.20.34.66    255.255.255.0
 7/5     enable  00-10-7b-00-0a-5c 172.20.34.59    255.255.255.0
 7/6     enable  00-10-7b-00-0a-5d 172.20.34.67    255.255.255.0
 7/7     enable  00-10-7b-00-0a-5e (Port host processor not online)
 7/8     enable  00-10-7b-00-0a-5f (Port host processor not online)

Port     Call-Manager(s)   DHCP-Server     TFTP-Sever      Gateway
-------- ----------------- --------------- --------------- ---------------
 7/1     172.20.34.207*    172.20.34.207   172.20.34.207   -
         callm.cisco.com
 7/2     172.20.34.207     172.20.34.207   172.20.34.207   172.20.34.20
 7/3     172.20.34.207     172.20.34.207   172.20.34.207   -
 7/4     172.20.34.207     172.20.34.207   172.20.34.207   -
 7/5     172.20.34.207     172.20.34.207   172.20.34.207   -
 7/6     172.20.34.207     172.20.34.207   172.20.34.207   -
 7/7     (Port host processor not online)
 7/8     (Port host processor not online)
```

```
Port     DNS-Server(s)   Domain
-------- --------------- --------------------------------------------------
 7/1     172.20.34.207   cisco.com
 7/2     172.20.34.207*  int.cisco.com
         171.69.45.34
         172.78.111.132
 7/3     172.20.34.207   -
 7/4     172.20.34.207   -
 7/5     172.20.34.207   -
 7/6     172.20.34.207   -
 7/7     (Port host processor not online)
 7/8     (Port host processor not online)

Port     CallManagerState DSP-Type
-------- ---------------- --------
 7/1     registered       C549
 7/2     registered       C549
 7/3     registered       C549
 7/4     registered       C549
 7/5     registered       C549
 7/6     notregistered    C549
 7/7     (Port host processor not online)
 7/8     (Port host processor not online)
Port  NoiseRegen NonLinearProcessing
----- ---------- -------------------
 7/1  disabled   disabled
 7/2  disabled   disabled
 7/3  disabled   disabled
 7/4  disabled   disabled
 7/5  enabled    disabled
 7/6  disabled   enabled
 7/7  (Port host processor not online)
 7/8  (Port host processor not online)

(*): Primary
Console>
```

This example show the port information on a 24-port FXS analog station interface services-configured module:

```
Console> (enable) show port 3
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 3/1                     onhook     1            full   64k FXS
 3/2                     onhook     1            full   64k FXS
 3/3                     onhook     1            full   64k FXS
 3/4                     onhook     1            full   64k FXS
 3/5                     onhook     1            full   64k FXS
 3/6                     onhook     1            full   64k FXS
 3/7                     onhook     1            full   64k FXS
 3/8                     onhook     1            full   64k FXS
 3/9                     onhook     1            full   64k FXS
 3/10                    onhook     1            full   64k FXS
 3/11                    onhook     1            full   64k FXS
 3/12                    onhook     1            full   64k FXS
 3/13                    onhook     1            full   64k FXS
 3/14                    onhook     1            full   64k FXS
 3/15                    onhook     1            full   64k FXS
 3/16                    onhook     1            full   64k FXS
 3/17                    onhook     1            full   64k FXS
 3/18                    onhook     1            full   64k FXS
 3/19                    onhook     1            full   64k FXS
 3/20                    onhook     1            full   64k FXS
 3/21                    onhook     1            full   64k FXS
```

```
 3/22                   onhook     1            full   64k FXS
 3/23                   onhook     1            full   64k FXS
 3/24                   onhook     1            full   64k FXS

Port     DHCP    MAC-Address       IP-Address      Subnet-Mask
-------- ------- ----------------- --------------- ---------------
 3/1-24  enable  00-10-7b-00-13-e4 172.20.34.50    255.255.255.0

Port     Call-Manager      DHCP-Server     TFTP-Sever      Gateway
-------- ----------------- --------------- --------------- ---------------
 3/1-24  172.20.34.207     172.20.34.207   172.20.34.207   -

Port     DNS-Server      Domain
-------- --------------- -------------------------
 3/1-24  172.20.34.207   -

Port     EchoCancel(ms) CallManagerState DSP-Type
-------- -------------- ---------------- --------
 3/1-24  4660           registered       C549

Port     ToneLocal     Impedance InputGain(dB) OutputAtten(dB)
-------- ------------- --------- ------------- ---------------
 3/1-24  northamerica  0         0             0

Port     RingFreq Timing    Timing         Timing    Timing
         (Hz)     Digit(ms) InterDigit(ms) Pulse(ms) PulseDigit(ms)
-------- -------- --------- -------------- --------- --------------
 3/1-24  20       100       100            0         0
Console> (enable)
```

Table 2-59 describes the possible fields (depending on the port type queried) in the **show port** command output.

Table 2-59 show port Command Output Fields

Field	Description
Port	Module and port number.
Name	Name (if configured) of the port.
Status	Status of the port (connected, notconnect, connecting, standby, faulty, inactive, shutdown, disabled, monitor, active, dot1p, untagged, inactive, or onhook).
Vlan	VLANs to which the port belongs.
Auxiliaryvlan[1]	Auxiliary VLANs to which the port belongs.
Duplex	Duplex setting for the port (auto, full, half).
Speed	Speed setting for the port (auto, 10, 100, 1000).
Type[2]	Port type (for example, 1000BASE-SX or 100BASE-FX, or T1, E1, transcoding, conferencing, mtp, or conf bridge for voice ports).
Security	Status of whether port security is enabled or disabled.
Secure-Src-Addr	Secure MAC address for the security-enabled port.
Last-Src-Addr	Source MAC address of the last packet received by the port.
Shutdown	Status of whether the port was shut down because of security.
Trap	Status of whether the port trap is enabled or disabled.
IfIndex	Number of the ifIndex.

Table 2-59 show port Command Output Fields (continued)

Field	Description
Broadcast-Limit	Broadcast threshold configured for the port.
Broadcast-Drop	Number of broadcast/multicast packets dropped because the broadcast limit for the port was exceeded.
Align-Err	Number of frames with alignment errors (frames that do not end with an even number of octets and have a bad CRC) received on the port.
FCS-Err	Number of valid size frames with FCS errors but no framing errors.
Xmit-Err	Number of transmit errors that occurred on the port (indicating that the internal transmit buffer is full).
Rcv-Err	Number of receive errors that occurred on the port (indicating that the internal receive buffer is full).
UnderSize	Number of received frames less than 64 octets long (but are otherwise well-formed).
Single-Coll	Number of times one collision occurred before the port transmitted a frame to the media successfully.
Multi-Coll	Number of times multiple collisions occurred before the port transmitted a frame to the media successfully.
Late-Coll	Number of late collisions (collisions outside the collision domain).
Excess-Col	Number of excessive collisions that occurred on the port (indicating that a frame encountered 16 collisions and was discarded).
Carri-Sen	Number of times the port sensed a carrier (to determine whether the cable is currently being used).
Runts	Number of received runt frames (frames that are smaller than the minimum IEEE 802.3 frame size) on the port.
Giants	Number of received giant frames (frames that exceed the maximum IEEE 802.3 frame size) on the port.
CE-State	Connection entity status.
Conn-State	Connection state of the port, as follows: • Disabled—The port has no line module or was disabled by the user. • Connecting—The port attempted to connect or was disabled. • Standby—The connection was withheld or was the inactive port of a dual-homing concentrator. • Active—The port made a connection. • Other—The concentrator was unable to determine the Conn-State.
Type	Type of port, such as A—A port and B—B port.

Table 2-59 show port Command Output Fields (continued)

Field	Description
Neig	Type of port attached to this port. The neighbor can be one of these types: • A—A port • B—B port • M—M port • S—Slave port • U—The concentrator cannot determine the type of the neighbor port.
Ler Con	Status of whether the port is currently in a LER condition.
Est	Estimated LER.
Alm	LER at which a link connection exceeds the LER alarm threshold.
Cut	LER cutoff value (the LER at which a link connection is flagged as faulty).
Lem-Ct	Number of LEM errors received on the port.
Lem-Rej-Ct	Number of times a connection was rejected because of excessive LEM errors.
Last-Time-Cleared	Last time the port counters were cleared.
Auto-Part	Number of times the port entered the auto-partition state due to excessive consecutive collisions.
Data-rate mismatch	Number of valid size frames that experienced overrun or underrun.
Src-addr change	Number of times the last source address changed.
Good-bytes	Total number of octets in frames with no error.
Short-event	Number of short events received.
InlinePowered[1]	InlinePowered for Admin (auto, on, off), Oper (on, off, denied), and Detected (yes, no).
PowerAllocated[1]	PowerAllocated for Watts (values displayed as Watts measurement) and Volts (values displayed as Volts measurement).
Age-Time[1]	Age timeout setting for the port.
Age-Left[1]	Age timeout remaining for the port.
Maximum-Addrs[1]	Maximum number of secured MAC addresses on the port.
CallManagerState[1]	Operational state of the voice port (Not Registered, Registered, Up, Down, and Alarm).
NoiseRegen[3]	Status of whether noise regeneration is enabled for the port.
NonLinear[3]	Status of whether nonlinear processing is enabled for the port.
Comp-Alg[3]	Type of compression algorithm used (for example G.711, G.723, and G.729).
IP-address[3]	IP address associated with the port.
Netmask[3]	Netmask associated with the port.

Table 2-59 show port Command Output Fields (continued)

Field	Description
MAC-Address[3]	MAC address associated with the port.
Call-Manager-IP[3]	Cisco CallManager IP address associated with the port.
DHCP-Server-IP[3]	DHCP server IP address associated with the port.
DNS-Server-IP[3]	DNS server IP address associated with the port.
TFTP-Server-IP[3]	TFTP server IP address associated with the port.

1. This field is applicable to the 48-port 10/100BASE-TX switching services-configured module.
2. This field changes according to the system configuration.
3. This field is applicable to the 8-port T1/E1 DSP services-configured module.

Related Commands

set port disable
set port enable
show port status

show port auxiliaryvlan

Use the **show port auxiliaryvlan** command to display the port auxiliary VLAN status for a specific port.

show port auxiliaryvlan {*vlan* | **untagged** | **dot1p** | **none**}

Syntax Description

vlan	Number of the VLAN; valid values are from **1** to **4094**.
untagged	Keyword to display the Cisco IP Phone 7960 that sends untagged packets without 802.1p priority.
dot1p	Keyword to display the Cisco IP Phone 7960 that sends packets with 802.1p priority.
none	Keyword to display the switch that does not send any auxiliary VLAN information in the CDP packets from that port.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

Examples

This example shows how to display the port information for a specific auxiliary VLAN:

```
Console> (enable) show port auxiliaryvlan
AuxiliaryVlan Status   Mod/Ports
------------- -------- ---------------------------------------------------
222           active   8/4-7
333           active   8/13-18
dot1p         dot1p    8/23,8/31-34
untagged      untagged 9/12
none          none     8/1-3,8/8-12,8/19-22,8/24-30,8/35-48,9/1-11,9/13-48
Console> (enable)
```

This example shows how to display the port information for a specific auxiliary VLAN:

```
Console> (enable) show port auxiliaryvlan 222
AuxiliaryVlan Status   Mod/Ports
------------- -------- ---------------------------------------------------
222           active   8/4-7
Console> (enable)
```

This example shows how to display the status of the switch that does not send any auxiliary VLAN information in the CDP packets:

```
Console> (enable) show port auxiliaryvlan none
AuxiliaryVlan Status   Mod/Ports
------------- -------- ---------------------------------------------------
none          none     8/1-3,8/8-12,8/19-22,8/24-30,8/35-48,9/1-11,9/13-48
Console> (enable)
```

This example shows how to display the status of the Cisco IP Phone 7960 that sends untagged packets without 802.1p priority:

```
Console> (enable) show port auxiliaryvlan untagged
AuxiliaryVlan Status   Mod/Ports
------------- -------- ---------------------------------------------------
untagged      untagged 9/12
Console> (enable)
```

This example shows how to display the status of the Cisco IP Phone 7960 that sends packets with 802.1p priority:

```
Console> (enable) show port auxiliaryvlan dot1p
AuxiliaryVlan Status   Mod/Ports
------------- -------- ---------------------------------------------------
dot1p         dot1p    8/23,8/31-34
Console> (enable)
```

Table 2-60 describes the possible fields (depending on the port type queried) in the **show port auxiliaryvlan** command output.

Table 2-60 show port auxiliaryvlan Command Output Fields

Field	Description
AuxiliaryVlan	Number of the auxiliary VLAN.
AuxVlanStatus	Status of the auxiliary VLAN.
Mod/Ports	Number of the module and ports assigned to the auxiliary VLAN.

Related Commands **set port auxiliaryvlan**

show port broadcast

Use the **show port broadcast** command to display broadcast information.

show port broadcast [*mod*[*/port*]]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not specify a *mod*, the ports on all modules are shown.

If you do not specify a *port*, all the ports on the module are shown.

On the 1000BASE-X switching module, when you specify a port for broadcast suppression, the traffic is suppressed only in the network-to-Catalyst 6000 family switch bus direction.

Examples

This example shows how to display broadcast information for port 2 on module 1:

```
Console> (enable) show port broadcast 1/2
Port     Broadcast-Limit Broadcast-Drop
-------- --------------- --------------------
1/2                20.00 %                  532
Console> (enable)
```

Table 2-61 describes the possible fields (depending on the port type queried) in the **show port broadcast** command output.

Table 2-61 show port broadcast Command Output Fields

Field	Description
Port	Module and port number.
Broadcast-Limit	Broadcast threshold configured for the port.
Broadcast-Drop	Number of broadcast or multicast packets dropped because the port broadcast limit was exceeded.

Related Commands

set port broadcast

show port capabilities

Use the **show port capabilities** command to display the capabilities on the ports.

show port capabilities [*mod*[/*port*]]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a *mod*, the ports on all modules are shown.

If you do not specify a *port*, all the ports on the module are shown.

Examples

This example shows how to list the port capabilities on a specific module and port:

```
Console> show port capabilities 1/1
Model                   WS-X6K-SUP2-2GE
Port                    1/1
Type                    Unknown GBIC
Speed                   1000
Duplex                  full
Trunk encap type        802.1Q,ISL
Trunk mode              on,off,desirable,auto,nonegotiate
Channel                 yes
Broadcast suppression   percentage(0-100)
Flow control            receive-(off,on,desired),send-(off,on,desired)
Security                yes
Dot1x                   yes
Membership              static,dynamic
Fast start              yes
QOS scheduling          rx-(1p1q4t),tx-(1p2q2t)
CoS rewrite             yes
ToS rewrite             DSCP
UDLD                    yes
Inline power            no
AuxiliaryVlan           no
SPAN                    source,destination
COPS port group         1/1-2
Link debounce timer     yes
Console>
```

This example shows the port capabilities on a 48-port 10/100BASE-TX switching services configured-module:

```
Console> show port capabilities 3/2
Model                   WS-X6248-RJ-45
Port                    3/2
Type                    10/100BaseTX
Speed                   auto,10,100
Duplex                  half,full
Trunk encap type        802.1Q,ISL
Trunk mode              on,off,desirable,auto,nonegotiate
Channel                 yes
Broadcast suppression   percentage(0-100)
Flow control            receive-(off,on),send-(off)
Security                yes
Membership              static
Fast start              yes
QOS scheduling          rx-((null)),tx-((null))
QOS classification      layer 2,layer 3
UDLD                    Capable
SPAN                    source,destination
Inline power            auto,on,off
Auxiliaryvlan           1..1000,dot1p,untagged,none
Console>
```

This example shows the port capabilities on an 8-port T1/E1 ISDN PRI services configured-module:

```
Console> show port capabilities 3/2
Model                   WS-X6608-T1   (or WS-X6608-E1)
Port                    3/2
Type                    T1, transcoding, conferencing
Speed                   1.544 Mps     (or 2.048Mps)
Duplex                  full
Channel                 no
Broadcast suppression   no
Flow control            no
Security                no
Membership              no
Fast start              no
QOS scheduling          no
QOS classification      no
UDLD                    no
Inline power            no
Auxiliaryvlan           no
Console>
```

This example shows the port capabilities on a 24-port FXS analog station interface services-configured module:

```
Console> show port capabilities 3/2
Model                   WS-X6624-FXS
Port                    3/2
Type                    FXS
Speed                   64kps
Duplex                  full
Trunk encap type        none
Trunk mode              off
Channel                 no
Broadcast suppression   no
Flow control            no
Security                no
Membership              no
Fast start              no
QOS scheduling          no
```

```
QOS classification       no
UDLD                     no
Inline power             no
Auxiliaryvlan            no
Console>
```

This example shows the port capabilities on an Intrusion Detection System Module:

```
Console> show port capabilities 5/2
Model                    WS-X6381-IDS
Port                     5/2
Type                     Intrusion Detection
Speed                    1000
Duplex                   full
Trunk encap type         no
Trunk mode               no
Channel                  no
Broadcast suppression    no
Flow control             no
Security                 no
Dot1x                    no
Membership               static
Fast start               no
QOS scheduling           rx-(none),tx-(none)
CoS rewrite              no
ToS rewrite              no
UDLD                     no
Inline power             no
AuxiliaryVlan            no
SPAN                     source
COPS port group          not supported
Link debounce timer      yes
Console>
```

Table 2-62 describes the possible fields (depending on the type of port queried) and the values in the **show port capabilities** command output.

Table 2-62 show port capabilities Command Output Fields

Field	Description
Model	Module model number.
Port	Module number and port number.
Type[1]	Port type (1000BASE-SX or 100BASE-FX).
Speed[1]	Speed setting for the port (auto, 10, 100, 1000).
Duplex	Duplex mode (half, full, auto).
Trunk encap type[2]	Trunk encapsulation type (ISL, 802.1Q, 802.10, or no).
Trunk mode[2]	Trunk administrative status of the port (on, off, auto, desirable, nonegotiate, or no).[3]
Channel	Status of which ports can form a channel group. The ports are shown in *mod/port* format. For example, 3/1-2 indicates module 3, ports 1 and 2. Also, any ports in range [*mod/1-mod/high_port*] or no ports may be indicated.
Broadcast suppression	Percentage of total available bandwidth that can be used by broadcast traffic (0–100).

Table 2-62 show port capabilities Command Output Fields (continued)

Field	Description
Flow control	Flow-control options you can set (receive-[off, on, desired], send-[off, on, desired], or no).
Security	Status of whether port security is enabled (yes, no).
Membership	Method of membership assignment of a port or range of ports to a VLAN (static, dynamic).
Fast start	Status of whether the spanning tree PortFast-start feature on the port is enabled (yes, no).
QOS scheduling	Status of whether the port supports QoS scheduling (yes, no).
QOS classification	Status of whether the port supports QoS classification (yes, no).
CoS rewrite	Status of whether the port supports CoS rewrite (yes, no).
SPAN	SPAN type supported.
ToS rewrite	Status of whether the port supports ToS rewrite (IP-Precedence).
UDLD	Status of whether the port is UDLD-capable or not.
Inline power[2]	Status of whether the port supports inline power (yes, no).
Auxiliaryvlan[2]	Status of whether the port supports voice VLANs (yes, no).
Link debounce timer	Status of whether the port supports debounce timer (yes, no).

1. This field will change depending on the module configuration.
2. This field is applicable to the 48-port 10/100BASE-TX switching services-configured module and the 24-port FXS analog station interface services-configured module.
3. "No" means that the port is trunk incapable.

Related Commands

set port broadcast
set port channel
set port security
set port speed
set spantree portfast
set trunk
show port
show port voice active

show port cdp

Use the **show port cdp** command to display the port CDP enable state and the message interval.

show port cdp [*mod*[*/port*]]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a *mod*, the ports on all modules are shown. If you do not specify a *port*, all the ports on the module are shown.

Examples

This example shows how to display CDP information for all ports:

```
Console> show port cdp
CDP               : enabled
Message Interval  : 60
Hold Time         : 180
Version           : V2

Port      CDP Status
--------  ----------
 1/1      enabled
 1/2      enabled
Console>
```

Table 2-63 describes the fields in the **show port cdp** command output.

Table 2-63 show port cdp Command Output Fields

Field	Description
CDP	Status of whether CDP is enabled or not.
Message-Interval	Interval between CDP message exchange with a neighbor.
Hold Time	Hold time setting.
Version	CDP version.
Port	Module and port number.
CDP Status	CDP status of the port (enabled, disabled).

Related Commands

set cdp
show cdp

show port channel

Use the **show port channel** command to display EtherChannel information.

show port channel [**all** | *mod*[*/port*]] [**statistics]**

show port channel [**all** | *mod*[*/port*]] {**info** [*type*]}

Syntax Description

all	(Optional) Keyword to display information about PAgP and LACP channels.
mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.
statistics	(Optional) Keyword to display statistics about the port (PAgP packets sent and received).
info	(Optional) Keyword to display port information such as speed, duplex status, priority, secure or dynamic status, and trunk status.
type	(Optional) Keyword to display feature-related parameters; valid values are **spantree**, **trunk**, **protcol**, **gmrp**, **gvrp**, **qos**, **rsvp, cops, dot1qtunnel, auxiliaryvlan**, and **jumbo**.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The protocol conditions are as follows:

- On indicates the port will receive all the flood traffic for that protocol.
- Off indicates the port will not receive any flood traffic for that protocol.
- Auto indicates the port will not receive any flood traffic for that protocol.

The GVRP registration status is defined as follows:

- Normal allows dynamic registering and deregistering each VLAN (except VLAN 1) on the port.
- Fixed supports manual VLAN creation and registration and prevents VLAN deregistration.
- Forbidden statically deregisters all the VLANs (except VLAN 1) from the port.

When you enter the **option** keyword with any of the options (**spantree** | **trunk** | **protcol** | **gmrp** | **gvrp** | **qos** | **rsvp** | **cops** | **dot1qtunnel** | **auxiliaryvlan** | **jumbo**), associated VLANs and the specified feature-related parameters are displayed.

If you do not specify a *mod* or a *port*, EtherChannel information is shown for all PAgP channeling ports on all modules.

If you enter the **all** keyword, information about PAgP and LACP channels is displayed.

Examples This example shows how to display Ethernet channeling information for module 1:

```
Console> show port channel 1
Port  Status     Channel   Admin Ch
                 Mode      Group Id
----- ---------- --------- ----- -----
 1/1  nonconnect on        195   769
 1/2  connected  on        195   769

Port  Device-ID                      Port-ID                  Platform
----- ------------------------------ ------------------------ ----------------
 1/1
 1/2
Console>
```

This example shows how to display port statistics:

```
Console> show port channel 4 statistics
Port  Admin   PAgP Pkts   PAgP Pkts PAgP Pkts PAgP Pkts PAgP Pkts PAgP Pkts PAgP Pkts
      Group   Transmitted Received  InFlush   RetnFlush OutFlush  InError
----- ------- ----------- --------- --------- --------- --------- ---------
 4/1       69          20         0         0         0         0         0
 4/2       69         105        60         0         0         0         0
 4/3      151           0         0         0        10         0         0
 4/4      151           0         5         0         0         0         0
 4/5       70           0         0         0         0         0         0
 4/6       70          42         0         0         2         0         0
 4/7      152           0        92         0         0         0         0
 4/8      152           0         0         0         0         0         0
Console>
```

This example shows how to display port information:

```
Console> show port channel 1 info
Switch Frame Distribution Method:mac both

Port  Status     Channel   Admin Channel Speed Duplex Vlan PortSecurity/
                 mode      group id                      Dynamic port
----- ---------- --------- ----- ------- ----- ------ ---- -------------
 1/1  notconnect auto          1       0 1000  full      1 -
 1/2  connected  auto          1       0 1000  full      1 -

Port  ifIndex Oper-group Neighbor   Oper-Distribution
                        Oper-group Method
----- ------- ---------- ---------- -----------------
 1/1  -               1            mac both
 1/2  -               2            mac both

Port  Device-ID                      Port-ID                  Platform
----- ------------------------------ ------------------------ ----------------
 1/1
 1/2

Port  Trunk-status Trunk-type    Trunk-vlans
----- ------------ ------------- -----------------------------------------------
 1/1  not-trunking negotiate     1-1005
 1/2  not-trunking negotiate     1-1005

Port  Portvlancost-vlans
----- --------------------------------------------------------------------------
 1/1
 1/2
```

```
Port  Port     Portfast Port    Port
      priority          vlanpri vlanpri-vlans
----- -------- -------- ------- ------------------------------------------------
 1/1        32 disabled       0
 1/2        32 disabled       0

Port  IP       IPX      Group
----- -------- -------- --------
 1/1  on       auto-on  auto-on
 1/2  on       auto-on  auto-on

Port  GMRP     GMRP         GMRP
      status   registration forwardAll
----- -------- ------------ ----------
 1/1  enabled  normal       disabled
 1/2  enabled  normal       disabled

Port  GVRP     GVRP          GVRP
      status   registeration applicant
----- -------- ------------- ---------
 1/1  disabled normal        normal
 1/2  disabled normal        normal

Port  Qos-Tx Qos-Rx Qos-Trust    Qos-DefCos
----- ------ ------ ------------ ----------
 1/1  2q2t   1q4t   untrusted             0
 1/2  2q2t   1q4t   untrusted             0
Console>
```

These examples show how to display feature-specific parameter information:

```
Console> (enable) show port channel 3 info spantree
Port  Port     Portfast Port    Port
      priority          vlanpri vlanpri-vlans
----- -------- -------- ------- ------------------------------------------------
3/1        32 disabled      12 2,4,90
3/2        32 disabled      12 2,4,90
3/3        32 disabled      12 2,4,90
3/4        32 disabled      12 2,4,90
Console>

Console> (enable) show port channel 3 info trunk
Port  Trunk-status Trunk-type    Trunk-vlans
----- ------------ ------------- ------------------------------------------------
3/1  not-trunking negotiate     1-1005
3/2  not-trunking negotiate     1-1005
3/3  not-trunking negotiate     1-1005
3/4  not-trunking negotiate     1-1005
Console>

Console> (enable) show port channel 3 info protcol
Port  IP       IPX      Group
----- -------- -------- --------
3/1  on       auto-on  auto-on
3/2  on       auto-on  auto-on
3/3  on       auto-on  auto-on
3/4  on       auto-on  auto-on
Console>
```

```
Console> (enable) show port channel 3 info gmrp
Port  GMRP     GMRP         GMPR
      status   registration forwardAll
----- -------- ------------ ----------
3/1  enabled  normal       disabled
3/2  enabled  normal       disabled
3/3  enabled  normal       disabled
3/4  enabled  normal       disabled
Console>

Console> (enable) show port channel 1 info gvrp
Port  GVRP     GVRP          GVRP
      status   registeration applicant
----- -------- ------------- ---------
1/1   disabled normal        normal
1/2   disabled normal        normal
Console>

Console> (enable) show port channel 1 info qos
Port  Qos-Tx   Qos-Rx   Qos-Trust    Qos-DefCos Qos-Interface
      PortType PortType Type                    Type
----- -------- -------- ------------ ---------- --------------
1/1   2q2t     1q4t     untrusted             0 port-based
1/2   2q2t     1q4t     untrusted             0 port-based
----- -------- -------- ------------ ---------- --------------

Port  ACL name                         Type
----- -------------------------------- ----
1/1                                    IP
                                       IPX
                                       MAC
1/2                                    IP
                                       IPX
                                       MAC
Port  Policy Source
----- -------------
1/1           COPS
1/2           COPS
Console>
```

Table 2-64 describes the possible fields (depending on the type of port queried) and the values in the **show port channel** command outputs.

Table 2-64 show port channel Command Outputs Fields

Field	Description
Port	Module and port number.
Status	Channeling status of the port (connected, notconnect).
Channel mode	Status of whether EtherChannel is on, off, auto, or desirable on the port.
Admin Group	Number of the admin group.
PAgP Pkts Transmitted	Number of PAgP packets transmitted.
PAgP Pkts Received	Number of PAgP packets received.
PAgP Pkts InFlush	Number of PAgP flush packets received.
PAgP Pkts RetnFlush	Number of PAgP flush packets returned.

Table 2-64 show port channel Command Outputs Fields (continued)

Field	Description
PAgP Pkts OutFlush	Number of PAgP flush packets transmitted.
PAgP Pkts InError	Number of PAgP error packets received.
Channel ID	Number of the channel group.
Neighbor device	Neighboring device with which the port is channeling.
Neighbor port	Port on the neighboring device with which the port is channeling.
Speed	Speed setting for the port (auto, 10, 100, 1000).
Duplex	Duplex setting for the port (auto, full, half).
Vlan	VLAN to which the port belongs.
Port priority	Priority associated with the port.
PortSecurity/Dynamic port	Status of whether the port is secure or dynamic.
ifIndex	Interface number to which the port belongs.
Oper-group	Capability of the group.
Neighbor device-id	Device ID of the neighboring device with which the port is channeling.
Neighbor port-id	Port ID of the neighboring device with which the port is channeling.
Neighbor Oper-group	Capability of the neighboring device.
Oper-Distribution	Frame distribution method operating status on a per-port basis (ip source, ip destination, ip both, mac source, mac destination, mac both, hotstandby-active, or hotstandby-idle).
Trunk-status	Status of whether the port is trunking or not.
Trunk-type	Type of trunk port.
Trunk-vlans	VLANs to which the port belongs.
Portvlancost-vlans	Port VLAN cost.
Portfast	Status of whether the PortFast-start mode is enabled or disabled.
Port vlanpri	Port VLAN priority.
Port vlanpri-vlans	Priority VLAN number.
IP	Status of the IP protocol (on, off, auto).
IPX	Status of the IPX protocol (on, off, auto).
Group	Status of the VINES, AppleTalk, and DECnet protocols (on, off, auto).
GMRP status	Status of whether GMRP is enabled or disabled.
GMRP registration	Status of the administrative control of an outbound port (normal, fixed, forbidden).
GMRP forward/all	Status of whether the Forward All feature is enabled or disabled.
GVRP status	Status of whether GVRP is enabled or disabled.

Table 2-64 show port channel Command Outputs Fields (continued)

Field	Description
GVRP registration	Status of the administrative control of an outbound port (normal, fixed, forbidden).
Qos-Tx	Transmit drop threshold.
Qos-Rx	Receive drop threshold.
Qos-Trust	Status of whether the port is trusted or untrusted.
Qos-DefCos	CoS value.
Qos Port-based	Status of whether the port is port-based QoS or not.
ACL name	Name of the ACL.
Policy Source	Type of policy source.
COPS Admin Roles	COPS admin role designation.
Dot1q tunnel mode	Status of the dot1q tunnel mode.
Jumbo	Status of the jumbo feature.
Auxiliaryvlan	Number of the auxiliary VLAN.
Protocol	Protocol associated with the port.

Related Commands

set port channel
show channel
show channel group

show port cops

Use the **show port cops** command to display COPS information on all or individual ports.

show port cops [*mod*[*/port*]]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a *mod* or a *port*, information is shown for all ports on all modules.

For a few minutes after a switchover from the active to the standby supervisor engine, note that if you enter the **show port cops** command, the output may be incorrect. If this is the case, the following warning displays:

```
COPS High Availability Switch Over in progress, hardware may be
programmed differently than as suggested by the output of these
commands.
```

Examples

This example shows how to display COPS information for all ports:

```
Console> show port cops
Port    Admin Roles                     Oper Roles
------  ------------------------------  ------------------------
 1/1    backbone_port                   backbone_port
        branch_office_port              -
        access_port                     -
 1/2    -                               -
 3/1    -                               -
 3/2    backbone_port                   backbone_port
 3/3    backbone_port                   backbone_port
 3/4    access_port                     access_port
 3/5    access_port                     branch_office_port
        backbone_port                   -
        branch_office_port              -
        net_port                        -
 3/6    access_port                     access_port
 3/7    -                               -
 3/8    -                               -
Console>
```

This example shows how to display COPS information for a specific port:

```
Console> show port cops 1/1
Port    Admin Roles                     Oper Roles
------  ------------------------------  -------------------------
 1/1    backbone_port                   backbone_port
        branch_office_port              -
        access_port                     -
 1/2    -                               -
Console>
```

Table 2-65 describes the fields displayed in the **show port cops** command output.

Table 2-65 show port cops Command Output Fields

Field	Description
Port	Module and port number.
Admin Roles	Administration role.
Oper Roles	Operating role.

Related Commands

clear port cops
set port cops

show port counters

Use the **show port counters** command to show all the counters for a port.

show port counters [*mod*[*/port*]]

Syntax Description

mod	(Optional) Number of the module for which to show port counter information.
port	(Optional) Number of the port on the module for which to show port counter information.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a *mod*, the ports on all modules are shown.

If you do not specify a *port*, all the ports on the module are shown.

Examples

This example shows counters for all ports:

```
Console> show port counters
Port  Align-Err  FCS-Err    Xmit-Err   Rcv-Err    UnderSize
----- ---------- ---------- ---------- ---------- ---------
 1/1           0          0          0          0         0
 1/2           0          0          0          0         0
 4/1           0          0          0          0         0
 4/2           0          0          0          0         0
 4/3           0          0          0          0         0
 4/4           0          0          0          0         0

Port  Single-Col Multi-Coll Late-Coll  Excess-Col Carri-Sen Runts     Giants
----- ---------- ---------- ---------- ---------- --------- --------- ---------
 1/1          12          0          0          0         0         0         -
 1/2           0          0          0          0         0         0         0
 4/1           0          0          0          0         0         0         0
 4/2           0          0          0          0         0         0         0
 4/3           0          0          0          0         0         0         0
 4/4           0          0          0          0         0         0         0

Last-Time-Cleared
--------------------------
Wed Jan 11 2000, 14:58:19
```

Table 2-66 describes the possible fields (depending on the port type queried) in the **show port counters** command output.

Table 2-66 show port counters Command Output Fields

Field	Description
Port	Module and port number.
Align-Err	Number of frames with alignment errors (frames that do not end with an even number of octets and have a bad CRC) received on the port.
FCS-Err	Number of frame check sequence errors that occurred on the port.
Xmit-Err	Number of transmit errors that occurred on the port (indicating that the internal transmit buffer is full).
Rcv-Err	Number of receive errors that occurred on the port (indicating that the internal receive buffer is full).
UnderSize	Number of received frames less than 64 octets long (but are otherwise well-formed).
Single-Coll	Number of times one collision occurred before the port successfully transmitted a frame to the media.
Multi-Coll	Number of times multiple collisions occurred before the port successfully transmitted a frame to the media.
Late-Coll	Number of late collisions (collisions outside the collision domain).
Excess-Col	Number of excessive collisions that occurred on the port (indicating that a frame encountered 16 collisions and was discarded).
Carri-Sen	Number of times the port sensed a carrier (to determine whether the cable is currently being used).
Runts	Number of received runt frames (frames that are smaller than the minimum IEEE 802.3 frame size) on the port.
Giants	Number of received giant frames (frames that exceed the maximum IEEE 802.3 frame size) on the port.
Last-Time-Cleared	Last time the port counters were cleared.

Related Commands

clear counters
show port

show port debounce

Use the **show port debounce** command to display whether the port debounce timers are enabled or disabled.

show port debounce [*mod* | *mod/port*]

Syntax Description

mod	(Optional) Number of the module.
mod/port	(Optional) Number of the module and the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a port, all ports are displayed.

Examples

This example shows how to display the debounce link timer for a specific port on a specific module:

```
Console> show port debounce 2/1
Port Debounce link timer
-----  ---------------
 2/1   disable
Console>
```

Related Commands

set port debounce

show port dot1qtunnel

Use the **show port dot1qtunnel** command to display the dot1q tunnel mode status.

show port dot1qtunnel [*mod*[*/port*]]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to display the dot1q tunnel mode status for a specific module:

```
Console> (enable) show port dot1qtunnel 4
Port   Dot1q tunnel mode
-----  -----------------
 4/1   access
 4/2   access
 4/3   access
 4/4   access
 4/5   trunk
 4/6   trunk
 4/7   trunk
 4/8   disabled
Console> (enable)
```

Related Commands

set port dot1qtunnel

show port dot1x

Use the **show port dot1x** command to display all the configurable and current state values associated with the authenticator PAE and backend authenticator and statistics for the different types of EAP packets transmitted and received by the authenticator on a specific port.

show port dot1x [*mod*[*/port*]]

show port dot1x statistics [*mod*[*/port*]]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.
statistics	Keyword to display statistics for different EAP packets transmitted and received by the authenticator on a specific port.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display all the configurable and current state values associated with the authenticator PAE and backend authenticator on a specific port:

```
Console> show port dot1x 3/3
Port  Auth-State          BEnd-State Port-Control        Port-Status
----- ------------------- ---------- ------------------- -------------
 3/3  force-authorized    idle       force-authorized    authorized
Port  Multiple-Host Re-authentication
----- ------------- -----------------
 3/3  disabled      disabled
Console>
```

This example displays the statistics of different types of EAP packets that are transmitted and received by the authenticator on a specific port:

```
Console> show port dot1x statistics 4/1,4/2
Port    Tx_Req/Id    Tx_Req    Tx_Total    Rx_Start    Rx_Logff     Rx_Resp/Id    Rx_Resp
4/1     1            2         4           2           0            1             0
4/2     3            4         6           0           1            1             0

Port    Rx_Invalid    Rx_Len_Err    Rx_Total    Last_Rx_Frm_Ver    Last_Rx_Frm_Src_Mac
4/1     0             0             3           1                  00-f0-3b-2b-d1-a9
4/2     0             0             3           1                  00-d0-62-95-7b-ff
Console>
```

Related Commands

clear dot1x config
set port dot1x
show dot1x

show port flowcontrol

Use the **show port flowcontrol** command to display per-port status information and statistics related to flow control.

show port flowcontrol [*mod*[/*port*]]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a *mod*, the ports on all modules are shown.

If you do not specify a *port*, all the ports on the module are shown.

Examples

This example shows how to display the flow-control port status and statistics for module 6:

```
Console> show port flowcontrol 6
Port   Send FlowControl    Receive FlowControl   RxPause    TxPause
       admin    oper       admin    oper
-----  -------- --------   -------- --------     ---------- ----------
 6/1   desired  off        off      off          0          0
 6/2   desired  off        off      off          0          0
 6/3   desired  off        off      off          0          0
 6/4   desired  off        off      off          0          0
 6/5   desired  off        off      off          0          0
 6/6   desired  off        off      off          0          0
 6/7   desired  off        off      off          0          0
 6/8   desired  off        off      off          0          0
Console>
```

Table 2-67 describes the fields in the **show port flowcontrol** command output.

Table 2-67 show port flowcontrol Command Output Fields

Field	Description
Port	Module and port number.
Send Flowcontrol Admin	Flow-control administration. Possible settings: on indicates the local port sends flow control to the far end; off indicates the local port does not send flow control to the far end; desired indicates the local end sends flow control to the far end if the far end supports it.
Send Flowcontrol Oper	Flow-control operation. Possible setting: on indicates flow control is operational; off indicates flow control is not operational; disagree indicates the two ports could not agree on a link protocol.
Receive Flowcntl Admin	Flow-control administration. Possible settings: on indicates the local port requires the far end to send flow control; off indicates the local port does not allow the far end to send flow control; desired indicates the local end allows the far end to send flow control.
Receive Flowcntl Oper	Flow-control operation. Possible setting: on indicates flow control is operational; off indicates flow control is not operational; disagree indicates the two ports could not agree on a link protocol.
RxPause	Number of Pause frames received.
TxPause	Number of Pause frames transmitted.

Related Commands **set port flowcontrol**

show port inlinepower

Use the **show port inlinepower** command to display the port power administration and operational status.

show port inlinepower [*mod*[/*port*]]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

An inline power-capable device can still be detected even if the inlinepower mode is set to off.

The Operational (Oper) status field descriptions are as follows:

- on—Power is being supplied by the port.
- off—Power is not being supplied by the port.
- denied—The system does not have enough available power for the port; power is not being supplied by the port.
- faulty—The port is unable to provide power to the connected device.

Examples

This example shows how to display the inline power for multiple ports on a specific module:

```
Console> show port inlinepower 3/2-6
Default Inline Power allocation per port: 9.500 Watts (0.22 Amps @42V)
Total inline power drawn by module 3: 0 Watt
Port      InlinePowered     PowerAllocated
      Admin Oper   Detected mWatt mA @42V
----- ----- ------ -------- ----- --------
 3/2  auto  on     yes      10.00 0.250
 3/3  auto  on     yes      9.8   0.198
 3/4  auto  denied yes      0     0
 3/5  off   off    no       0     0
 3/6  off   off    yes      0     0
Console>
```

Related Commands

set inlinepower defaultallocation
set port inlinepower
show environment

show port jumbo

Use the **show port jumbo** command to display the jumbo frame settings for all ports with the feature enabled.

show port jumbo

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the jumbo frame settings for ports with the feature enabled:

```
Console> show port jumbo
Jumbo frames MTU size is 9216 bytes.
Jumbo frames enabled on port(s) 6/1-2,7/1-8.
Console>
```

This example shows the display if the jumbo frame feature could not be enabled on some ports at system startup:

```
Console> show port jumbo
Jumbo frames MTU size is 9216 bytes.
Jumbo frames enabled on port(s) 6/1-2.
Jumbo frames are in an inconsistent state on port(s) 7/1-8
Console>
```

Related Commands

set port jumbo

show port lacp-channel

Use the **show port lacp-channel** command to display information about LACP channels by port or module number.

show port lacp-channel [*mod*[/*port*]] [**statistics**]

show port lacp-channel [*mod*[/*port*]] **info** [*type*]

Syntax Description

mod[/*port*]	(Optional) Number of the module and the (optional) port number on the module.
statistics	(Optional) Keyword to display the LACP channel statistics.
info	Keyword to display detailed LACP channel information.
type	(Optional) Keyword to display feature-related parameters; valid values are **auxiliaryvlan**, **cops**, **dot1qtunnel**, **gmrp**, **gvrp**, **jumbo**, **protocol**, **qos**, **rsvp**, **spantree**, **trunk**..

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not enter a module or a port number, information about all modules is displayed.

If you enter the module number only, information about all ports on the module is displayed.

For differences between PAgP and LACP, refer to the "Guidelines for Port Configuration" section of the "Configuring EtherChannel" chapter of the *Catalyst 6000 Family Software Configuration Guide*.

Examples

This example shows how to display LACP channel information for all system modules:

```
Console> show port lacp-channel
Port  Channel   Admin Ch    Partner Oper                        Partner
      Mode       Key  Id    Sys ID                              Port
----- --------- ----- ----- ----------------------------------- -----
 2/1  active    143   768   1276,45-12-24-AC-78-90              5/1
 2/2  active    143   768   1276,45-12-24-AC-78-90              5/2
----- --------- ----- ----- ----------------------------------- -----
 4/3  passive   151   769   13459,89-BC-24-56-78-90             1/1
 4/4  passive   151   769   13459,89-BC-24-56-78-90             1/2
----- --------- ----- ----- ----------------------------------- -----
 4/7  passive   152   770   8000,AC-12-24-56-78-90              4/3
 4/8  passive   152   770   8000,AC-12-24-56-78-90              4/4
----- --------- ----- ----- ----------------------------------- -----
Console>
```

This example shows how to display LACP channel information for all ports on module 4:

```
Console> show port lacp-channel 4
Port  Channel   Admin Ch    Partner Oper                          Partner
      Mode       Key  Id    Sys ID                                Port
----- --------- ----- ----- ------------------------------------ -----
 4/1  active    69    0     0,00-00-00-00-00-00                   3/1
 4/2  active    69    0     0,00-00-00-00-00-00                   4/5
 4/3  passive   151   769   13459,89-BC-24-56-78-90               1/1
 4/4  passive   151   769   13459,89-BC-24-56-78-90               1/2
 4/5  active    70    0     0,00-00-00-00-00-00                   7/3
 4/6  active    70    0     0,00-00-00-00-00-00                   7/4
 4/7  passive   152   770   8000,AC-12-24-56-78-90                4/3
 4/8  passive   152   770   8000,AC-12-24-56-78-90                4/4
Console>
```

This example shows how to display LACP channel information for port 7 on module 4:

```
Console> show port lacp-channel 4/7
Port  Channel   Admin Ch    Partner Oper                          Partner
      Mode       Key  Id    Sys ID                                Port
----- --------- ----- ----- ------------------------------------ -----
 4/7  passive   152   770   8000,AC-12-24-56-78-90                4/3
 4/8  passive   152   770   8000,AC-12-24-56-78-90                4/4
Console>
```

This example shows how to display detailed LACP channel information for port 7 on module 4:

```
Console> show port lacp-channel 4/7 info
I = Isolated Port.  C = Channeling Port.  N = Not Connected.
H = Hot Stand-by Port.  S = Suspended Port.

Port  LACP Port Port  Speed Duplex Vlan Trunk status Port  STP Port PortSecurity/
      Priority  Status                              Cost  Priority Dynamic port
----- --------- ------ ----- ------ ---- ------------ ----- -------- -------------
 4/7  130       C      1000  full   1    not-trunking     4       32
 4/8  131       C      1000  full   1    not-trunking     4       32

Port  Admin Channel_id ifIndex Partner Oper            Partner    Partner  Partner
       Key                     Sys ID                 Port prior port     Oper Key
----- ----- ---------- ------- ---------------------- ---------- -------- ----------
 4/7  152   770        31      8000,AC-12-24-56-78-90  248         4/3      15678
 4/8  152   770        31      8000,AC-12-24-56-78-90  249         4/4      15768
Console>
```

This example shows how to display LACP channel statistics for all ports on module 4:

```
Console> show port lacp-channel 4 statistics
Port  Admin    LACP Pkts  LACP Pkts Marker Pkts Marker Pkts LACP Pkts
       Key    Transmitted Received  Transmitted   Received    Errors
----- ------- ----------- --------- ----------- ----------- ---------
 4/1       69          20         0           0           0         0
 4/2       69         105        60           0           0         0
 4/3      151           0         0           0          10         0
 4/4      151           0         5           0           0         0
 4/5       70           0         0           0           0         0
 4/6       70          42         0           0           2         0
 4/7      152           0        92           0           0         0
 4/8      152           0         0           0           0         0
Console>
```

This example shows how to display LACP channel statistics for port 7 on module 4:

```
Console> show port lacp-channel 4/7 statistics
Port  Admin    LACP Pkts  LACP Pkts Marker Pkts Marker Pkts LACP Pkts
       Key    Transmitted Received  Transmitted   Received    Errors
----- ------- ----------- --------- ----------- ----------- ---------
 4/7      152           0        92           0           0         0
 4/8      152           0         0           0           0         0
Console>
```

Examples

clear lacp-channel statistics
set channelprotocol
set lacp-channel system-priority
set port lacp-channel
set spantree channelcost
set spantree channelvlancost
show lacp-channel

show port mac

Use the **show port mac** command to display port MAC counter information.

show port mac [*mod*[/*port*]]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display port MAC counter information for a specific module:

```
Console> show port mac 1

Port     Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast
-------- -------------------- -------------------- --------------------
 1/1                      0                    0                    0
 1/2                      0                    0                    0
 1/3                      0                    0                    0
 1/4                      0                    0                    0

Port     Xmit-Unicast         Xmit-Multicast       Xmit-Broadcast
-------- -------------------- -------------------- --------------------
 1/1                      0                    0                    0
 1/2                      0                    0                    0
 1/3                      0                    0                    0
 1/4                      0                    0                    0

Port     Rcv-Octet            Xmit-Octet
-------- -------------------- --------------------
 1/1                      0                    0
 1/2                      0                    0
 1/3                      0                    0
 1/4                      0                    0

MAC      Dely-Exced MTU-Exced  In-Discard Lrn-Discrd In-Lost    Out-Lost
-------- ---------- ---------- ---------- ---------- ---------- ----------
 1/1              0          0          0          0          0          0
 1/2              0          0          0          0          0          0
 1/3              0          0          0          0          0          0
 1/4              0          0          0          0          0          0

Last-Time-Cleared
--------------------------
Fri Sep 1 2000, 20:03:06
Console>
```

Table 2-68 describes the possible fields in the **show port mac** command output.

Table 2-68 show port mac Command Output Fields

Field	Description
Rcv-Unicast	Number of unicast frames received on the port.
Rcv-Multicast	Number of multicast frames received on the port.
Rcv-Broadcast	Number of broadcast frames received on the port.
Xmit-Unicast	Number of unicast frames transmitted by the port.
Xmit-Multicast	Number of multicast frames transmitted by the port.
Xmit-Broadcast	Number of broadcast frames transmitted by the port.
Rcv-Octet	Number of octet frames received on the port.
Xmit-Octet	Number of octet frames transmitted on the port.
Dely-Exced	Number of transmit frames aborted due to excessive deferral.
MTU-Exced	Number of frames for which the MTU size was exceeded.
In-Discard	Number of incoming frames that were discarded because the frame did not need to be switched.
Out-Discard	Number of outbound packets chosen to be discarded even though no errors had been detected to prevent their being transmitted.
In-Lost	Number of incoming frames.
Out-Lost	Number of outbound packets.

Related Commands **clear counters**

show port mac-address

Use the **show port mac-address** command to display the MAC address associated with a physical port or ports.

show port mac-address [*mod*[/*port*]]

Syntax Description

mod[/*port*]	(Optional) Number of the module and optionally, the number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a module number, the MAC addresses for all ports on all modules are shown. If you specify a module number but no port number, the MAC addresses for all ports on the specified module are shown.

Examples

This example shows how to display the MAC address for port 1 on module 2:

```
Console> show port mac-address 2/1
Port  Mac address
----- ---------------------
 2/1  00-50-3e-7e-71-3c
Console>
```

This example shows how to display the MAC addresses for all ports on module 2:

```
Console> show port mac-address 2
Port  Mac address
----- ---------------------
 2/1  00-50-3e-7e-71-3c
 2/2  00-50-3e-7e-71-3d
Console>
```

This example shows how to display the MAC addresses for all ports on all modules:

```
Console> show port mac-address
Port  Mac address
----- ---------------------
 2/1  00-50-3e-7e-71-3c
 2/2  00-50-3e-7e-71-3d
```

```
Port  Mac address
----- ----------------------
 5/1  00-d0-d3-33-80-9c
 5/2  00-d0-d3-33-80-9d
.
.
.
 5/48 00-d0-d3-33-80-cb

Port  Mac address
----- ----------------------
 7/1  00-50-54-6c-94-9c
 7/2  00-50-54-6c-94-9d
 7/3  00-50-54-6c-94-9e
 7/4  00-50-54-6c-94-9f
 7/5  00-50-54-6c-94-a0
 7/6  00-50-54-6c-94-a1
 7/7  00-50-54-6c-94-a2
 7/8  00-50-54-6c-94-a3
Console>
```

show port negotiation

Use the **show port negotiation** command to display the link negotiation protocol setting for the specified port.

show port negotiation [*mod*[/*port*]]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This command is not supported on WS-X6316-GE-TX and on WS-X6516-GE-TX.

Examples

This example shows how to display the link negotiation protocol settings on module 3, port 1:

```
Console> show port negotiation 3/1
Port     Link Negotiation
------- --------------------
3/1      enabled
Console>
```

Related Commands

set port negotiation
show port flowcontrol

show port protocol

Use the **show port protocol** command to view protocol filters configured on the EtherChannel ports.

show port protocol [*mod*[/*port*]]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a *port* value, filters configured on all the ports on the module are shown.

Examples

This example shows how to view protocol filters on configured ports:

```
Console> show port protocol
Port     Vlan       IP       IP Hosts IPX      IPX Hosts Group    Group Hosts
-------- ---------- -------- -------- -------- --------- -------- -----------
1/1      1          on       0        on       0         on       0
1/2      1          on       0        on       0         on       0
2/1      1          on       3        auto-on  0         auto-on  0
2/2      1          on       0        on       0         on       0
2/3      1          on       0        on       0         on       0
2/4      1          on       0        on       0         on       0
2/5      1          on       0        on       0         on       0
2/6      1          on       0        on       0         on       0
2/7      1          on       0        on       0         on       0
2/8      1          on       0        on       0         on       0
2/9      1          on       0        on       0         on       0
2/10     1          on       0        on       0         on       0
2/11     1          on       0        on       0         on       0
2/12     1          on       0        on       0         on       0
Console>
```

Related Commands

set port protocol

show port qos

Use the **show port qos** command to display QoS-related information.

show port qos [*mod*[*/port*]]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

Note When a switchover occurs, you cannot view the ACLs and policers deployed using COPS-DS until the COPS-DS client on the new active supervisor engine establishes connection to the PDP and downloads the QoS policy. The runtime fields in the output display will be blank until QoS policy is downloaded to the new active supervisor engine.

Examples

This example shows how to display QoS-related information for a specific module and port:

```
Console> show port qos 2/1
QoS is enabled for the switch.
QoS policy source for the switch set to local.

Port  Interface Type Interface Type Policy Source Policy Source
      config         runtime        config        runtime
----- -------------- -------------- ------------- -------------
2/1      vlan-based     vlan-based          COPS         local

Port  TxPort Type  RxPort Type  Trust Type   Trust Type   Def CoS Def CoS
                                config       runtime      config  runtime
----- ------------ ------------ ------------ ------------ ------- -------
2/1          2q2t         1q4t    untrusted    untrusted       0

Config:
Port  ACL name                         Type
----- -------------------------------- ----
No ACL is mapped to port 2/1.
```

```
Runtime:
Port  ACL name                          Type
----- ------------------------------- ----
No ACL is mapped to port 2/1.
Console>
```

This example shows how to display QoS-related information for a single port on a specific module, which, in this example, is connected to a port on a phone device:

```
Console> (enable) show port qos 3/4
QoS is disabled for the switch.
Configured settings are not used.
QoS policy source for the switch set to local.

Port  Interface Type Interface Type Policy Source Policy Source
      config         runtime        config        runtime
----- -------------- -------------- ------------- -------------
 3/4               -              -         local         local

Port  TxPort Type  RxPort Type  Trust Type   Trust Type    Def CoS Def CoS
                                config       runtime       config  runtime
----- ------------ ------------ ------------ ------------- ------- -------
 3/4          2q2t         1q4t    untrusted    trust-cos        0       0
Port  Ext-Trust Ext-Cos
----- --------- -------
 3/4  untrusted       0

(*)Trust type set to untrusted.

Config:
Port  ACL name                          Type
----- ------------------------------- ----
No ACL is mapped to port 3/4.

Runtime:
Port  ACL name                          Type
----- ------------------------------- ----
No ACL is mapped to port 3/4.
Console> (enable)
```

Related Commands

- **set port qos**
- **set port qos cos**
- **set port qos trust**

show port rsvp

Use the **show port rsvp** command to display RSVP information on a per-port basis.

show port rsvp [*mod*[*/port*]]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display RSVP information for a specific port:

```
Console> (enable) show port rsvp 2
Port  DSBM     Managed Configured Elected DSBM DSBM IP Address
      Election Segment Priority   Priority
----- -------- ------- ---------- ------------ ---------------
 2/1   enabled     yes        232          232    171.21.34.25
 2/2  disabled      no        128            -               -
Console> (enable)
```

Related Commands

set port rsvp dsbm-election

show port security

Use the **show port security** command to view port security configuration information and statistics.

show port security [*mod*[*/port*]]

show port security statistics {*mod*[*/port*]}

show port security statistics system

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.
statistics	Keyword to display security statistics.
system	Keyword to display system-wide configuration information.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display port security configuration information on a specific port that is a secured port:

```
Console> (enable) show port security 4/1
Port  Security Violation Shutdown-Time Age-Time Maximum-Addrs Trap     IfIndex
----- -------- --------- ------------- -------- ------------- -------- -------
 4/1  enabled  shutdown  120           1440     25            disabled 3

Port Secure-Src-Addrs  Age-Left Last-Src-Addr     Shutdown Shutdown-Time-Left
---- ----------------- -------- ----------------- -------- ------------------
 4/1 00-11-22-33-44-55 4        00-11-22-33-44-55 No       -
     00-10-14-da-77-f1 100
Console> (enable)
```

This example shows the display on a port that has experienced a security violation:

```
Console> (enable) show port security 4/1
Port  Security Violation Shutdown-Time Age-Time Maximum-Addrs Trap     IfIndex
----- -------- --------- ------------- -------- ------------- -------- -------
 4/1  enabled  shutdown  120           600      25            disabled 3

Port Secure-Src-Addrs  Age-Left Last-Src-Addr     Shutdown Shutdown-Time-Left
---- ----------------- -------- ----------------- -------- ------------------
 4/1 00-11-22-33-44-55 60       00-11-22-33-44-77 Yes      -
     00-10-14-da-77-f1 200
     00-11-22-33-44-66 200
Console> (enable)
```

This example shows that port 4/1 has been shut down and that the timeout left is 60 minutes before the port will be reenabled:

```
Console> (enable) show port security 4/1
Port  Security Violation Shutdown-Time Age-Time Maximum-Addrs Trap     IfIndex
----- -------- --------- ------------ -------- ------------- -------- -------
 4/1  enabled  restrict  120          600      25            disabled 3

Port Secure-Src-Addrs  Age-Left Last-Src-Addr     Shutdown Shutdown-Time-Left
---- ----------------- -------- ----------------- -------- ------------------
 4/1 00-11-22-33-44-55 60       00-11-22-33-44-77 Yes      -
     00-10-14-da-77-ff
Console> (enable)
```

This example shows how to display system-wide configuration information:

```
Console> (enable) show port security statistics system
Module 1:
  Total ports: 2
  Total secure ports: 0
  Total MAC addresses: 2
  Total global address space used (out of 1024): 0
  Status: installed
Module 2:
  Total ports: 1
  Total secure ports: 0
  Total MAC addresses: 0
  Total global address space used (out of 1024): 0
  Status: removed
Module 3:
  Module does not support port security feature
Module 5:
  Total ports: 48
  Total secure ports: 0
  Total MAC addresses: 48
  Total global address space used (out of 1024): 0
  Status: installed
Module 15:
  Module does not support port security feature
Total secure ports in the system: 0
Console> (enable)
```

This example shows how to display security statistical information for a specific module:

```
Console> (enable) show port security statistics 2
Port  Total-Addrs Maximum-Addrs
----- ----------- -------------
Module 2:
  Total ports: 1
  Total secure ports: 0
  Total MAC addresses: 0
  Total global address space used (out of 1024): 0
  Status: removed
Console> (enable)
```

Related Commands clear port security
set port security

show port spantree

Use the **show port spantree** command to view port spanning tree information.

show port spantree [*mod*[*/port*]]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a *mod* value, the ports on all modules are shown. If you do not specify a *port* value, all the ports on the module are shown.

Examples

This example shows how to display spanning tree information on a specific module:

```
Console> (enable) show port spantree 5
Port(s)                  Vlan Port-State    Cost      Prio Portfast Channel_id
------------------------ ---- ------------ --------- ---- -------- ----------
5/1                      1    not-connected   2684354   32 disabled 0
5/2                      1    not-connected   2684354   32 disabled 0
5/3                      1    not-connected   2684354   32 disabled 0
5/4                      1    not-connected   2684354   32 disabled 0
5/5                      1    not-connected   2684354   32 disabled 0
5/6                      1    not-connected   2684354   32 disabled 0
5/7                      1    not-connected   2684354   32 disabled 0
5/8                      1    not-connected   2684354   32 disabled 0
5/9                      1    forwarding       268435   32 disabled 0
.
.
.
```

Related Commands

show spantree

show port status

Use the **show port status** command to display port status information.

show port status [*mod*[*/port*]]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a *mod* value, the ports on all modules are shown. If you do not specify a *port* value, all the ports on the module are shown.

Examples

This example shows how to display port status information for all ports:

```
Console> show port status
Port  Name               Status     Vlan      Duplex Speed  Type
----- ------------------ ---------- ---------- ------ ------ ------------
 1/1                     connected  52         half   100    100BaseTX
 1/2                     notconnect            half   100    100BaseTX
Console>
```

Table 2-69 describes the fields in the **show port status** command output.

Table 2-69 show port status Command Output Fields

Field	Description
Port	Module and port number.
Name	Name (if configured) of the port.
Status	Status of the port (connected, notconnect, connecting, standby, faulty, inactive, shutdown, disabled, or monitor).
Vlan	VLANs to which the port belongs.
Duplex	Duplex setting for the port (auto, full, half).
Speed	Speed setting for the port (auto, 10, 100, 1000).
Type[1]	Port type (100BASE-TX).

1. These fields will change according to the system configuration.

show port sync-restart-delay

Use the **show port sync-restart-delay** command to display a port's synchronization restart delay.

show port sync-restart-delay [*mod*[*/port*]]

Syntax Description

mod	(Optional) Number of the module and the port on the module.
port	(Optional) Number of the port on the module

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The **set port sync-restart-delay** and **show port sync-restart-delay** commands are available in both binary mode and text configuration mode, but the synchronization delay you specify is only saved in text configuration mode.

Examples

This example shows how to display the synchronization restart delay for a specific port:

```
Console> show port sync-restart-delay 2/1
Port   Sync restart delay in ms
-----  ------------------------
 2/1   210
Console>
```

Related Commands

clear config
set port sync-restart-delay

show port trap

Use the **show port trap** command to display port trap status.

show port trap [*mod*[*/port*]]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a *mod* value, the ports on all modules are shown. If you do not specify a *port* value, all the ports on the module are shown.

Examples

This example shows how to display the port trap status for a specific module:

```
Console> show port trap 1

Port   Trap
-----  --------
 1/1   disabled
 1/2   enabled
 1/3   disabled
 1/4   disabled
Console>
```

Related Commands

set port trap

show port trunk

Use the **show port trunk** command to display port trunk information.

show port trunk [*mod*[*/port*]]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a *mod* value, the ports on all modules are shown. If you do not specify a *port* value, all the ports on the module are shown.

Examples

This example shows how to display trunking information for a specific port:

```
Console> (enable) show port trunk 4/5
* - indicates vtp domain mismatch

Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 4/5      nonegotiate  dot1q          trunking      1

Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------------
 4/5      1-1005

Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------------
 4/5      1-3,1003,1005

Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------------
 4/5      1005
Console> (enable)
```

Table 2-70 describes the fields in the **show port trunk** command output.

Table 2-70 show port trunk Command Output Fields

Field	Description
Port	Module and port numbers.
Mode	Trunk administrative status of the port (on, off, auto, or desirable).
Encapsulation	Trunking type configured by administration.
Status	Status of whether the port is trunking or nontrunking.
Native VLAN	Number of the native VLAN for the trunk link (for 802.1Q trunks, the VLAN for which untagged traffic can be transmitted and received over the trunk; for ISL trunks, packets are tagged on all VLANs, including the native VLAN).
Vlans allowed on trunk	Range of VLANs allowed to go on the trunk (default is 1 to 1000).
Vlans allowed and active in management domain	Range of active VLANs within the allowed range.
Vlans in spanning tree forwarding state and not pruned	Range of VLANs that actually go on the trunk with Spanning Tree Protocol forwarding state.

Related Commands **set trunk**

show port voice

Use the **show port voice** command to display voice port information.

show port voice [**noalias**]

Syntax Description

noalias	(Optional) Keyword to force the display to show IP addresses, not IP aliases.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This command is not supported by the NAM.

Examples

This example shows how to display voice port information:

```
Console> show port voice
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 7/1                     connected  100          full     1 T1
 7/2                     notconnect 100          full     1 T1
 7/3                     connected  100          full     1 T1
 7/4                     connected  100          full     1 T1
 7/5                     notconnect 100          full     1 T1

Port     DHCP    MAC-Address       IP-Address      Subnet-Mask
-------- ------- ----------------- --------------- ---------------
 7/1     disable 00-e0-b0-ff-31-c0 sjcf-12a-sw1-p7 255.255.254.0
 7/2     disable 00-e0-b0-ff-31-c1 sjcf-12a-sw1-p7 255.255.254.0
 7/3     disable 00-e0-b0-ff-31-c2 sjcf-12a-sw1-p7 255.255.254.0
 7/4     disable 00-e0-b0-ff-31-c3 sjcf-12a-sw1-p7 255.255.254.0
 7/5     disable 00-e0-b0-ff-31-c4 sjcf-12a-sw1-p7 255.255.254.0

Port     Call-Manager(s)   DHCP-Server     TFTP-Server     Gateway
-------- ----------------- --------------- --------------- ---------------
 7/1     gigantic-2.cisc*  -               10.34.1.11      10.34.10.1
         10.34.1.11
 7/2     10.34.16.10*      -               10.34.1.11      10.34.10.1
         10.34.1.11
 7/3     10.34.16.10*      -               10.34.1.11      10.34.10.1
         10.34.1.11
 7/4     10.34.16.10*      -               10.34.1.11      10.34.10.1
         10.34.1.11
 7/5     10.34.1.11*       -               10.34.1.11      10.34.10.1
         10.34.16.10
         10.34.42.11
(*):Primary
```

```
Port     DNS-Server(s)     Domain
-------- ----------------- ------------------------------------------------
 7/1     dns-sj3.cisco.c*  cisco.com
         dns-sj4.cisco.c
 7/2     dns-sj3.cisco.c*  cisco.com
         dns-sj4.cisco.c
 7/3     dns-sj3.cisco.c*  cisco.com
         dns-sj4.cisco.c
 7/4     dns-sj3.cisco.c*  cisco.com
         dns-sj4.cisco.c
 7/5     dns-sj3.cisco.c*  cisco.com
         dns-sj4.cisco.c
(*):Primary

Port     CallManagerState DSP-Type
-------- ---------------- --------
 7/1     registered       C549
 7/2     registered       C549
 7/3     registered       C549
 7/4     registered       C549
 7/5     registered       C549

Port  NoiseRegen NonLinearProcessing
----- ---------- -------------------
 7/1  enabled    enabled
 7/2  enabled    enabled
 7/3  enabled    enabled
 7/4  enabled    enabled
 7/5  enabled    enabled
Console>
```

This example shows how to display voice port information without displaying the IP address in DNS name format:

```
Console> show port voice noalias
Port  Name                 Status     Vlan       Duplex Speed Type
----- -------------------- ---------- ---------- ------ ----- ------------
 7/1                       connected  100          full     1 T1
 7/2                       notconnect 100          full     1 T1
 7/3                       connected  100          full     1 T1
 7/4                       connected  100          full     1 T1
 7/5                       notconnect 100          full     1 T1

Port     DHCP    MAC-Address       IP-Address      Subnet-Mask
-------- ------- ----------------- --------------- ---------------
 7/1     disable 00-e0-b0-ff-31-c0 10.34.10.11     255.255.254.0
 7/2     disable 00-e0-b0-ff-31-c1 10.34.10.12     255.255.254.0
 7/3     disable 00-e0-b0-ff-31-c2 10.34.10.13     255.255.254.0
 7/4     disable 00-e0-b0-ff-31-c3 10.34.10.14     255.255.254.0
 7/5     disable 00-e0-b0-ff-31-c4 10.34.10.15     255.255.254.0

Port     Call-Manager(s)   DHCP-Server     TFTP-Server     Gateway
-------- ----------------- --------------- --------------- ---------------
 7/1     10.34.16.10*      -               10.34.1.11      10.34.10.1
         10.34.1.11
 7/2     10.34.16.10*      -               10.34.1.11      10.34.10.1
         10.34.1.11
 7/3     10.34.16.10*      -               10.34.1.11      10.34.10.1
         10.34.1.11
 7/4     10.34.16.10*      -               10.34.1.11      10.34.10.1
         10.34.1.11
```

```
 7/5     10.34.1.11*       -               10.34.1.11      10.34.10.1
         10.34.16.10
         10.34.42.11
(*):Primary

Port     DNS-Server(s)     Domain
-------- ----------------- ------------------------------------------------
 7/1     171.68.10.70*     cisco.com
         171.68.10.140
 7/2     171.68.10.70*     cisco.com
         171.68.10.140
 7/3     171.68.10.70*     cisco.com
         171.68.10.140
 7/4     171.68.10.70*     cisco.com
         171.68.10.140
 7/5     171.68.10.70*     cisco.com
         171.68.10.140
(*):Primary

Port     CallManagerState DSP-Type
-------- ---------------- --------
 7/1     registered       C549
 7/2     registered       C549
 7/3     registered       C549
 7/4     registered       C549
 7/5     registered       C549

Port  NoiseRegen NonLinearProcessing
----- ---------- -------------------
 7/1  enabled    enabled
 7/2  enabled    enabled
 7/3  enabled    enabled
 7/4  enabled    enabled
```

Related Commands

set port voice interface dhcp
show port voice fdl
show port voice interface

show port voice active

Use the **show port voice active** command to display active call information on a port.

show port voice active [*mod/port*] [**all** | **call** | **conference** | **transcode**] [*ipaddr*]

Syntax Description

mod/port	(Optional) Number of the module and port on the module.
all	(Optional) Keyword to display all calls (regular calls, conference calls, and transcoding calls) in the system.
call	(Optional) Keyword to display call information for the 24-port FXS analog interface and the 8-port T1/E1 PSTN interface modules.
conference	(Optional) Keyword to display call information for the 8-port T1/E1 PSTN interface module configured for conferencing.
transcode	(Optional) Keyword to display call information for the 8-port T1/E1 PSTN interface module configured for transcoding.
ipaddr	(Optional) Remote IP address.

Defaults

The default is all active calls are displayed.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The information displayed when using the **show port voice active** command is not available through the supervisor engine SNMP agent.

The **call** keyword is supported by the 24-port FXS analog interface and the 8-port T1/E1 PSTN interface modules.

The **conference** and **transcode** keywords are supported by the 8-port T1/E1 PSTN interface module.

You can use the optional *mod* or *mod/port* variables to display calls that belong to the specified module or port in detailed format.

There are up to 8 calls per port for the 8-port T1/E1 ISDN PRI services-configured module but only one call per port for the 24-port FXS analog station interface services-configured module.

The *ipaddr* option displays one specific call for the specified IP address. You can also use an IP alias.

This command is not supported by the NAM.

Examples

This example shows how to display all calls (regular calls, conference calls, and transcoding calls) in the system:

```
Console> show port voice active
Port  Type         Total Conference-ID/ Party-ID IP-Address
                         Transcoding-ID
----- ------------ ----- -------------- -------- ---------------
 6/3  transcoding  1     2              12       192.1.1.12
                                        10       10.6.106.101
 8/2  call         1     -              -        123.46.1.100
 8/5  call         1     -              -        123.46.1.101
 8/7  conferencing 1     1              8        192.1.1.5
                                        7        123.45.1.52
                                        9        192.1.1.14
Total: 3
Console> (enable)
```

This example shows how to display regular calls:

```
Console> (enable) show port voice active call
Port  Total IP-Address
----- ----- ---------------
 8/2  1     123.46.1.100
 8/5  1     123.46.1.101
Total: 2 calls
Console> (enable)
```

This example shows the output display for the 8-port T1/E1 PSTN interface module configured for transcoding:

```
Console> (enable) show port voice active transcode
Port  Total Transcoding-ID Party-ID IP-Address
----- ----- -------------- -------- ---------------
 6/3  1     2              12       192.1.1.12
                           10       10.6.106.101
Total: 1 transcoding session
Console> (enable)
```

This example shows the output display for the 8-port T1/E1 PSTN interface module configured for conferencing:

```
Console> (enable) show port voice active conference
Port  Total Conference-ID  Party-ID IP-Address
----- ----- -------------- -------- ---------------
 8/7  1     1              8        192.1.1.5
                           7        123.45.1.52
                           9        192.1.1.14
Total: 1 conferencing session
Console> (enable)
```

This example shows how to display calls for a specified port:

```
Console> show port voice active 3/2
Port 3/2:
Channel #1:
  Remote IP address                       : 165.34.234.111
  Remote UDP port                         : 124
  Call state                              : Ringing
  Codec Type                              : G.711
  Coder Type Rate                         : 35243
  Tx duration                             : 438543 sec
  Voice Tx duration                       : 34534 sec
  ACOM Level Current                      : 123213
  ERL Level                               : 123 dB
```

```
  Fax Transmit Duration                    : 332433
  Hi Water Playout Delay                   : 23004 ms
  Logical If index                         : 4
  Low water playout delay                  : 234 ms
  Receive delay                            : 23423 ms
  Receive bytes                            : 2342342332423
  Receive packets                          : 23423423402384
  Transmit bytes                           : 23472377
  Transmit packets                         : 94540
Channel #2:
  Remote IP address                        : 165.34.234.112
  Remote UDP port                          : 125
  Call state                               : Ringing
  Codec Type                               : G.711
  Coder Type Rate                          : 35243
  Tx duration                              : 438543 sec
  Voice Tx duration                        : 34534 sec
  ACOM Level Current                       : 123213
  ERL Level                                : 123 dB
  Fax Transmit Duration                    : 332433
  Hi Water Playout Delay                   : 23004 ms
  Logical If index                         : 4
  Low water playout delay                  : 234 ms
  Receive delay                            : 23423 ms
  Receive bytes                            : 2342342332423
  Receive packets                          : 23423423402384
  Transmit bytes                           : 23472377
  Transmit packets                         : 94540
Port  3/7 :
  Conference ID: 1
    Party ID: 8
      Remote IP address                    : 192.1.1.5
      UDP Port                             : 28848
      Codec Type                           : G729 B CS ACELP VAD
      Packet Size (ms)                     : 20
    Party ID: 7
      Remote IP address                    : 123.45.1.52
      UDP Port                             : 28888
      Codec Type                           : G711 ULAW PCM
      Packet Size (ms)                     : 20
    Party ID: 9
      Remote IP address                    : 192.1.1.14
      UDP Port                             : 28898
      Codec Type                           : G711 ULAW PCM
      Packet Size (ms)                     : 20
Total: 2
Console>
```

This example shows the output display for a specified IP address on a 24-port FXS analog interface module or the 8-port T1/E1 PSTN interface module:

```
Console> show port voice active 3/2 171.69.67.91
  Remote IP address                        : 171.69.67.91
  Remote UDP port                          : 125
  Call state                               : Ringing
  Codec Type                               : G.711
  Coder Type Rate                          : 35243
  Tx duration                              : 438543 sec
  Voice Tx duration                        : 34534 sec
  ACOM Level Current                       : 123213
  ERL Level                                : 123 dB
  Fax Transmit Duration                    : 332433
  Hi Water Playout Delay                   : 23004 ms
  Logical If index                         : 4
```

```
  Low water playout delay                 : 234 ms
  Receive delay                           : 23423 ms
  Receive bytes                           : 2342342332423
  Receive packets                         : 23423423402384
  Transmit bytes                          : 23472377
  Transmit packets                        : 94540
Console>
```

Related Commands **set port voice interface dhcp**

show port voice fdl

Use the **show port voice fdl** command to display the facilities data link statistics for the specified ports.

show port voice fdl [*mod*[*/port*]]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

Examples

This example shows how to display FDL information on an 8-port T1/E1 ISDN PRI services- configured module:

```
Console> (enable) show port voice fdl 7/1-3
Port  ErrorEvents       ErroredSecond     SeverlyErroredSecond
      Last 15' Last 24h Last 15' Last 24h Last 15' Last 24h
----- -------- -------- -------- -------- -------- -----------
 7/1  17       18       19       20       21       22
 7/2  17       18       19       20       21       22
 7/3  17       18       19       20       21       22

Port  FailedSignalState FailedSignalSecond
      Last 15' Last 24h Last 15' Last 24h
----- -------- -------- -------- ---------
 7/1  37       38       39       40
 7/2  37       38       39       40
 7/3  37       38       39       40

Port         LES              BES              LCV
      Last 15' Last 24h Last 15' Last 24h Last 15' Last 24h
----- -------- -------- -------- -------- -------- --------
 7/1  41       48       49       50       53       54
 7/2  41       48       49       50       53       54
 7/3  41       48       49       50       53       54
Console> (enable)
```

Table 2-71 describes the possible fields (depending on the port type queried) in the **show port voice fdl** command output.

Table 2-71 show port voice fdl Command Output Fields

Field	Description
ErrorEvents	Count of errored events.
ErroredSecond	Count of errored seconds.
SeverelyErroredSecond	Count of severely errored seconds.
FailedSignalState	Count of failed signal state errors.
FailedSignalSecond	Count of failed signal state.
LES	Line errored seconds detected.
BES	Bursty errored seconds detected.
LCV	Line code violation seconds detected.

Related Commands **show port voice**

show port voice interface

Use the **show port voice interface** command to display the port voice interface configuration.

show port voice interface [*mod*[*/port*]]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

Examples

This example shows how to display voice interface information for a specific module:

```
Console> show port voice interface 5
Port     DHCP    MAC-Address       IP-Address      Subnet-Mask
-------- ------- ----------------- --------------- ---------------
 5/1-24  disable 00-10-7b-00-13-ea 10.6.15.158     255.255.255.0

Port     Call-Manager(s)   DHCP-Server     TFTP-Server     Gateway
-------- ----------------- --------------- --------------- ---------------
 5/1-24  10.6.15.155       -               10.6.15.155     -

Port     DNS-Server(s)     Domain
-------- ----------------- --------------------------------------------------
 5/1-24  12.2.2.1*         cisco.cisco.com
         7.7.7.7
(*): Primary
Console>
```

Related Commands

set port voice interface dhcp
show port voice
show port voice active

show proc

Use the **show proc** command to display CPU, memory allocation, and process utilization information.

show proc [**cpu** | **mem**]

Syntax Description

cpu	(Optional) Keyword to specify CPU information.
mem	(Optional) Keyword to specify memory allocation information.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can enter this command only in privileged mode.

If you do not specify **cpu** or **mem**, process information is displayed. The **mem** keyword allows you to display memory allocation information, such as how much each process has allocated and freed.

Examples

This example shows how to display CPU information:

```
Console> (enable) show proc cpu
(W)CPU utilization for five seconds: 1.0%; one minute: 1. 0%; five minutes: 1. %

PID Runtime(ms) Invoked uSecs   5Sec   1Min    5min   TTY Process
0   0           0       0       99.10%  99.0 %  99.0 %  0    idle
1   1           36      1000     0.0 %   0.0 %   0.0 %  0    Flash MIB Updat
2   1342        2846    460000   0.0 %   0.0 %   0.0 %  0    SynDiags
3   730172      4440594 400000   0.0 %   0.0 %   0.0 %  0    SynConfig
4   33752       424120  1000     0.0 %   0.0 %   0.0 %  0    Statuspoll
5   7413        44916   1000     0.0 %   0.0 %   0.0 %  0    SWPoll64bCnt
6   9568        15889836 1000     0.0 %   0.0 %   0.0 %  0     SL_TASK
7   746         636118  105000   0.0 %   0.0 %   0.0 %  0    RedundantTask
Console> (enable)
```

This example shows how to display process utilization information:

```
Console> (enable) show proc
PID Q  T  PC         Runtime(ms) Invoked uSecs  Stacks    TTY Process
0   1  rd 0x80407b10 0           0       0      1640/6144 0   idle
1   65376 st 0x80407d8c 1           36      1000   1188/6144 0   Flash MIB
Upda
2   2  st 0x80407d8c 1342        2846    460000 3160/6144 0   SynDiags
3   1  rd 0x80407d8c 729979      4439406 400000 1672/6144 0   SynConfig
4   2  si 0x80407d8c 33739       424007  1000   1572/6144 0   Statuspoll
5   4  si 0x80407d8c 7413        44916   1000   1888/6144 0   SWPoll64bCnt
6   2  si 0x80407d8c 9565        15885713 1000   1096/6144 0   SL_TASK
7   2  si 0x80407d8c 746         635948  105000 1192/6144 0   RedundantTask
```

```
Memory Pool Utilization
Memory Pool Type 1Min  5Min  10Min
---------------- ----- ----- -----
DRAM               49%   49%   49%
FLASH              82%   82%   82%
NVRAM              49%   49%   49%
MBUF                2%    2%    2%
CLUSTER            12%   12%   12%
MALLOC             15%   15%   15%
Console> (enable)
```

This example shows how to display process information:

```
Console> (enable) show proc mem

Memory Used:  7141936
       Free: 53346800
      Total: 60488736

PID        TTY        Allocated  Freed      Holding    Process
---------- ---------- ---------- ---------- ---------- ---------------
1          -2         2928912    4544       2924368    Kernel and Idle
2          -2         160        0          160        Flash MIB Updat
3          -2         160        0          160        L2L3IntHdlr
4          -2         0          0          0          L2L3PatchRev
5          -2         288        0          288        SynDiags
6          -2         128        0          128        GenMsgHndlr
7          -2         1158560    526480     632080     SynConfig
8          -2         32         0          32         TempMon
9          -2         16         0          16         EM_garbageColle
10         -2         192        0          192        PowerMgmt
11         -2         1136       0          1136       FabricConfig
12         -2         97536      0          97536      SL_TASK
13         -2         18368      5056       13312      RedundantTask
14         -2         2384       0          2384       Status Poll
15         -2         96         0          96         SWPoll64bCnt
16         0          384        0          384        HavailTask
17         -2         10304      0          10304      SyncTask
18         -2         48         0          48         SecurityRx
19         -2         144        0          144        DeviceLinkChk
20         -2         10576      10560      16         Earl
21         -2         2768       2464       304        DTP_Rx
22         -2         280624     151680     128944     EthChnlRx
23         -2         0          0          0          llcSSTPFlood
24         -2         1584       1152       432        EthChnlConfig
25         -2         1232       0          1232       ACL
26         -2         27760      3552       24208      VaclLog
27         0          0          0          0          L3Aging
28         0          209168     0          209168     NetFlow
29         0          2688400    112        2688288    Fib
30         -2         0          0          0          Fib_bg_task
31         -2         176        0          176        ProtocolFilter
32         -2         16         0          16         telnetd
33         -2         16         0          16         tftpd
34         -2         1744       1632       112        ProtocolTimer
35         -2         96         0          96         ciscoRmonTimer
36         -2         96         0          96         ciscoUsrHistory
37         -2         112        0          112        rmonMediaIndep
38         -2         0          0          0          SnmpTraps
39         -2         0          0          0          memPoolMain
40         -2         16         0          16         Acct Send Bkg
41         -2         80         0          80         l2t_server
42         -2         144        0          144        Authenticator_S
43         -2         16         0          16         dot1x_rx
```

```
44          -2          16          0           16          Backend_Rx
45          -2          16          0           16          Backend_SM
46          -2          3216        2992        224         Debug Port Coun
47          -2          16          0           16          SysLogTask
48          -2          112         0           112         pinggateA
49          -2          8704        8000        704         cdpd
50          -2          124576      124416      160         cdpdtimer
51          -2          1296        1088        208         SptTimer
52          -2          2336        1120        1216        SptBpduRx
53          -2          144         0           144         SptBpduTx
54          -2          0           0           0           GL2Prot_Tunnel
55          -2          176         0           176         VtpTimer
56          -2          16          1072        4294966240 HPConfig
57          -2          96          0           96          RMON AlarmTimer
58          -2          0           0           0           sptTraps
59          -2          6128        5952        176         McastRx
60          -2          16          0           16          IGMPQuerierProc
61          -2          272         0           272         M-MLS_stats
62          -2          5808        1504        4304        M-MLS_manager
63          -2          47520       15216       32304       QoSTask
64          0           11936       0           11936       Read Stats Task
65          0           32          0           32          QDE Task
66          -2          144         0           144         EnvMon
67          -2          1120        0           1120        VlanStatsTask
70          -2          16          0           16          HPActive
71          -2          48          0           48          HPTrapMgr
143         0           57200       4208        52992       Console
144         -2          256208      29920       226288      snmpdm
145         -2          208         0           208         VtpRx
146         2252448660  68448       6864        61584       telnet146
191         -2          29360       19504       9856        AclManager

Memory Pool Utilization
Memory Pool Type 1Min  5Min  10Min
---------------- ----- ----- -----
DRAM               45%   45%   45%
FLASH              83%   83%   83%
NVRAM              49%   49%   49%
MBUF                2%    2%    2%
CLUSTER            11%   11%   11%
MALLOC             11%   11%   11%

Console> (enable)
```

Table 2-72 describes the possible fields in the **show proc** command outputs.

Table 2-72 show proc Command Output Fields

Field	Description
CPU Utilization	Sum of all the loads from all the processes running on the CPU in the last 5 seconds, 1 minute, and 5 minutes.
PID	Process ID.
Runtime	Time the process has run since initiation (in milliseconds).
Invoked	Number of times the process was invoked since initiation.
uSecs	Maximum time a process ran in a single invocation.
5sec	Amount of time this process ran on the CPU in the last 5-second interval.
1Min	Average memory pool usage over the last 1-minute interval.

Table 2-72 show proc Command Output Fields (continued)

Field	Description
5Min	Average memory pool usage over the last 5-minute interval.
10Min	Average memory pool usage over the last 10-minute interval.
TTY	TTY associated with the process.
Process	Name of the process.
Allocated	Amount of all the memory allocated by the process since it was initiated, including the memory previously freed up.
Freed	Amount of memory the process has freed up until now.
Holding	Amount of memory the process is currently holding.
Q	Process priority in terms of numbers. A low number means high priority.
T	State of the process (Running, we = waiting for event, st = sleeping, si = sleeping on an interval, rd = ready to run, id = idle, xx = dead/zombie).
PC	Calling PC for “show_process” function.
Stacks	Size of the stack used by the process/the total stack size allocated to the process (in bytes).

show protocolfilter

Use the **show protocolfilter** command to list whether protocol filtering is enabled or disabled.

show protocolfilter

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display whether protocol filtering is enabled or disabled:

```
Console> show protocolfilter
Protocol filtering is enabled on this switch.
Console>
```

Related Commands

set port protocol

show pvlan

Use the **show pvlan** command to show the configuration for a given private VLAN.

show pvlan [*vlan* | **primary** | **isolated** | **community** | **twoway-community**]

Syntax Description

vlan	(Optional) Number of the private VLAN.
primary	(Optional) Keyword to display the primary private VLANs.
isolated	(Optional) Keyword to display the isolated private VLANs.
community	(Optional) Keyword to display the community private VLANs.
twoway-community	(Optional) Keyword to display the bidirectional community private VLANs.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

A **twoway-community** PVLAN is a bidirectional community PVLAN that carries traffic among community ports and to and from community ports to and from the MSFC.

Examples

This example shows how to display the status for VLAN 10:

```
Console> show pvlan 10
Primary Secondary Secondary-Type Ports
------- --------- -------------- ------------
10      20        isolated       6/1
Console>
```

This example shows how to display the status for all VLANs set as primary:

```
Console> show pvlan primary
Primary Secondary Secondary-Type Ports
------- --------- -------------- ------------
10      20        isolated       6/1
11      21        isolated       6/2
30      -         -
Console>
```

This example shows how to display the status for all VLANs set as isolated:

```
Console> show pvlan isolated
Primary Secondary Secondary-Type Ports
------- --------- -------------- ------------
10      20        isolated       6/1
11      21        isolated       6/2
-       31        isolated
Console>
```

This example shows how to display the status for all VLANs set as community:

```
Console> show pvlan community
Primary Secondary Secondary-Type Ports
------- --------- -------------- ------------
7       902       community      2/4-6
Console>
```

Related Commands

clear config pvlan
clear pvlan mapping
clear vlan
set pvlan
set pvlan mapping
set vlan
show pvlan mapping
show vlan

show pvlan capability

Use the **show pvlan capability** command to determine whether or not a port can be made a private port.

show pvlan capability *mod/port*

Syntax Description

mod/port	Number of the module and the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to determine if a port can be made into a PVLAN:

```
Console> (enable) show pvlan capability 5/20
Ports 5/13 - 5/24 are in the same ASIC range as port 5/20.

Port 5/20 can be made a private vlan port.
Console> (enable)
```

These examples show the output if a port cannot be made into a PVLAN:

```
Console> (enable) show pvlan capability 3/1
Port 3/1 cannot be made a private vlan port due to:
-----------------------------------------------------
Promiscuous ports cannot be made private vlan ports.
Console> (enable)

Console> (enable) show pvlan capability 5/1
Ports 5/1 - 5/12 are in the same ASIC range as port 5/1.

Port 5/1 cannot be made a private vlan port due to:
-----------------------------------------------------
Trunking ports are not Private Vlan capable.
Conflict with Promiscuous port(s) : 5/2
Console> (enable)

Console> (enable) show pvlan capability 5/2
Ports 5/1 - 5/12 are in the same ASIC range as port 5/2.

Port 5/2 cannot be made a private vlan port due to:
-----------------------------------------------------
Promiscuous ports cannot be made private vlan ports.
Conflict with Trunking port(s) : 5/1
Console> (enable)
```

```
Console> (enable) show pvlan capability 5/3
Ports 5/1 - 5/12 are in the same ASIC range as port 5/3.

Port 5/3 cannot be made a private vlan port due to:
-----------------------------------------------------
Conflict with Promiscuous port(s) : 5/2
Conflict with Trunking port(s) : 5/1
Console> (enable)

Console> (enable) show pvlan capability 15/1
Port 15/1 cannot be made a private vlan port due to:
-----------------------------------------------------
Only ethernet ports can be added to private vlans.
Console> (enable)
```

Related Commands

clear config pvlan
clear pvlan mapping
clear vlan
set pvlan
set pvlan mapping
set vlan
show pvlan capability
show pvlan mapping
show vlan

show pvlan mapping

Use the **show pvlan mapping** command to show the private VLAN mappings configured on promiscuous ports.

show pvlan mapping [*private_vlan* | *mod/port*]

Syntax Description

private_ vlan	(Optional) Number of the private VLAN.
mod/port	(Optional) Number of the module and port.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the private VLAN mapping by port:

```
Console> show pvlan mapping
Port Primary Secondary
---- ------- ---------
 6/3  10      20
Console>
```

This example shows how to display the private VLAN mapping for a specific VLAN:

```
Console> show pvlan mapping 10
Primary Secondary Ports
------- --------- -----
10      20        6/3
Console>
```

This example shows how to display the private VLAN mapping for a specific port:

```
Console> show pvlan mapping 6/3
Port Primary Secondary
---- ------- ---------
 6/3  10      20
Console>
```

This example shows the results when no VLANs are mapped:

```
Console> show pvlan mapping
Port Primary Secondary
---- ------- ---------
No Private Vlan Mappings configured.
Console>
```

Related Commands

- clear config pvlan
- clear pvlan mapping
- clear vlan
- set pvlan
- set pvlan mapping
- set vlan
- show pvlan mapping
- show vlan

show qos acl editbuffer

Use the **show qos acl editbuffer** command to display ACL names in the edit buffer.

show qos acl editbuffer

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Enter the **show qos acl editbuffer** command to display the committed access lists that you configured. The information is helpful when you are adding or deleting ACEs.

Examples

This example shows how to display QoS ACL edit buffer contents:

```
Console> (enable) show qos acl editbuffer
ACL                                Type Status
---------------------------------  ---- ----------
ip1                                IP   Committed
ipx1                               IPX  Committed
mac1                               MAC  Committed
```

Related Commands

commit
rollback

show qos acl info

Use the **show qos acl info** command to display QoS ACL information.

show qos acl info default-action {**ip** | **ipx** | **mac** | **all**}

show qos acl info runtime {*acl_name* | **all**}

show qos acl info config {*acl_name* | **all**} [**editbuffer** [*editbuffer_index*]]

Syntax Description

default-action	Keyword to display default action (using the **set qos acl default-action** command) for packets that do not match any entry in an access list.
ip	Keyword to display QoS IP ACL information.
ipx	Keyword to display all QoS IPX ACL information.
mac	Keyword to display all QoS MAC ACL information.
all	Keyword to display all QoS ACL information.
runtime	Keyword to display runtime ACE information.
acl_name	Name of the ACL to be displayed.
config	Keyword to display configured ACE information.
editbuffer	(Optional) Keyword to display edit buffer information.
editbuffer_index	(Optional) Position of the ACE in the ACL.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to display all ACL default configurations:

```
Console> (enable) show qos acl info default-action all
set qos acl default-action
--------------------------
ip dscp 7 my1 my2
ipx dscp 0
mac dscp 0
Console> (enable)
```

This example shows how to display edit buffer information for a specific ACL:

```
Console> (enable) show qos acl info my_ip_acl editbuffer
set qos acl ip my_ip_acl
------------------------------------------------
1. set qos acl ip my_ip_acl trustdscp microflow my-micro tcp 1.2.3.4 255.0.0.0
eq port 21 172.20.20.1 255.255.255.0
```

```
2. set qos acl ip my_ip_acl trustdscp microflow my-micro aggregate agg tcp
173.22.3.4 255.0.0.0 eq port 19 173.22.20.1 255.255.255.0 tos 5
ACL status: Not Committed
Console> (enable)
```

This example shows how to display information for a specific ACL:

```
Console> (enable) show qos acl info my_ip_acl
set qos acl ip my_ip_acl
---------------------------------------------------
1. trust-dscp microflow my-micro tcp 1.2.3.4 255.0.0.0 eq
port 21 172.20.20.1 255.255.255.0 tos 5
2. trust-dscp microflow my-micro aggregate agg tcp
173.22.3.4 255.0.0.0 eq port 19 173.22.20.1 255.255.255.0 tos 5
Console> (enable)
```

This example shows how to display runtime information for all ACLs:

```
Console> (enable) show qos acl info runtime all
set qos acl IP _Cops_1
-------------------------------------------
1. dscp 0 any

set qos acl IP _Cops_2
-------------------------------------------
1. dscp 8 ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
2. dscp 16 tcp any any
3. dscp 24 udp any any
Console> (enable)
```

Related Commands

clear qos policer
set qos acl default-action
set qos policer

show qos acl map

Use the **show qos acl map** command to display the ACL mapping information.

show qos acl map {**config** | **runtime**} {*acl_name* | *mod/port* | *vlan* | **all**}

Syntax Description

config	Keyword to display NVRAM QoS information.
runtime	Keyword to display QoS runtime information.
acl_name	Name of the list.
mod/port	Number of the module and the port.
vlan	VLAN list.
all	Keyword to display information regarding all ACLs.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can enter the **config** keyword to display information that was configured through the CLI and saved in NVRAM, regardless of the current runtime information.

Note When a switchover occurs, you cannot view the ACLs and policers deployed using COPS-DS until the COPS-DS client on the new active supervisor engine establishes connection to the PDP and downloads the QoS policy. The runtime fields in the output display will be blank until QoS policy is downloaded to the new active supervisor engine.

Examples

This example shows how to display information for all ACLs:

```
Console> show qos acl map all
ACL name   Vlan #            Ports
--------   ----------------- ----------------------------
web-acc    1,4-7
isp1       2                 1/1
Console>
```

This example shows how to display information for a specific VLAN:

```
Console> show qos acl map 1
Vlan  ACL name
----  ---------------
1     web-acc
Console>
```

This example shows how to display information for a specific ACL:

```
Console> show qos acl map isp1

ACL name   Vlan #            Ports
--------   ----------------  ---------------
isp1       2                 1/1
Console>
```

Related Commands clear qos acl
set qos acl map

show qos acl resource-usage

Use the **show qos acl resource-usage** command to display ACL management information.

show qos acl resource-usage

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display ACL management information:

```
Console> (enable) show qos acl resource-usage
ACL resource usage:
Label:0%
Logical Operation Unit:0%
TCAM mask:0%
TCAM value:0%
Console> (enable)
```

Related Commands

commit
rollback

show qos bridged-packet-policing

Use the **show qos bridged-packet-policing** command to display the VLAN-bridged packet-policing status.

show qos bridged-packet-policing {**config** | **runtime**} [*vlan*]

Syntax Description

config	Keyword to display NVRAM configuration.
runtime	Keyword to display the run time configuration.
vlan	(Optional) Number of the VLAN.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not specify a VLAN number, the status of all VLANs are displayed.

Examples

This example shows how to display the NVRAM configuration of a specific VLAN:

```
Console> show qos bridged-microflow-policing config 1
QoS microflow policing is disabled for bridged packets on vlan 1.
Console>
```

This example shows how to display the NVRAM configuration of all VLANs:

```
Console> show qos bridged-microflow-policing config
QoS microflow policing is disabled for bridged packets on vlan(s) 1-1000,1025-40
94.
Console>
```

Related Commands

clear qos policer
set qos bridged-microflow-policing
set qos policer

show qos info

Use the **show qos info** command to display QoS-related information for a specified port.

show qos info {**runtime** | **config**} {*mod*/*port*}

show qos info config *port_type* {**tx** | **rx**}

Syntax Description

runtime	Keyword to show the current QoS runtime information.
config	Keyword to display NVRAM QoS configuration.
mod/port	Number of the module and port.
port_type	Port type; valid values are **2q2t**, **1p3q1t**, **1p2q2t**, **1p2q1t** for transmit and **1q4t**, **1p1q4t**, and **1p1q0t**, **1p1q8t** for receive. See the "Usage Guidelines" section for additional information.
tx	Keyword to display transmit port information.
rx	Keyword to display receive port information.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

You can enter the **show qos info runtime** *mod*/*port* command to view the currently used values in the hardware or the **show qos info runtime** *mod*/*port* command to view the values that have been configured administratively (present in NVRAM). The outputs differ when QoS has been disabled. When you disable QoS, the values set on all the ports are different from the values present in NVRAM. When you enable QoS, the values in NVRAM are used to program the hardware.

The display of **show qos info runtime** *mod*/*port* shows both the absolute values and the percentages you specified for the drop thresholds, queue sizes, and WRR. However, the absolute values may not exactly match the percentages specified due to the granularity of permitted settings in hardware.

The number preceding the **t** letter in the *port_type* value (for example, **2q2t**, **1p2q2t**, **1q4t**, or **1p1q4t**) determines the number of threshold values the hardware supports. For example, with **2q2t** and **1p2q2t**, the number of thresholds specified is two; with **1q4t** and **1p1q4t**, the number of thresholds specified is four. Due to the granularity of programming the hardware, the values set in hardware will be close approximations of the values provided.

The number preceding the **q** letter in the *port_type* value determines the number of the queues that the hardware supports. For example, with **2q2t** and **1p2q2t**, the number of queues specified is two; with **1q4t** and **1p1q4t**, the number of queues specified is four. The system defaults for the transmit queues attempt to keep the maximum latency through a port at a maximum of 10 ms.

The number preceding the **p** letter in the *port_type* value (for example, **1p2q2t** and **1p1q4t**) determines the threshold in the priority queue.

The **1p2q1t** and **1p1q8t** port types are not supported.

Note When a switchover occurs, you cannot view the ACLs and policers deployed using COPS-DS until the COPS-DS client on the new active supervisor engine establishes connection to the PDP and downloads the QoS policy. The runtime fields in the output display will be blank until QoS policy is downloaded to the new active supervisor engine.

Examples

This example shows how to display QoS-related NVRAM-transmit threshold information:

```
Console> (enable) show qos info config 2q2t tx
QoS setting in NVRAM for 2q2t transmit:
QoS is disabled
 CoS = 0
Queue and Threshold Mapping:
Queue Threshold CoS
----- --------- ---------------
1     1         0 1
1     2         2 3
2     1         4 5
2     2         6 7
Tx drop thresholds:
Queue #  Thresholds - percentage (abs values )
-------  ------------------------------------
1        40% 100%
2        40% 100%
Queue Sizes:
Queue #  Sizes - percentage (abs values )
-------  ------------------------------------
1        80%
2        20%
WRR Configuration:
Ports have transmit ratios between queue 1 and 2 of
100:256
Console> (enable)
```

This example shows how to display QoS-related NVRAM receive-threshold information:

```
Console> (enable) show qos info config 1p1q4t rx
QoS setting in NVRAM for 1p1q4t receive:
QoS is disabled
Queue and Threshold Mapping for 1p1q4t (rx):
Queue Threshold CoS
----- --------- ---------------
1     1         0
1     2         2 3
1     3         4 5
1     4         1 6 7
2     1
Rx drop thresholds:
Queue #  Thresholds - percentage (abs values )
-------  ------------------------------------
1        50% 60% 80% 100%
Console> (enable)
```

This example shows how to display all QoS-related NVRAM threshold information:

```
Console> (enable) show qos info config 2q2t tx
QoS setting in NVRAM for 2q2t transmit:
QoS is enabled
Queue and Threshold Mapping:
Queue Threshold CoS
----- --------- ---------------
1     1         0 1
1     2         2 3
2     1         4 5
2     2         6 7
Tx drop thresholds:
Queue #  Thresholds - percentage (abs values )
-------  ------------------------------------
1        40% 100%
2        40% 100%
Queue Sizes:
Queue #  Sizes - percentage (abs values )
-------  ------------------------------------
1        80%
2        20%
WRR Configuration:
Ports with 2q2t have ratio of 100:255 between transmit queue 1 and 2
Console> (enable)
```

This example shows how to display the current QoS runtime information:

```
Console> (enable) show qos info runtime 1/1
Run time setting of QoS:
QoS is enabled on 2/1
Port 2/1 has 2 transmit queue with 2 drop thresholds (2q2t).
Port 2/1 has 1 receive queue with 4 drop thresholds (1q4t).
The qos trust type is set to trust-cos.
                    CoS = 0
Queue and Threshold Mapping:
Queue Threshold CoS
----- --------- ---------------
1     1         0 1
1     2         2 3
2     1         4 5
2     2         6 7
Rx drop thresholds:
Queue #  Thresholds - percentage (abs values )
-------  ------------------------------------
1        50% (38912 bytes) 60% (46688 bytes) 80% (62240 bytes) 100% (73696
bytes)
Tx drop thresholds:
Queue #  Thresholds - percentage (abs values )
-------  ------------------------------------
1        40% (144224 bytes) 100% (360416 bytes)
2        40% (32864 bytes) 100% (77792 bytes)
Queue Sizes:
Queue #  Sizes - percentage (abs values)
-------  ------------------------------------
1        80% (360416 bytes)
2        20% (81888 bytes)
WRR Configuration:
Ports with speed 1000Mbps have ratio of 100:255 between transmit queue 1
and 2 (25600:65280 bytes)
Console> (enable)
```

This example shows how to display the current QoS configuration information:

```
Console> (enable) show qos info config 8/1
QoS setting in NVRAM:
QoS is disabled
Port 8/1 has 3 transmit queue with 2 drop thresholds (1p2q2t).
Port 8/1 has 2 receive queue with 4 drop thresholds (1p1q4t).
ACL attached:
The qos trust type is set to untrusted.
 CoS = 0
Queue and Threshold Mapping for 1p2q2t (tx):
Queue Threshold CoS
----- --------- ---------------
1     1         0 1
1     2         2 3
2     1         4 5
2     2         7
3     1         6
Queue and Threshold Mapping for 1p1q4t (rx):
Queue Threshold CoS
----- --------- ---------------
1     1         0
1     2         2 3
1     3         4 5
1     4         1 6 7
2     1
Rx drop thresholds:
Rx drop thresholds are disabled for untrusted ports.
Queue #  Thresholds - percentage (abs values )
-------  ---------------------------------
1        50% 60% 80% 100%
Tx drop thresholds:
Tx drop-thresholds feature is not supported for this port type.
Tx WRED thresholds:
Queue #  Thresholds in percentage ( in abs values )
-------  ---------------------------------------
1        80% 100%
2        80% 100%
Queue Sizes:
Queue #  Sizes - percentage (abs values )
-------  ---------------------------------
1        70%
2        15%
3        15%
WRR Configuration of ports with speed 1000Mbps:
Queue #  Ratios (abs values )
-------  ---------------------------------
1        100
2        255
Console> (enable)
```

This example shows another display of the current QoS configuration information:

```
Console> (enable) show qos info config 1p2q2t tx
QoS setting in NVRAM for 1p2q2t transmit:
QoS is enabled
Queue and Threshold Mapping:
Tx WRED thresholds:
Queue #  Thresholds - percentage
-------  -----------------------------------------
1        0%:60% 0%:90%
2        0%:50% 0%:90%
Tx queue size ratio:
Queue #  Sizes - percentage
```

```
-------  ------------------------------------
1        70%
2        15%
3        15%
WRR Configuration of ports with 1p2q2t:
Queue #  Ratios
-------  ------------------------------------
1        5
2        255
Console> (enable)
```

Related Commands set qos

show qos mac-cos

Use the **show qos mac-cos** command to display the currently configured QoS-related information for the MAC address and VLAN pair.

show qos mac-cos *dest_mac* [*vlan*] [**config**]

show qos mac-cos all [**config**]

Syntax Description

dest_mac	MAC address of the destination host.
vlan	(Optional) Number of the VLAN; valid values are from **1** to **1005**.
config	(Optional) Keyword to display NVRAM QoS configuration.
all	Keyword to specify all MAC address and VLAN pairs.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

You can enter the **show qos mac-cos** command to display the currently configured QoS-related information.

You can enter the **config** keyword to display information that was configured through the CLI and saved in NVRAM, regardless of the current runtime information.

Examples

This example shows how to display currently configured QoS-related information for all MAC address and VLAN pairs:

```
Console> (enable) show qos mac-cos all
VLAN  Dest MAC           CoS
----  -----------------  ---
1      01-02-03-04-05-06  2
9      04-05-06-07-08-09  3
Console> (enable)
```

This example shows how to display currently configured QoS-related information for a specific MAC address:

```
Console> (enable) show qos mac-cos 01-02-03-04-05-06
VLAN  Dest MAC           CoS
----  -----------------  ---
1      01-02-03-04-05-06  2
Console> (enable)
```

Related Commands clear qos mac-cos
set qos mac-cos

show qos maps

Use the **show qos maps** command to display the mapping of different maps.

show qos maps {**config** | **runtime**} [[**cos-dscp-map** | **ipprec-dscp-map** | **dscp-cos-map** | **policed-dscp-map** [**normal-rate** | **excess-rate**]]

Syntax Description

config	Keyword to display NVRAM QoS configuration.
runtime	Keyword to display current QoS configuration.
cos-dscp-map	(Optional) Keyword to specify the CoS-to-DSCP map.
ipprec-dscp-map	(Optional) Keyword to specify the IP precedence-to-DSCP map.
dscp-cos-map	(Optional) Keyword to specify the DSCP-to-CoS map.
policed-dscp-map	(Optional) Keyword to specify the marked-down map.
normal-rate	(Optional) Keyword to specify normal rate.
excess-rate	(Optional) Keyword to specify excess rate.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

You can enter the **config** keyword to display information that was configured through the CLI and saved in NVRAM, regardless of the current runtime information.

If you do not specify an option, all maps are displayed.

Note When a switchover occurs, you cannot view the ACLs and policers deployed using COPS-DS until the COPS-DS client on the new active supervisor engine establishes connection to the PDP and downloads the QoS policy. The runtime fields in the output display will be blank until QoS policy is downloaded to the new active supervisor engine.

Examples

This example shows how to display the cos-dscp-map map:

```
Console> show qos maps cos-dscp-map
CoS - DSCP map:
CoS   DSCP
---   ---------------
0     10
...
7     52
Console>
```

This example shows how to display the ipprec-dscp-map map:

```
Console> show qos maps ipprec-dscp-map
IP-Precedence - DSCP map:
IP-Prec   DSCP
-------   -------------------
0         1
...
7         52
Console>
```

This example shows how to display the dscp-cos-map map:

```
Console> show qos maps dscp-cos-map
DSCP - CoS map:
DSCP             CoS
---------------  ----
34-40,60         0
...
50               7
Console>
```

This example shows how to display the policed-dscp-map map:

```
Console> show qos maps policed-dscp-map
DSCP policed-dscp map:
In-profile DSCP  Policed DSCP
---------------  -------------
0-20             0
Console>
```

This example shows how to display all maps:

```
Console> show qos maps
CoS - DSCP map:
CoS   DSCP
---   ---------------
0     10
...
7     52

IP-Precedence - DSCP map:
IP-Prec   DSCP
-------   -------------------
0         1
...
7         52

IP-Precedence - CoS map:
IP-Prec   CoS
-------   -----
0         0
...
7         7
DSCP - CoS map:
DSCP             CoS
---------------  ----
34-40,60         0
...
50               7
```

```
DSCP policed-dscp map:
In-profile DSCP  Policed DSCP
---------------  -------------
0-20             0
Console>
```

This example shows how to display normal-rate maps:

```
Console> (enable) show qos maps config policed-dscp-map normal-rate
DSCP - Policed DSCP map normal-rate:
DSCP                              Policed DSCP
--------------------------------  ------------
                       0, 24-63  0
                              1  1
                              2  2
                              3  3
                              4  4
                              5  5
                              6  6
                              7  7
                              8  8
                              9  9
                             10  10
                             11  11
                             12  12
                             13  13
                             14  14
                             15  15
                             16  16
                             17  17
                             18  18
                             19  19
                             20  20
                             21  21
                             22  22
                             23  23
Console>
```

Related Commands

clear qos cos-dscp-map
clear qos policed-dscp-map
set qos map

show qos policer

Use the **show qos policer** command to display microflow or aggregate policers currently configured.

show qos policer {**config** | **runtime**} {**microflow** [*policer_name*] | **aggregate** [*policer_name*] | **all**}

Syntax Description

config	Keyword to display NVRAM QoS configuration.
runtime	Keyword to show the current QoS runtime information.
microflow	Keyword to specify microflow policing information.
aggregate	Keyword to specify aggregate policing rule information.
policer_name	(Optional) Name of the policer.
all	Keyword to specify all policing information.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

Note When a switchover occurs, you cannot view the ACLs and policers deployed using COPS-DS until the COPS-DS client on the new active supervisor engine establishes connection to the PDP and downloads the QoS policy. The runtime fields in the output display will be blank until QoS policy is downloaded to the new active supervisor engine.

Examples

This example shows how to display all currently configured policing information:

```
Console> show qos policer config all
QoS microflow policers:
Microflow name                  Avg. rate Burst size Exceed action
------------------------------ --------- ---------- -------------
mic                                    55         64 drop
                               ACL attached
                               ------------------------------------

QoS aggregate policers:
No aggregate policer found.
Console>
```

This example shows how to display microflow policing information:

```
Console> show qos policer config microflow
QoS microflow policers:
Microflow name        Average rate     Burst size       Exceed action
```

```
--------------------  ---------------  ---------------  -------------
my-micro              1000             2000             drop
Microflow name        ACL attached
--------------------  ---------------------------------------------
my-micro              my-acl
Console>
```

This example shows how to display aggregate policing information:

```
Console> show qos policer config aggregate
QoS aggregate policers:
No aggregate policer found.
Console>
```

This example shows how to display aggregate policing information for a specific policer:

```
Console> (enable) show qos policer config aggregate
QoS aggregate policers:
Aggregate name                Normal rate (kbps)  Burst size (kb) Normal action
----------------------------- ------------------  --------------- -------------
test2                                     64             100  policed-dscp
                              Excess rate (kbps)  Burst size (kb) Excess action
                              ------------------  --------------  --------------
                                        8000000             100  policed-dscp
                              ACL attached
                              -----------------------------------
Console> (enable)
```

Related Commands clear qos policer
set qos policer

show qos policy-source

Use the **show qos policy-source** command to display the QoS policy source information.

show qos policy-source

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Types Switch command.

Command Modes Normal.

Usage Guidelines This command displays whether the QoS policy source is set to local or COPS.

Examples This example shows how to view the QoS policy source:

```
Console> show qos policy-source
QoS policy source for the switch set to local.
Console>
```

Related Commands **set qos policy-source**

show qos rsvp

Use the **show qos rsvp** command to display RSVP information.

show qos rsvp info

show qos rsvp flow-info

Syntax Description

info	Keyword to display RSVP status information.
flow-info	Keyword to display RSVP flow information.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The maximum number of RSVP flows displayed in the **show qos rsvp flow-info** command output are as follows:

- 1024 for switches configured with the Supervisor Engine 1 with Layer 3 Switching Engine WS-F6K-PFC (Policy Feature Card)
- 1056 for systems configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2)

Examples

This example shows how to display RSVP status information:

```
Console> (enable) show qos rsvp info
RSVP disabled.
RSVP policy timeout set to 30 minutes.
RSVP local policy set to forward.
Console> (enable)
```

This example shows how to display RSVP flow information:

```
Console> (enable) show qos rsvp flow-info
RSVP enabled. Only RSVP qualitative service supported.
RSVP policy timeout set to 30 minutes.

Flow # SrcAddr         DstAddr         SrcPort DstPort Prot DSCP Time Valid
------ --------------- --------------- ------- ------- ---- ---- -----------
1         172.21.23.34    177.23.45.67    3001    3101  UDP    6           30
2         172.21.23.34    177.23.45.67    3002    3102  UDP    4           15
3         172.21.23.34    177.23.45.67    3003    3103  TCP    2           68
4         172.21.34.67    177.68.89.23    4004    4005  UDP    1           23
Console> (enable)
```

Related Commands clear qos policer
set qos rsvp

show qos statistics

Use the **show qos statistics** command to display the various QoS-related counters for a specified port.

show qos statistics {*mod*[*/port*]}

show qos statistics l3stats

Syntax Description

mod/port	Number of the module and, optionally, the number of the port on the module.
l3stats	Keyword to display Layer 3 statistics information.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

In the **show qos statistics** output, the Threshold #:Packets dropped field lists each threshold and the number of packets dropped. For example, 1:0 pkt, 2:0 pkts means that threshold 1 and threshold 2 dropped 0 packets.

Examples

This example shows how to display the QoS statistics for module 2, port 1:

```
Console> (enable) show qos statistics 2/1
Warning: QoS is disabled.
On Transmit:Port 2/1 has 2 Queue(s) 2 Threshold(s)
Q #  Threshold #:Packets dropped
---  -----------------------------------------------
1    1:0 pkts, 2:0 pkts
2    1:0 pkts, 2:0 pkts
On Receive:Port 2/1 has 1 Queue(s) 4 Threshold(s)
Q #  Threshold #:Packets dropped
---  -----------------------------------------------
1    1:0 pkts, 2:0 pkts, 3:0 pkts, 4:0 pkts
Console> (enable)
```

This example shows how to display the QoS Layer 3 statistics:

```
Console> (enable) show qos statistics l3stats
Warning: QoS is disabled.
QoS Layer 3 Statistics show statistics since last read.
Packets dropped due to policing: 0
IP packets with ToS changed:     0
IP packets with CoS changed:     26
Non-IP packets with CoS changed: 0
Console> (enable)
```

This example shows how to display the QoS statistics for module 2:

```
Console> (enable) show qos statistics 2
Warning: QoS is disabled.
On Transmit:Port 2/1 has 2 Queue(s) 2 Threshold(s)
Q #  Threshold #:Packets dropped
---  ----------------------------------------------
1    1:0 pkts, 2:0 pkts
2    1:0 pkts, 2:0 pkts
On Receive:Port 2/1 has 1 Queue(s) 4 Threshold(s)
Q #  Threshold #:Packets dropped
---  ----------------------------------------------
1    1:0 pkts, 2:0 pkts, 3:0 pkts, 4:0 pkts

On Transmit:Port 2/2 has 2 Queue(s) 2 Threshold(s)
Q #  Threshold #:Packets dropped
---  ----------------------------------------------
1    1:0 pkts, 2:0 pkts
2    1:0 pkts, 2:0 pkts
On Receive:Port 2/2 has 1 Queue(s) 4 Threshold(s)
Q #  Threshold #:Packets dropped
---  ----------------------------------------------
1    1:0 pkts, 2:0 pkts, 3:0 pkts, 4:0 pkts
Console> (enable)
```

Related Commands

set qos
set qos drop-threshold
set qos mac-cos
set qos txq-ratio
set qos wrr

show qos statistics export info

Use the **show qos statistics export info** command to display QoS data export configuration and statistical information.

show qos statistics export info

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display QoS data export configuration and statistical information:

```
Console> (enable) show qos statistics export info
QoS Statistics Status and Configuration Information
---------------------------------------------------
Export Status: disabled.
Export time interval: 35 seconds
Export destination: Stargate, UDP port 9996

Port   Export
------ --------
 1/1    enabled
 1/2   disabled
 2/2    enabled
 2/5    enabled
 2/7    enabled

Aggregate name  Export
--------------- --------
ipagg_1          enabled
ipagg_2         disabled
ipagg_3          enabled
Console> (enable)
```

Related Commands

set qos statistics export aggregate
set qos statistics export port

show qos status

Use the **show qos status** command to display if QoS is enabled on the switch.

show qos status

Syntax Description This command has no keywords or arguments.

Defaults This command has no default settings.

Command Types Switch command.

Command Modes Normal.

Examples This example shows how to display if QoS is enabled on the switch:

```
Console> (enable) show qos status
Qos is enabled on this switch.
Console> (enable)
```

Related Commands **set qos**

show radius

Use the **show radius** command to display configured RADIUS parameters.

show radius [**noalias**]

Syntax Description

noalias	(Optional) Keyword to force the display to show IP addresses, not IP aliases.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

You can enter this command in normal or privileged mode, but the RADIUS key is displayed only if this command is entered in privileged mode.

Examples

This example shows how to display RADIUS information:

```
Console> show radius
Login Authentication:  Console Session   Telnet Session
---------------------  ----------------  ----------------
tacacs                 disabled          disabled
radius                 disabled          disabled
local                  enabled(primary)  enabled(primary)

Enable Authentication: Console Session   Telnet Session
---------------------- ----------------- ----------------
tacacs                 disabled          disabled
radius                 disabled          disabled
local                  enabled(primary)  enabled(primary)

Radius Deadtime:              0 minutes
Radius Key:
Radius Retransmit:            2
Radius Timeout:               5 seconds

Radius-Server                 Status   Auth-port
----------------------------- -------  ------------
172.20.52.3                   primary  1812
Console>
```

Related Commands

- set radius deadtime
- set radius key
- set radius retransmit
- set radius server
- set radius timeout

show rcp

Use the **show rcp** command to display rcp information.

show rcp

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display rcp information:

```
Console> (enable) show rcp
rcp username for VMPS   :xena
rcp username for others :jdoe
Console> (enable)
```

Related Commands

clear rcp
set rcp username

show reset

Use the **show reset** command to display scheduled reset information.

show reset

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display scheduled reset information:

```
Console> (enable) show reset
Reset schedule for Fri Jan 21 2000, 23:00:00 (in 3 days 12 hours 56 minutes 57 seconds).
Reset reason: Software upgrade
Console> (enable)
```

Related Commands

reset—switch

show rgmp group

Use the **show rgmp group** command to display all multicast groups or the count of multicast groups that are joined by RGMP-capable routers.

show rgmp group [*mac_addr*] [*vlan_id*]

show rgmp group count [*vlan_id*]

Syntax Description

mac_addr	(Optional) MAC destination address reserved for the use of RGMP packets.
vlan_id	(Optional) Number of the VLAN; valid values are from **1** to **1005**.
count	Keyword to display the total number of entries in a VLAN group that are joined by RGMP-capable routers.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example displays all multicast groups joined by RGMP-capable routers:

```
Console> show rgmp group

Vlan          Dest MAC/Route Des    RGMP Joined Router Ports
---------------------------------------------------------------------
1             01-00-5e-00-01-28          5/1,5/15
1             01-00-5e-01-01-01          5/1
2             01-00-5e-27-23-70*         3/1,5/1
Total Number of Entries=3

'*'- Configured manually
Console>
```

This example displays the total number of entries of VLAN group 1 that are joined by RGMP-capable routers:

```
Console> show rgmp group count 1
RGMP enabled.
Total Number of Entries=2
Console>
```

Related Commands

clear rgmp statistics
set rgmp
show rgmp statistics

show rgmp statistics

Use the **show rgmp statistics** command to display all the RGMP-related statistics for a given VLAN.

show rgmp statistics [*vlan*]

Syntax Description

vlan	(Optional) Number of the VLAN.

Defaults

The default is VLAN 1.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example displays RGMP-related statistics for a specific VLAN:

```
Console> show rgmp statistics 23
RGMP enabled
RGMP Statistics for vlan <23>:
Recieve:
Valid pkts:       20
Hellos:           10
Joins:            5
Leaves:           5
Join Alls:        0
Leave Alls:       0
Byes:             0
Discarded:        0
Transmit:
Total Pkts:       10
Failures:         0
Hellos:           10
Joins:            0
Leaves:           0
Join Alls:        0
Leave Alls:       0
Byes:             0
Console>
```

Related Commands

clear rgmp statistics
set rgmp
show rgmp group

show rspan

Use the **show rspan** command to display the remote SPAN configuration.

show rspan

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The fields displayed depends on the configuration. For example, if this is a source session, the Destination, Incoming Packets, and Learning fields are not displayed. If this is a destination session, the Admin Source, Oper Source, Direction, Multicast, Filter, and Max Bandwidth fields are not displayed. If there is no VLAN filtering on the source session, the Filter field is not displayed.

Examples

This example shows the display output from the **show rspan** command:

```
Console> (enable) show rspan

Destination     : -
Rspan Vlan      : 900
Admin Source    : VLAN 50
Oper Source     : Port 2/1,2/3,2/5,2/7,2/9,2/11,2/13,2/15,2/17,2/19
Direction       : receive
Incoming Packets: -
Learning        : -
Multicast       : disabled
Filter          : 10,20,30,40,500,600,700,800,900
Status          : active

-----------------------------------------

Destination     : Port 3/1
Rspan Vlan      : 901
Admin Source    : -
Oper Source     : -
Direction       : -
Incoming Packets: disabled
Learning        : disabled
Multicast       : -
Filter          : -
Status          : active
-----------------------------------------
```

```
Destination     : Port 6/1
Rspan Vlan      : 906
Admin Source    : -
Oper Source     : -
Direction       : -
Incoming Packets: disabled
Learning        : -
Multicast       : -
Filter          : -

-----------------------------------------

Destination     : -
Rspan Vlan      : 903
Admin Source    : INBAND
Oper Source     : INBAND
Direction       : transmit
Incoming Packets: -
Learning        : -
Multicast       : disabled
Filter          : -

-----------------------------------------

Destination     : Port 7/1
Rspan Vlan      : 902
Admin Source    : -
Oper Source     : -
Direction       : -
Incoming Packets: enabled
Learning        : -
Multicast       : -
Filter          : -
Console> (enable)
```

Related Commands set rspan

show running-config

Use the **show running-config** command to display the configuration information currently running on the switch or the configuration for a specific ACL.

show running-config [**system** | *mod_num*] [**all**]

show running-config acl location

show running-config qos acl {*acl_name*| **all**}

Syntax Description

system	(Optional) Keyword to display current system configuration.
mod_num	(Optional) Number of the module.
all	(Optional) Keyword to specify all modules and system configuration information, including the IP address.
acl location	Keywords to display current ACL configuration information.
qos acl *acl_name*	Keywords and variable to display current QoS ACL configuration information for a specific ACL.
qos acl all	Keywords and variable to display current QoS ACL configuration information for all ACLs.

Defaults

The default displays only nondefault configurations.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can view the entire configuration by entering the **all** keyword.

Examples

This example shows how to display the nondefault system and module configuration:

```
Console> (enable) show running-config
This command shows non-default configurations only.
Use 'show config all' to show both default and non-default configurations.
..............

..................
..................

..

begin
!
```

```
# ***** NON-DEFAULT CONFIGURATION *****
!
!
#time: Mon Jun 11 2001, 08:22:17
!
#version 6.3(0.56)PAN
!

!
#!
#vtp
set vtp domain dan
set vtp mode transparent
set vlan 1 name default type ethernet mtu 1500 said 100001 state active
set vlan 1002 name fddi-default type fddi mtu 1500 said 101002 state active
set vlan 1004 name fddinet-default type fddinet mtu 1500 said 101004 state acti
e stp ieee
set vlan 1005 name trnet-default type trbrf mtu 1500 said 101005 state active s
p ibm
set vlan 2,10-11
set vlan 1003 name token-ring-default type trcrf mtu 1500 said 101003 state act
ve mode srb aremaxhop 7 stemaxhop 7 backupcrf off
!
#ip
set interface sc0 1 172.20.52.19/255.255.255.224 172.20.52.31

set ip route 0.0.0.0/0.0.0.0         172.20.52.1
!
#set boot command
set boot config-register 0x10f
set boot system flash bootflash:cat6000-sup2-d.6-3-0-56-PAN.bin
set boot system flash bootflash:cat6000-sup2-d.6-3-0-54-PAN.bin
set boot system flash bootflash:cat6000-sup2-d.6-3-0-46-PAN.bin
set boot system flash bootflash:cat6000-sup2-d.6-3-0-44-PAN.bin
set boot system flash bootflash:
!
#qos
set qos wred 1p2q2t tx queue 1 60:80 80:100
set qos wred 1p2q2t tx queue 2 60:80 80:100
set qos wred 1p3q1t tx queue 1 80:100
set qos wred 1p3q1t tx queue 2 80:100
set qos wred 1p3q1t tx queue 3 80:100
!
#mmls nonrpf
set mmls nonrpf timer 0
!
#security ACLs
clear security acl all
#pbf set
set pbf mac 00-01-64-61-39-c3
#adj set
set security acl adjacency ADJ2 10 00-00-00-00-00-0a 00-00-00-00-00-0b mtu 9600
#
commit security acl all
!
# default port status is enable
!
!
#module 1 empty
!
#module 2 : 2-port 1000BaseX Supervisor
!
#module 3 : 48-port 10/100BaseTX Ethernet
set vlan 10   3/1
```

```
set vlan 11   3/2
!
#module 4 empty
!
#module 5 : 0-port Switch Fabric Module
!
#module 6 empty
!
#module 7 empty
!
#module 8 empty
!
#module 9 empty
!
#module 15 empty
!
#module 16 empty
end
Console> (enable)
```

This example shows how to display the nondefault system configuration for module 3:

```
Console> (enable) show running-config 3
This command shows non-default configurations only.
Use 'show config <mod> all' to show both default and non-default configurations.
.....................
begin
!
# ***** NON-DEFAULT CONFIGURATION *****
!
!
#time: Mon Jun 11 2001, 08:33:25
!
# default port status is enable
!
!
#module 3 : 48-port 10/100BaseTX Ethernet
set vlan 10   3/1
set vlan 11   3/2
end
Console> (enable)
```

Related Commands

clear config
show startup-config
write

show security acl

Use the **show security acl** command to display the contents of the VACL that are currently configured or last committed to NVRAM and hardware.

show security acl

show security acl [**editbuffer**]

show security acl info {*acl_name* | **adjacency**| **all**} [**editbuffer** [*editbuffer_index*]]

Syntax Description

editbuffer	(Optional) Keyword to display the VACLs in the edit buffer.
info	Keyword to display the contents of a VACL that were last committed to NVRAM and hardware.
acl_name	Name of the VACL to be displayed.
adjacency	Keyword to display adjacency information.
all	Keyword to display all ACL information.
editbuffer_index	(Optional) Name of the edit buffer index.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the name and type of the VACLs currently configured:

```
Console> show security acl
ACL                              Type VLANS
-------------------------------  ---- -----
ip1                              IP   3,5,8
ip2                              IP   12,47
ip3                              IP   56
ipx1                             IPX  5,12,45
ipx2                             IPX
ipx3                             IPX
mac2                             MAC  5
iplast                           IP
Console>
```

This example shows how to display VACLs in the edit buffer:

```
Console> show security acl editbuffer
ACL                              Type Status
-------------------------------  ---- -------------------
ip1                              IP   Committed
ip2                              IP   Committed
ip3                              IP   Committed
```

```
ipx1                              IPX  Committed
ipx2                              IPX  Committed
ipx3                              IPX  Committed
mac2                              MAC  Committed
iplast                            IP   Committed
Console>
```

This example shows how to display the configuration for a specified VACL last committed to NVRAM and hardware:

```
Console> show security acl info ip1
set security acl ip ip1
---------------------------------------------------
1. permit any
Console>
```

This example shows how to display the configuration for all VACLs last committed to NVRAM and hardware:

```
Console> show security acl info all
set security acl adjacency a_1
---------------------------------------------------
1. 2 00-0a-0a-0a-0a-0a

set security acl adjacency a_2
---------------------------------------------------
1. 2 00-0a-0a-0a-0a-0b

set security acl adjacency a_3
---------------------------------------------------
1. 2 00-0a-0a-0a-0a-0c

set security acl adjacency a_4
---------------------------------------------------
1. 2 00-0a-0a-0a-0a-0d

set security acl adjacency b_1
---------------------------------------------------
1. 1 00-20-20-20-20-20

set security acl adjacency b_2
---------------------------------------------------
1. 1 00-20-20-20-20-21

set security acl adjacency b_3
---------------------------------------------------
1. 1 00-20-20-20-20-22

set security acl adjacency b_4
---------------------------------------------------
1. 1 00-20-20-20-20-23


set security acl ip ip1
---------------------------------------------------
arp permit
1. redirect a_1 ip host 44.0.0.1 host 43.0.0.1
2. redirect a_2 ip host 44.0.0.2 host 43.0.0.2
3. redirect a_3 ip host 44.0.0.3 host 43.0.0.3
4. redirect a_4 ip host 44.0.0.4 host 43.0.0.4
5. permit ip any any

set security acl ip ip2
```

```
--------------------------------------------------
arp permit
1. redirect b_1 ip host 43.0.0.1 host 44.0.0.1
2. redirect b_2 ip host 43.0.0.2 host 44.0.0.2
3. redirect b_3 ip host 43.0.0.3 host 44.0.0.3
4. redirect b_4 ip host 43.0.0.4 host 44.0.0.4
5. permit ip any any


Console>
```

This example shows how to display the contents of the VACL edit buffer:

```
Console> show security acl info ip1 editbuffer
set security acl ip ip1
--------------------------------------------------
1. permit any

ACL Status:Committed
Console>
```

Related Commands

clear security acl
commit
rollback

show security acl capture-ports

Use the **show security acl capture-ports** command to display the capture port list.

show security acl capture-ports

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to display capture port list entries:

```
Console> (enable) show security acl capture-ports
ACL Capture Ports: 1/2,2/2
Console> (enable)
```

Related Commands

clear security acl capture-ports
set security acl capture-ports

show security acl log

Use the **show security acl log** command to display VACL log information.

show security acl log config

show security acl log flow *protocol* {*src_ip_spec* | *dest_ip_spec*} [**vlan** *vlan_num*]

show security acl log flow {**ip**} {*src_ip_spec* | *dest_ip_spec*} [**vlan** *vlan_num*]

show security acl log flow {**icmp** | **1**} {*src_ip_spec* | *dest_ip_spec*} [*icmp_type* [*icmp_code*]] [**vlan** *vlan_num*]

show security acl log flow {**tcp** | **6**} {{*src_ip_spec* [*operator port* [*port*]]} | {*dest_ip_spec* [*operator port* [*port*]]}} [**vlan** *vlan_num*]

show security acl log flow {**udp** | **17**} *src_ip_spec* [*operator port* [*port*]] *dest_ip_spec* [*operator port* [*port*]] [**vlan** *vlan_num*]

Syntax Description

config	Keyword to display the VACL log configuration information including the maximum number of the flow pattern and redirect rate.
flow	Keyword to display the flow information specified by the arguments since its last syslog report.
protocol	Keyword or number of an IP protocol; valid numbers are from **0** to **255** representing an IP protocol number. See the “Usage Guidelines” section for the list of valid keywords.
src_ip_spec	Source IP address and the source mask. See the “Usage Guidelines” section for the format.
dest_ip_spec	Destination IP address and the destination mask. See the “Usage Guidelines” section for the format.
vlan *vlan_num*	(Optional) Number of the VLAN to be displayed; valid values are from **1** to **1005** and from **1025** to **4094**.
ip	Keyword to match any Internet Protocol packets.
icmp | **1**	Keyword or number to match ICMP packets.
icmp_type	(Optional) ICMP message type name or a number; valid values are from **0** to **255**. See the “Usage Guidelines” section for a list of valid names.
icmp_code	(Optional) ICMP message code name or a number; valid values are from **0** to **255**. See the “Usage Guidelines” section for a list of valid names.
tcp | **6**	Keyword or number to match TCP packets.
operator	(Optional) Operands; valid values include **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range).
port	(Optional) Number or name of a TCP or UDP port; valid port numbers are from **0** to **65535**. See the “Usage Guidelines” section for a list of valid names.
udp | **17**	Keyword or number to match UDP packets.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is supported on systems configured with Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) only.

Configurations you make by entering this command are saved to NVRAM and hardware only after you enter the **commit** command. Enter ACEs in batches and then enter the **commit** command to save them in NVRAM and in the hardware.

When you specify the source IP address and the source mask, use the form *source_ip_address source_mask* and follow these guidelines:

- The *source_mask* is required; 0 indicates a care bit, 1 indicates a don't-care bit.
- Use a 32-bit quantity in four-part dotted-decimal format.
- Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.
- Use **host** source as an abbreviation for a *source* and *source-wildcard* of source 0.0.0.0.

Valid *protocol* keywords include **icmp** (1), **ip**, **ipinip** (4), **tcp** (6), **udp** (17), **igrp** (9), **eigrp** (88), **gre** (47), **nos** (94), **ospf** (89), **ahp** (51), **esp** (50), **pcp** (108), and **pim** (103). The IP number is displayed in parentheses. Use the keyword **ip** to match any Internet Protocol.

ICMP packets that are matched by ICMP message type can also be matched by the ICMP message code.

Valid names for *icmp_type* and *icmp_code* are administratively-prohibited, alternate-address, conversion-error, dod-host-prohibited, dod-net-prohibited, echo, echo-reply, general-parameter-problem, host-isolated, host-precedence-unreachable, host-redirect, host-tos-redirect, host-tos-unreachable, host-unknown, host-unreachable, information-reply, information-request, mask-reply, mask-request, mobile-redirect, net-redirect, net-tos-redirect, net-tos-unreachable, net-unreachable, network-unknown, no-room-for-option, option-missing, packet-too-big, parameter-problem, port-unreachable, precedence-unreachable, protocol-unreachable, reassembly-timeout, redirect, router-advertisement, router-solicitation, source-quench, source-route-failed, time-exceeded, timestamp-reply, timestamp-request, traceroute, ttl-exceeded, and unreachable.

If the operator is positioned after the source and source-wildcard, it must match the source port. If the operator is positioned after the destination and destination-wildcard, it must match the destination port. The range operator requires two port numbers. All other operators require one port number.

TCP port names can be used only when filtering TCP. Valid names for TCP ports are bgp, chargen, daytime, discard, domain, echo, finger, ftp, ftp-data, gopher, hostname, irc, klogin, kshell, lpd, nntp, pop2, pop3, smtp, sunrpc, syslog, tacacs-ds, talk, telnet, time, uucp, whois, and www.

UDP port names can be used only when filtering UDP. Valid names for UDP ports are biff, bootpc, bootps, discard, dns, dnsix, echo, mobile-ip, nameserver, netbios-dgm, netbios-ns, ntp, rip, snmp, snmptrap, sunrpc, syslog, tacacs-ds, talk, tftp, time, who, and xdmcp.

The number listed with the protocol type is the layer protocol number (for example, **udp | 17**).

Examples

This example shows how to display VACL log information:

```
Console> (enable) show security acl log config
VACL LOG Configration
------------------------------------------------------------
Max Flow Pattern    : 512
Redirect Rate (pps) : 1000
Console> (enable)
```

This example shows how to display the flow information:

```
Console> (enable) show security acl log flow ip vlan 1
Total matched entry number = 1
Entry No. #1, IP Packet
---------------------------------------
Vlan Number             : 1
Mod/Port Number         : 2/1
Source IP address       : 21.0.0.0
Destination IP address : 255.255.255.255
TCP Source port         : 2000
TCP Destination port    : 3000
Received Packet Number : 10
Console> (enable)
```

Related Commands

clear security acl log flow
set security acl log

show security acl map

Use the **show security acl map** command to display VACL-to-VLAN mapping for a specified VACL or VLAN.

show security acl map *acl_name*

show security acl map *vlan*

Syntax Description

acl_name	Name of the VACL to be displayed.
vlan	Number of the VLAN to be displayed; valid values are from **1** to **1005** and from **1025** to **4094**.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the mappings of a specific VACL:

```
Console> (enable) show security acl map IPACL1
ACL IPACL1 is mapped to VLANs:
1
Console> (enable)
```

This example shows how to display the mappings of a specific VLAN:

```
Console> (enable) show security acl map 1
VLAN 1 is mapped to IP ACL IPACL1.
VLAN 1 is mapped to IPX ACL IPXACL1.
VLAN 1 is mapped to MAC ACL MACACL1.
Console> (enable)
```

Related Commands

clear security acl map
commit
rollback
set security acl map

show security acl resource-usage

Use the **show security acl resource-usage** command to display VACL management information.

show security acl resource-usage

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The switch interface mapping table that associates an interface (for example, VLANs) into flows programmed in TCAM.

Hardware resources are used to calculate Layer 4 port operation; for example, if you enter the **permit tcp any lt 20 host 1.2.3.4 gt 30** command, "**lt 20**" and "**gt 30**" are the Layer 4 port operation.

Examples

This example shows how to display VACL management information:

```
Console> (enable) show security acl resource-usage
ACL resource usage:
ACL storage (mask/value) :(50%/19%)
ACL to switch interface mapping table :2%
ACL layer 4 port operators :0%
Console> (enable)
```

Table 2-73 describes the possible fields in the **show security acl resource-usage** command output.

Table 2-73 show security acl resource-usage Command Output Fields

Field	Description
ACL storage (mask/value)	Status of mask entry usage, where mask is the percentage of mask entries used, and value is the percentage of value entries currently used.
ACL to switch interface mapping table	Percentage of ACL to switch interface mapping table usage.
ACL layer 4 port operators	Percentage of ACL Layer 4 port operators.

Related Commands

clear security acl
commit
rollback

show snmp

Use the **show snmp** command to display SNMP information.

show snmp [**noalias**]

Syntax Description

noalias	(Optional) Keyword that forces the display to show IP addresses, not IP aliases.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal and privileged.

Usage Guidelines

If you enter **show snmp** in privileged mode, the output display includes information for the read-only, the read-write, and the read-write-all community strings. If you enter **show snmp** in normal mode, the display includes only information for the read-only community string.

Examples

This example shows SNMP information when you enter the **show snmp** command in normal mode:

```
Console> show snmp
RMON:                        Disabled
Extended RMON Netflow Enabled : None.
Memory usage limit for new RMON entries: 85 percent
Traps Enabled:
None
Port Traps Enabled: None

Community-Access     Community-String
----------------     --------------------
read-only            public

Trap-Rec-Address                            Trap-Rec-Community
------------------------------------------  --------------------
192.122.173.42                              public
Console>
```

This example shows SNMP information when you enter the **show snmp** command in privileged mode:

```
Console> (enable) show snmp
RMON: Enabled
Extended Rmon: Extended RMON module is not present
Traps Enabled: Chassis
Port Traps Enabled: None
```

```
Community-Access     Community-String
---------------      --------------------
read-only            public
read-write           private
read-write-all       secret

Trap-Rec-Address                          Trap-Rec-Community
----------------------------------------  --------------------
192.122.173.42                            public
Console>
```

Table 2-74 describes the possible fields (depending on the port type queried) in the **show snmp** command output.

Table 2-74 show snmp Command Output Fields

Field	Description
RMON	Status of whether RMON is enabled or disabled.
Extended RMON	Status of whether extended RMON is enabled or disabled.
Traps Enabled	Trap types that are enabled.
Port Traps Enabled	Set of ports whose linkup/linkdown trap is enabled.
Community-Access	Configured SNMP communities.
Community-String	SNMP community strings associated with each SNMP community.
Trap-Rec-Address	IP address or IP alias of trap receiver hosts.
Trap-Rec-Community	SNMP community string used for trap messages to the trap receiver.

Related Commands

set snmp rmon
set snmp trap

show snmp access

Use the **show snmp access** command to display SNMP access information.

show snmp access [**volatile** | **nonvolatile** | **read-only**]

show snmp access [**-hex**] g*roupname* **security-model** {**v1** | **v2c**}

show snmp access [**-hex**] g*roupname* **security-model v3** {**noauthentication** | **authentication** | **privacy**} [**context** [**-hex**] *contextname*]

Syntax Description

volatile	(Optional) Keyword to display information for volatile storage types.
nonvolatile	(Optional) Keyword to display information for nonvolatile storage types.
read-only	(Optional) Keyword to display information for read-only storage types.
-hex	(Optional) Keyword to display *groupname*, *username*, and *contextname* as a hexadecimal character.
groupname	Name of the SNMP group or collection of users who have a common access policy.
security-model v1 | **v2c** | **v3**	Keywords to specify security model v1, v2c, or v3.
noauthentication	Keyword to display information for security models not set to use authentication protocol.
authentication	Keyword to display information for authentication protocol.
privacy	Keyword to display information regarding messages sent on behalf of the user that are protected from disclosure.
context *contextname*	(Optional) Keyword and variable to specify the name of a context string.

Defaults

The default storage type is **volatile**.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you use special characters for the *groupname* (nonprintable delimiters for these parameters), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

If you do not enter a context name, a NULL context string is used.

There are three versions of SNMP:

- Version 1 (SNMPv1)—This is the initial implementation of SNMP. Refer to RFC 1157 for a full description of functionality.
- Version 2 (SNMPv2c)—The second release of SNMP, described in RFC 1902, has additions and enhancements to data types, counter size, and protocol operations.
- Version 3 (SNMPv3)—This is the most recent version of SNMP and is fully described in RFC 2571, RFC 2572, RFC 2573, RFC 2574, and RFC 2575. SNMPv3 has significant enhancements to administration and security.

The SNMP functionality on the Catalyst enterprise LAN switches for SNMP v1 and SNMP v2c remains intact; however, the functionality has greatly expanded for SNMPv3. Refer to the "Configuring SNMP" chapter of the *Catalyst 6000 Family Software Configuration Guide* for more information on SNMPv3.

The **read-only** keyword is supported for security model v3 only.

Examples

This example shows how to display all SNMP access information:

```
Console> (enable) show snmp access
Group Name:defaultROgroup
Context:
Security Model:v1
Security Level:noauthentication
Context Match:vlan-1
Read View:defaultAdminView
Write View:
Notify View:defaultAdminView
Storage Type:read-only
Row Status:active

Group Name:defaultROgroup
Context:
Security Model:v2c
Secuirty Level:noauthentication
Context Match:vlan-55
Read View:defaultAdminView
Write View:
Notify View:defaultAdminView
Storage Type:read-only
Row Status:active
```

Related Commands

clear snmp access
set snmp access
show snmp context

show snmp community

Use the **show snmp community** command to display SNMP context information.

show snmp community

show snmp community [**read-only** | **volatile | nonvolatile**]

show snmp community index [**-hex]** {*index name*}

Syntax Description

read-only	(Optional) Keyword to specify that the community is defined as read only.
volatile	(Optional) Keyword to specify the community type is defined as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Keyword to specify the community type is defined as persistent memory and the content remains after the device is turned off and on again.
index	Keyword to specify the index of community names.
-hex	(Optional) Keyword to display *index name* as a hexadecimal character.
index name	Name of the community index.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal and privileged.

Usage Guidelines

If you enter the **show snmp community** command in privileged mode, the output display includes information for the read-only, the read-write, and the read-write-all community strings. If you enter the **show snmp community** command in normal mode, the display includes only information for the read-only community string.

Examples

This example shows the output when you enter the **show snmp community** command for the read-only community string in normal mode:

```
Console> show snmp community
Community Index: sysCommunityRo.0
Community Name: public
Security Name: public
Context Name:
```

```
Transport Tag:
Storage Type: read-only
Row Status: active
Console>
```

This example shows the display output when you enter the **show snmp community** command for the read-only, the read-write, and the read-write-all community strings in privileged mode:

```
Console> (enable) show snmp community
Community Index: sysCommunityRo.0
Community Name: public
Security Name: public
Context Name:
Transport Tag:
Storage Type: read-only
Row Status: active

Community Index: sysCommunityRw.0
Community Name: private
Security Name: private
Context Name:
Transport Tag:
Storage Type: read-only
Row Status: active

Community Index: sysCommunityRwa.0
Community Name: secret
Security Name: secret
Context Name:
Transport Tag:
Storage Type: read-only
Row Status: active

Console> (enable)
```

Related Commands

clear snmp community
set snmp community

show snmp context

Use the **show snmp context** command to display SNMP context information.

show snmp context

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display SNMP context information:

```
Console> (enable) show snmp context
Index Context
----- --------
    0
    1 vlan-1
    2 vlan-55
    3 vlan-1002
    4 vlan-1003
    5 vlan-1004
    6 vlan-1005
Console> (enable)
```

Related Commands

clear snmp access
set snmp access
show snmp access

show snmp counters

Use the **show snmp counters** command to display SNMP counter information.

show snmp counters [**v3** | {{*mod/port*} {**dot1d** | **dot3** | **hcrmon** | **ifmib** | **rmon**}}]

Syntax Description

v3	(Optional) Keyword to specify SNMPv3 counters.
mod/port	Module number and port number.
dot1d	Keyword to specify dot1d counters.
dot3	Keyword to specify dot3 counters.
hcrmon	Keyword to specify HCRMON counters.
ifmib	Keyword to specify if-MIB counters.
rmon	Keyword to specify RMON counters.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal

Usage Guidelines

There are three versions of SNMP:

- Version 1 (SNMPv1)—This is the initial implementation of SNMP. Refer to RFC 1157 for a full description of functionality.
- Version 2 (SNMPv2c)—The second release of SNMP, described in RFC 1902, has additions and enhancements to data types, counter size, and protocol operations.
- Version 3 (SNMPv3)—This is the most recent version of SNMP and is fully described in RFC 2571, RFC 2572, RFC 2573, RFC 2574, and RFC 2575. SNMPv3 has significant enhancements to administration and security.

The SNMP functionality on the Catalyst enterprise LAN switches for SNMP v1 and SNMP v2c remains intact; however, the functionality has greatly expanded for SNMPv3. Refer to the "Configuring SNMP" chapter of the *Catalyst 6000 Family Software Configuration Guide* for more information on SNMPv3.

Examples

This example shows how to display all SNMP counters:

```
Console> show snmp counters
mib2 SNMP group counters:
snmpInPkts                 = 13993
snmpOutPkts                = 13960
snmpInBadVersions          = 0
snmpInBadCommunityNames    = 33
snmpInBadCommunityUses     = 0
snmpInASNParseErrs         = 0
```

```
snmpInTooBigs             = 0
snmpInNoSuchNames         = 0
snmpInBadValues           = 0
snmpInReadOnlys           = 0
snmpInGenErrs             = 0
snmpInTotalReqVars        = 61747
snmpInTotalSetVars        = 0
snmpInGetRequests         = 623
snmpInGetNexts            = 13337
snmpInSetRequests         = 0
snmpInGetResponses        = 0
snmpInTraps               = 0
snmpOutTooBigs            = 0
snmpOutNoSuchNames        = 230
snmpOutBadValues          = 0
snmpOutGenErrs            = 0
snmpOutGetRequests        = 0
snmpOutGetNexts           = 0
snmpOutSetRequests        = 0
snmpOutGetResponses       = 13960
snmpOutTraps              = 0
Console>
```

Table 2-75 describes the fields in the **show snmp counters** command output.

Table 2-75 show snmp counters Command Output Fields

Field	Description
snmpInPkts	Number of messages delivered to the SNMP entity from the transport service.
snmpOutPkts	Number of SNMP messages passed from the SNMP protocol entity to the transport service.
snmpInBadVersions	Number of SNMP messages delivered to the SNMP entity for an unsupported SNMP version.
snmpInBadCommunityNames	Number of SNMP messages delivered to the SNMP entity that used an SNMP community name not known to said entity.
snmpInBadCommunityUses	Number of SNMP messages delivered to the SNMP entity that represented an SNMP operation not allowed by the SNMP community named in the message.
snmpInASNParseErrs	Number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages.
snmpInTooBigs	Number of SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as “tooBig.”
snmpInNoSuchNames	Number of SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as “noSuchName.”
snmpInBadValues	Number of SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as “badValue.”
snmpInReadOnlys[1]	Number of valid SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as “readOnly.”
snmpInGenErrs	Number of SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as “genErr.”

Table 2-75 show snmp counters Command Output Fields (continued)

Field	Description
snmpInTotalReqVars	Number of MIB objects retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.
snmpInTotalSetVars	Number of MIB objects altered successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs.
snmpInGetRequests	Number of SNMP Get-Request PDUs accepted and processed by the SNMP protocol entity.
snmpInPkts	Number of messages delivered to the SNMP entity from the transport service.
snmpOutPkts	Number of SNMP messages passed from the SNMP protocol entity to the transport service.
snmpInBadVersions	Number of SNMP messages delivered to the SNMP entity for an unsupported SNMP version.
snmpInBadCommunityNames	Number of SNMP messages delivered to the SNMP entity that used an SNMP community name not known to said entity.
snmpInBadCommunityUses	Number of SNMP messages delivered to the SNMP entity that represented an SNMP operation not allowed by the SNMP community named in the message.
snmpInASNParseErrs	Number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages.
snmpInTooBigs	Number of SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as “tooBig.”
snmpInNoSuchNames	Number of SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as “noSuchName.”
snmpInBadValues	Number of SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as “badValue.”
snmpInGenErrs	Number of SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as “genErr.”
snmpInTotalReqVars	Number of MIB objects retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.
snmpInTotalSetVars	Number of MIB objects altered successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs.
snmpInGetRequests	Number of SNMP Get-Request PDUs accepted and processed by the SNMP protocol entity.
snmpInGetNexts	Number of SNMP Get-Next PDUs accepted and processed by the SNMP protocol entity.
snmpInSetRequests	Number of SNMP Set-Request PDUs accepted and processed by the SNMP protocol entity.
snmpInGetResponses	Number of SNMP Get-Response PDUs accepted and processed by the SNMP protocol entity.

Table 2-75 show snmp counters Command Output Fields (continued)

Field	Description
snmpInTraps	Number of SNMP Trap PDUs accepted and processed by the SNMP protocol entity.
snmpOutTooBigs	Number of SNMP PDUs generated by the SNMP protocol entity with the value of the error-status field as “tooBig.”
snmpOutNoSuchNames	Number of SNMP PDUs generated by the SNMP protocol entity with the value of the error-status as “noSuchName.”
snmpOutBadValues	Number of SNMP PDUs generated by the SNMP protocol entity with the value of the error-status field as “badValue.”
snmpOutGenErrs	Number of SNMP PDUs generated by the SNMP protocol entity with the value of the error-status field as “genErr.”
snmpOutGetRequests	Number of SNMP Get-Request PDUs generated by the SNMP protocol entity.
snmpOutGetNexts	Number of SNMP Get-Next PDUs generated by the SNMP protocol entity.
snmpOutSetRequests	Number of SNMP Set-Request PDUs generated by the SNMP protocol entity.
snmpOutGetResponses	Number of SNMP Get-Response PDUs generated by the SNMP protocol entity.
snmpOutTraps	Number of SNMP Trap PDUs generated by the SNMP protocol entity.

1. It is a protocol error to generate an SNMP PDU that contains the value “readOnly” in the error-status field. This object is provided as a means of detecting incorrect implementations of the SNMP.

This example shows how to display the SNMPv3 counters:

```
Console> show snmp counters v3
snmpv3 MPD statistics:
snmpUnknownSecurityModels     = 0
snmpInvalidMsgs               = 0
snmpUnknownPDUHandlers        = 0

snmpv3 TARGET statistics:
snmpUnavailableContexts       = 0
snmpUnknownContexts           = 0

snmpv3 USM statistics:
usmStatsUnsupportedSecLevels  = 0
usmStatsNotInTimeWindows      = 0
usmStatsUnknownUserNames      = 0
usmStatsUnknownEngineIDs      = 0
usmStatsWrongDigests          = 0
usmStatsDecryptionErrors      = 0
Console>
```

show snmp engineid

Use the **show snmp engineid** command to display the SNMP local engine ID.

show snmp engineid

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If the SNMP engine ID is cleared, the system automatically regenerates a local SNMP engine ID.

The SNMP engine and the SNMP entity have a one-to-one mapping. You can also identify the SNMP entity, which is represented as hexadecimal numbers only, and must be from 5 to 32 bytes long; for example, 00:00:00:09:0a:fe:ff:12:97:33:45:12.

Examples

This example shows how to display the SNMP engine ID:

```
Console> (enable) show snmp engineid
EngineId: 00:00:00:09:00:d0:00:4c:18:00
Engine Boots: 1234455
Console> (enable)
```

Table 2-76 describes the fields in the **show snmp engineid** command output.

Table 2-76 show snmp engineid Command Output Fields

Field	Description
EngineId	String identifying the name of the SNMP copy on the device.
Engine Boots	Number of times an SNMP engine has been started or reinitialized.

Related Commands

show snmp

show snmp group

Use the **show snmp group** command to display the name of the SNMP group or collection of users who have a common access policy.

show snmp group [**volatile** | **nonvolatile** | **read-only**]

show snmp group [**-hex**] {*groupname*} [**-hex**] **user** {*username*}
[**security-model** {**v1** | **v2c** | **v3**}]

Syntax Description

volatile	(Optional) Keyword to specify the storage type is defined as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Keyword to specify the storage type is defined as persistent memory and the content remains after the device is turned off and on again.
read-only	(Optional) Keyword to specify that the storage type is defined as read only.
-hex	(Optional) Keyword to display *groupname* and *username* as a hexadecimal character.
groupname	Name of the SNMP group or collection of users who have a common access policy.
user *username*	Keyword and variable to specify the SNMP group username.
security-model v1 | **v2c** | **v3**	(Optional) Keywords to specify security model v1, v2c, or v3.

Defaults

The default storage type is **volatile**.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you use special characters for the *groupname* and *username* (nonprintable delimiters for these parameters), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

There are three versions of SNMP:

- Version 1 (SNMPv1)—This is the initial implementation of SNMP. Refer to RFC 1157 for a full description of functionality.
- Version 2 (SNMPv2c)—The second release of SNMP, described in RFC 1902, has additions and enhancements to data types, counter size, and protocol operations.
- Version 3 (SNMPv3)—This is the most recent version of SNMP and is fully described in RFC 2571, RFC 2572, RFC 2573, RFC 2574, and RFC 2575. SNMPv3 has significant enhancements to administration and security.

The SNMP functionality on the Catalyst enterprise LAN switches for SNMP v1 and SNMP v2c remains intact; however, the functionality has greatly expanded for SNMPv3. Refer to the "Configuring SNMP" chapter of the *Catalyst 6000 Family Software Configuration Guide* for more information on SNMPv3.

The **read-only** keyword is supported for security model v3 only.

Examples

This example shows how to display the SNMP group:

```
Console> (enable) show snmp group
Security Model: v1
Security Name: public
Group Name: defaultROgroup
Storage Type: volatile
Row Status: active

Security Model: v1
Security Name: secret
Group Name: defaultRWALLgroup
Storage Type: volatile
Row Status: active

Security Model: v1
Security Name: private
Group Name: defaultRWgroup
Storage Type: volatile
Row Status: active

Security Model: v2c
Security Name: public
Group Name: defaultROgroup
Storage Type: volatile
Row Status: active
Console> (enable)
```

Table 2-77 describes the fields in the **show snmp group** command output.

Table 2-77 show snmp group Command Output Fields

Field	Description
Security Model	Security model used by the group.
Security Name	Security string definition.
Group Name	Name of the SNMP group or collection of users who have a common access policy.
Storage Type	Keyword to indicate whether the settings are volatile or nonvolatile.
Row Status	Status of the entry.

Related Commands

clear snmp group
set snmp group

show snmp notify

Use the **show snmp notify** command to display the snmpNotifyTable configuration.

show snmp notify [**volatile** | **nonvolatile** | **read-only**]

show snmp notify [**-hex**] {*notifyname*}

Syntax Description

volatile	(Optional) Keyword to specify the storage type is defined as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Keyword to specify the storage type is defined as persistent memory and the content remains after the device is turned off and on again.
read-only	(Optional) Keyword to specify that the storage type is defined as read only.
-hex	(Optional) Keyword to display *notifyname* as a hexadecimal character.
notifyname	A unique identifier to index the snmpNotifyTable.

Defaults

The default storage type is **nonvolatile**.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you use special characters for the *notifyname* (nonprintable delimiters for this parameter), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

The **read-only** keyword is supported for security model v3 only.

Examples

This example shows how to display the SNMP notify information for a specific *notifyname*:

```
Console> (enable) show snmp notify snmpV1Notification
Notify Name: snmpV1Notification
Notify Tag: snmpV1Trap
Notify Type: trap
Storage Type: volatile
Row Status: active
Console> (enable)
```

Table 2-78 describes the fields in the **show snmp notify** command output.

Table 2-78 show snmp notify Command Output Fields

Field	Description
Notify Name	Unique identifier used to index the snmpNotifyTable.
Notify Tag	Name of the entry in the snmpNotifyTable.
Notify Type	Type of notification.
Storage Type	Storage type (volatile or nonvolatile).
Row Status	Status of the entry.

Related Commands

clear snmp notify
set snmp notify

show snmp rmonmemory

Use the **show snmp rmonmemory** command to display the memory usage limit in percentage.

show snmp rmonmemory

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The percentage value displayed indicates that you cannot create new RMON entries or restore entries from the NVRAM if the specified memory usage is exceeded.

Examples

This example shows how to display the RMON memory limit use:

```
Console> (enable) show snmp rmonmemory
85 percent
Console> (enable)
```

Related Commands

set snmp rmonmemory

show snmp targetaddr

Use the **show snmp targetaddr** command to display the SNMP target address entries in the snmpTargetAddressTable.

show snmp targetaddr [**volatile** | **nonvolatile** | **read-only**]

show snmp targetaddr [**-hex**] {*addrname*}

Syntax Description

volatile	(Optional) Keyword to specify the storage type is defined as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Keyword to specify the storage type is defined as persistent memory and the content remains after the device is turned off and on again.
read-only	(Optional) Keyword to specify that the storage type is defined as read only.
-hex	(Optional) Keyword to display *addrname* as a hexadecimal character.
addrname	Name of the target agent; the maximum length is 32 bytes.

Defaults

The default storage type is **nonvolatile**.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you use special characters for the *addrname* (nonprintable delimiters for this parameter), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

The **read-only** keyword is supported for security model v3 only.

Examples

This example shows how to display specific target address information in the snmpTargetAddressTable:

```
Console> (enable) show snmp targetaddr cisco
Target Address Name: cisco
IP Address: 170.0.25.1
UDP Port#: 165
Timeout: 100
Retry count: 5
Tag List: tag1 tag2 tag3
Parameters: jeorge
Storage Type: nonvolatile
Row Status: active
Console> (enable)
```

Table 2-79 describes the fields in the **show snmp targetaddr** command output.

Table 2-79 show snmp targetaddr Command Output Fields

Field	Description
Target Address Name	Name of the target address.
IP Address	Target IP address.
UDP Port #	Number of the UDP port of the target host to use.
Timeout	Number of timeouts.
Retry count	Number of retries.
Tag List	Tags that point to target addresses to send notifications to.
Parameters	Entry in the snmpTargetParamsTable; the maximum length is 32 bytes.
Storage Type	Storage type (volatile or nonvolatile).
Row Status	Status of the entry.

Related Commands

clear snmp targetaddr
set snmp targetaddr

show snmp targetparams

Use the **show snmp targetparams** command to display the SNMP parameters used in the snmpTargetParamsTable when generating a message to a target.

show snmp targetparams [**volatile** | **nonvolatile** | **read-only**]

show snmp targetparams [**-hex**] {*paramsname*}

Syntax Description

volatile	(Optional) Keyword to specify that the storage type is defined as temporary memory and that the content is deleted if the device is turned off.
nonvolatile	(Optional) Keyword to specify the storage type is defined as persistent memory and that the content remains after the device is turned off and on again.
read-only	(Optional) Keyword to specify that the storage type is defined as read only.
-hex	(Optional) Keyword to display *paramsname* as a hexadecimal character.
paramsname	Name of the parameter in the snmpTargetParamsTable; the maximum length is 32 bytes.

Defaults

The default storage type is **volatile**.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you use special characters for the *paramsname* (nonprintable delimiters for this parameter), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

The **read-only** keyword is supported for security model v3 only.

Examples

This example shows how to display specific target parameter information in the snmpTargetParamsTable:

```
Console> (enable) show snmp targetparams snmpV1TrapParams
Target Parameter Name: snmpV1TrapParams
Message Processing Model: v1
Security Name: public
Security Level: noauthentication
Storage Type: volatile
Row Status: active
Console> (enable)
```

Table 2-80 describes the fields in the **show snmp targetparams** command output.

Table 2-80 show snmp targetparams Command Output Fields

Field	Description
Target Parameter Name	A unique identifier used to index the snmpTargetParamsTable.
Message Processing Model	Version number used by the Message Processing Model.
Security Name	Security string definition.
Security Level	Type of security level: • Authentication—The security level is set to use the authentication protocol. • Noauthentication—The security level is not set to use the authentication protocol.
Storage Type	Status of whether the settings are volatile or nonvolatile.
Row Status	Status of the entry.

Related Commands **clear snmp targetparams**
set snmp targetparams

show snmp user

Use the **show snmp user** command to display SNMP information for a specific user.

show snmp user [**volatile** | **nonvolatile** | **read-only**]

show snmp user [**-hex**] {*user*} [**remote** {*engineid*}]

show snmp user summary

Syntax Description

volatile	(Optional) Keyword to specify the storage type is defined as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Keyword to specify the storage type is defined as persistent memory and the content remains after the device is turned off and on again.
read-only	(Optional) Keyword to specify that the storage type is defined as read only.
-hex	(Optional) Keyword to display *user* as a hexadecimal character.
user	Name of the SNMP user.
remote *engineid*	(Optional) Keyword and variable to specify the username on a remote SNMP engine.
summary	Keyword to specify a summary of SNMP users.

Defaults

The default storage type is **nonvolatile**, and the local SNMP engine ID is used.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you use special characters for *user* (nonprintable delimiters for this parameter), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

The **read-only** keyword is supported for security model v3 only.

Examples

This example shows how to display specific user information:

```
Console> (enable) show snmp user joe
EngineId: 00:11:22:33:44
User Name: joe
Authentication Protocol: md5
Privacy Protocol: des56
Storage Type: volatile
Row Status: active
Console> (enable)
```

Table 2-81 describes the fields in the **show snmp user** command output.

Table 2-81 show snmp user Command Output Fields

Field	Description
EngineId	String identifying the name of the copy of SNMP on the device.
User Name	String identifying the name of the SNMP user.
Authentication Protocol	Type of authentication protocol.
Privacy Protocol	Type of privacy authentication protocol.
Storage Type	Status of whether the settings are volatile or nonvolatile.
Row Status	Status of the entry.

Related Commands

clear snmp user
set snmp user

show snmp view

Use the **show snmp view** command to display the SNMP MIB view configuration.

show snmp view [**volatile** | **nonvolatile** | **read-only**]

show snmp view [**-hex**] {*viewname*} {*subtree*}

Syntax Description

volatile	(Optional) Keyword to specify the storage type is defined as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Keyword to specify the storage type is defined as persistent memory and the content remains after the device is turned off and on again.
read-only	(Optional) Keyword to specify that the storage type is defined as read only.
-hex	(Optional) Keyword to display the *viewname* as a hexadecimal character.
viewname	Name of a MIB view.
subtree	Name of the subtree.

Defaults

The default view is **volatile**.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you use special characters for the *viewname* value (nonprintable delimiters for this parameter), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

A MIB subtree used with a mask defines a view subtree; it can be in OID format or a text name mapped to a valid OID.

The **read-only** keyword is supported for security model v3 only.

Examples

This example shows how to display the SNMP MIB view:

```
Console> (enable) show snmp view
View Name: defaultUserView
Subtree OID: 1.3.6.1
Subtree Mask:
View Type: included
Storage Type: volatile
Row Status: active
Control> (enable)
```

Table 2-82 describes the fields in the **show snmp view** command output.

Table 2-82 show snmp view Command Output Fields

Field	Description
View Name	Name of a MIB view.
Subtree OID	Name of a MIB subtree in OID format or a text name mapped to a valid OID.
Subtree Mask	Subtree mask can be all ones, all zeros, or a combination of both.
View Type	Status of whether the MIB subtree is included or excluded.
Storage Type	Storage type (volatile or nonvolatile).
Row Status	Status of the entry.

Related Commands

clear snmp view
set snmp view

show span

Use the **show span** command to display information about the current SPAN configuration.

show span [**all**]

Syntax Description

all	(Optional) Keyword to display local and remote SPAN configuration information.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display SPAN information for the switch. In this example, the SPAN source is port 2/1 and the SPAN destination is port 2/12. Only transmit traffic is monitored. Normal incoming packets are disabled on the SPAN destination port. Monitoring multicast traffic is enabled.

```
Console> (enable) show span
------------------------------------------------------------
Destination     : Port 4/1
Admin Source    : Port 2/2
Oper Source     : Port 2/2
Direction       : transmit/receive
Incoming Packets: enabled
Learning        : -
Multicast       : enabled
Filter          : 10,20,30,40,50,60,70,80,90,100
Status          : inactive
Console> (enable)
```

Table 2-83 describes the fields in the **show span** command output.

Table 2-83 show span Command Output Fields

Field	Description
Destination	Destination port for SPAN information.
Admin Source	Source port or VLAN for SPAN information.
Oper Source	Operator port or VLAN for SPAN information.
Direction	Status of whether transmit, receive, or transmit and receive information is monitored.
Incoming Packets	Status of whether reception of normal incoming packets on the SPAN destination port is enabled or disabled.

Table 2-83 show span Command Output Fields (continued)

Field	Description
Learning	Status of whether learning is enabled or disabled for the SPAN destination port.
Multicast	Status of whether monitoring multicast traffic is enabled or disabled.
Filter	Monitored VLANs in source trunk ports.
Max. Bandwidth	Bandwidth limits for SPAN traffic, in Mbps.

Related Commands

clear config
set spantree root

show spantree

Use the **show spantree** command to display spanning tree information for a VLAN or port.

show spantree [*vlan*] [**active**]

show spantree *mod*/*port*

Syntax Description

vlan	(Optional) Number of the VLAN; valid values are from **1** to **1001** and from **1025** to **4094**.
active	(Optional) Keyword to display only the active ports.
mod/*port*	Number of the module and the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify the VLAN number, VLAN 1 is displayed.

If you are in MISTP mode, instance information is not displayed.

The maximum length of the channel port list can be 47. The spaces in the Port(s) column may not be enough to display the entire list in one line. If this is the case, the port list is split into multiple lines. For example, in the following display, ports 6/5-8, 6/13, 6/15, 6/17, 6/19 are channeling:

```
...
Port(s)                  Vlan Port-State    Cost      Prio Portfast Channel_id
------------------------ ---- ------------ --------- ---- -------- ----------
6/5-8,6/13,6/15,6/17,6/1 1    not-connected 2684354   32   disabled 0
9
...
```

The LACP channel protocol does not support half-duplex links. If a port is in active/passive mode and becomes half duplex, the port is suspended (and a syslog message is generated). The port is shown as "connected" using the **show port** command and as "not connected" using the **show spantree** command. This discrepancy is because the port is physically connected but never joined spanning tree. To get the port to join spanning tree, either set the duplex to full or set the channel mode to off for that port.

Examples

This example (while in PVST+ mode) shows how to display the active spanning tree port configuration for VLAN 1:

```
Console> (enable) show spantree 1 active
VLAN 1
Spanning tree mode          PVST+
Spanning tree type          ieee
Spanning tree enabled

Designated Root             00-60-70-4c-70-00
Designated Root Priority    16384
Designated Root Cost        19
Designated Root Port        2/3
Root Max Age   14 sec   Hello Time 2  sec   Forward Delay 10 sec

Bridge ID MAC ADDR          00-d0-00-4c-18-00
Bridge ID Priority          32768
Bridge Max Age 20 sec   Hello Time 2  sec   Forward Delay 15 sec

Port                     Vlan Port-State    Cost      Prio Portfast Channel_id
------------------------ ---- ------------- --------- ---- -------- ----------
 2/3                     1    forwarding           19   32 disabled 0
 2/12                    1    forwarding           19   32 disabled 0
Console> (enable)
```

This example (while in MISTP mode) shows how to display the active spanning tree port configuration for VLAN 1:

```
Console> (enable) show spantree 1 active
VLAN 1
Spanning tree mode          MISTP
Spanning tree type          ieee
Spanning tree enabled
VLAN mapped to MISTP Instance: 1

Port                     Vlan Port-State    Cost      Prio Portfast Channel_id
------------------------ ---- ------------- --------- ---- -------- ----------
 2/3                     1    forwarding       200000   32 disabled 0
 2/12                    1    forwarding       200000   32 disabled 0
Console> (enable)
```

Table 2-84 describes the fields in the **show spantree** command output:

Table 2-84 show spantree Command Output Fields

Field	Description
VLAN	VLAN for which the spanning tree information is shown.
Spanning tree	Status of whether Spanning Tree Protocol is enabled or disabled.
Designated Root	MAC address of the designated spanning tree root bridge.
Designated Root Priority	Priority of the designated root bridge.
Designated Root Cost	Total path cost to reach the root.
Designated Root Port	Port through which the root bridge can be reached (shown only on nonroot bridges).
Root Max Age	Amount of time a BPDU packet should be considered valid.
Hello Time	Number of times the root bridge sends BPDUs.
Forward Delay	Amount of time the port spends in listening or learning mode.

Table 2-84 show spantree Command Output Fields (continued)

Port	Port number.
Vlan	VLAN to which the port belongs.
Port-State	Spanning tree port state (disabled, inactive, not-connected, blocking, listening, learning, forwarding, bridging, or type-pvid-inconsistent).
Cost	Cost associated with the port.
Prio	Priority associated with the port.
Portfast	Status of whether the port is configured to use the PortFast feature.
Channel_id	Channel ID number.

Related Commands

show spantree backbonefast
show spantree blockedports
show spantree portvlancost
show spantree statistics
show spantree summary
show spantree uplinkfast

show spantree backbonefast

Use the **show spantree backbonefast** command to display whether the spanning tree BackboneFast Convergence feature is enabled.

show spantree backbonefast

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This command is not available in MISTP mode.

This command is not available in MST mode.

Examples

This example shows how to display whether the spanning tree BackboneFast Convergence feature is enabled:

```
Console> show spantree backbonefast
Backbonefast is enabled.
Console>
```

Related Commands

set spantree backbonefast
show spantree defaultcostmode

show spantree blockedports

Use the **show spantree blockedports** command to display only the blocked ports on a per-VLAN or per-instance basis.

show spantree blockedports [*vlans*]

show spantree blockedports mistp-instance [*instance*]

show spantree blockedports mst [*instance*]

Syntax Description

vlans	(Optional) Number of the VLANs.
mistp-instance *instance*	Keyword and optional variable to display instance-specific information; valid values are from **1** to **16**.
mst *instance*	Keyword and optional variable to display instance-specific information; valid values are **0** to **15**.

Defaults

The default is all blocked ports in all VLANs are displayed.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a VLAN number, all blocked ports in the system are displayed.

Examples

This example shows how to display the blocked ports for VLAN 1002:

```
Console> show spantree blockedports 1002
Number of blocked ports (segments) in VLAN 1002 : 0
Console>
```

This example shows how to display the blocked ports for an MISTP instance:

```
Console> show spantree blockedports mistp-instance 1
Number of blocked ports (segments) in Instance 1 : 0
Console>
```

This example shows how to display the blocked ports for an MST instance:

```
Console> show spantree blockedports mst 0
Number of blocked ports (segments) in Instance 0: 0
Console>
```

Related Commands

show spantree

show spantree bpdu-skewing

Use the **show spantree bpdu-skewing** command to display BPDU skewing detection status.

show spantree bpdu-skewing *vlan* [*mod/port*]

show spantree bpdu-skewing {**mistp-instance** *instance*} *mod/port*

show spantree bpdu-skewing mst [*instance* | *mod/port*]

Syntax Description

vlan	Number of the VLAN; valid values are from **1** to **1005** and from **1025** to **4094**.
mod/port	(Optional) Number of the module and the port on the module.
mistp-instance *instance*	Keyword and variable to display instance-specific information; valid values are from **1** to **16**.
mst	Keyword to display MST instance information.
instance	(Optional) Number of the instance; valid values are from **1** to **15**.
mod/port	(Optional) Number of the module and the port on the module.

Defaults

The default is the BPDU skew status for all VLANs is displayed.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This command is not supported by the NAM.

The **mistp-instance** *instance* options are available in MISTP mode only.

You can use this command to troubleshoot slow network convergence due to skewing. Skewing occurs when spanning tree timers lapse, expected BPDUs are not received, and spanning tree detects topology changes. The difference between the expected result and the BPDUs actually received is a *skew.* The skew causes BPDUs to reflood the network to keep the spanning tree topology database up to date.

Examples

This example shows how to display the BPDU skew status for a VLAN:

```
Console> show spantree bpdu-skewing 1

Bpdu skewing statistics for vlan 1

Port            Last Skew (ms)   Worst Skew (ms)       Worst Skew Time
--------------  ---------------  ---------------  -------------------------
8/2                       5869           108370  Tue Nov 21 2000, 06:25:59
8/4                       4050           113198  Tue Nov 21 2000, 06:26:04
8/6                     113363           113363  Tue Nov 21 2000, 06:26:05
.
```

```
.
.
8/24                        4111          113922  Tue Nov 21 2000, 06:26:05
8/26                      113926          113926  Tue Nov 21 2000, 06:26:05
8/28                        4111          113931  Tue Nov 21 2000, 06:26:05
Console> (enable)
```

This example shows how to display the BPDU skew status for a specific module and port on a VLAN:

```
Console> (enable) show spantree bpdu-skewing 1 5/9
Bpdu skewing statistics for vlan 1

Port            Last Skew (ms)   Worst Skew (ms)       Worst Skew Time
--------------  ---------------  ---------------  ------------------------
 5/9                      3992             4407  Mon Mar 26 2001, 11:31:37
Console> (enable)
```

Table 2-85 describes the fields in the **show spantree bpdu-skewing** command output.

Table 2-85 show spantree bpdu-skewing Command Output Fields

Field	Description
Last Skew (ms)	Duration of the last skew; absolute time in milliseconds.
Worst Skew (ms)	Duration of the worst skew; absolute time in milliseconds.
Worst Skew Date	Date and time of the worst skew duration.

Related Commands

set spantree bpdu-skewing
show spantree summary

show spantree conflicts

Use the **show spantree conflicts** command to display the MAC address of the root switch in the instance, the time remaining before the VLAN joins the instance, and the number of seconds left before the entry expires and is removed from the table.

show spantree conflicts *vlan*

Syntax Description

vlan	Number of the VLAN.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This command is available in MISTP or MISTP/PVST+ mode only.

This command is not available in MST mode.

When only one entry is printed (or when all the entries are associated to the same instance), the VLAN is mapped to that instance. If two or more entries are associated with different instances, then the VLAN has a conflict, is blocked, and is not mapped to any instance.

The time left timers associated with the mapping of a VLAN to an MISTP instance are started with the maximum age of the BPDU and can be up to the maximum age. This field can show "inactive" to indicate the MAC address is the same as the MAC address of the switch (for example, the switch is the root). In all the other cases, the entry is a number, and the timer restarts every time an incoming BPDU confirms the mapping.

The delay timer field can display the following:

- Number in seconds that represents the timer running; this timer can be up to the maximum forward delay. The timer is initialized with the fwd delay.
- If the timer is not running, "inactive" is displayed because the VLAN is already mapped to the instance or a conflict is in progress.

Examples

This example shows the output if there are no conflicts on the specified VLAN:

```
Console> (enable) show spantree conflicts 1
No conflicts for vlan 1
Inst MAC               Delay     Time left
---- ----------------- --------- ---------
 1   00-30-a3-4a-0c-00  inactive        35
Console> (enable)
```

This example shows the output if there are conflicts on the specified VLAN:

```
Console> (enable) show spantree conflicts 1
Inst MAC               Delay     Time left
---- ----------------- --------- ---------
 1   00-30-a3-4a-0c-00  inactive        35
 3   00-30-f1-e5-00-01  inactive        23
Console> (enable)
```

Table 2-86 describes the fields in the **show spantree conflict** command output.

Table 2-86 show spantree conflict Command Output Fields

Field	Description
Inst	Instance number that is requesting to map the VLAN.
MAC	MAC address of the root sending the BPDU claiming the VLAN, taken from the root ID of the BPDU.
Delay	Time remaining before the VLAN joins the instance.
Time left	Age of the entry, as time in seconds left before the entry expires and is removed from the table.

Related Commands **show spantree mistp-instance**

show spantree defaultcostmode

Use the **show spantree defaultcostmode** command to display the current default port cost mode.

show spantree defaultcostmode

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the default port cost mode:

```
Console> (enable) show spantree defaultcostmode
Portcost and portvlancost set to use 802.1d default values.
Console> (enable)
```

Related Commands

set spantree defaultcostmode

show spantree guard

Use the **show spantree guard** command to display spanning tree guard information for the VLANs or instances on a port.

show spantree guard [*vlan*]

show spantree guard [*mod/port*]

show spantree guard mistp-instance [*instance*]

show spantree guard mistp-instance [*mod/port*]

show spantree guard mst [*instance*]

show spantree guard mst [*mod/port*]

Syntax Description

vlan	(Optional) Number of the VLAN; valid values are from **1** to **1005** and from **1025** to **4094**.
mod/*port*	(Optional) Number of the module and the port on the module.
mistp-instance *instance*	Keyword and optional variable to display MISTP instance-specific information; valid values are from **1** to **16**.
mst *instance*	Keyword and optional variable to display MST instance-specific information; valid values are from **0** to **15**.

Defaults

The default is VLAN 1, and the default port list is “all the ports” in the specified or default VLAN.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

When you enable the spanning tree root guard or loop guard feature, the command works on a per-port basis. When you enable the feature on a port, a logical port is blocked on a per-VLAN basis. This means that you can specify a port (or a list of ports) and specify a VLAN, but you cannot specify both.

Examples

This example shows how to display spanning tree guard information for a specific VLAN:

```
Console> show spantree guard 1004
Port Vlan Port-State           Guard type
---- ---- -------------------  ------------
1/1  1004  root-inconsistent    root
1/2  1004  not-connected        none
2/1  1004  loop-inconsistent    loop
2/2  1004  forwarding           loop
.
```

```
.
.
Console>
```

This example shows how to display spanning tree guard information for a specific instance:

```
Console> show spantree guard mistp-instance 3
Port                     Inst Port-State    Guard Type
------------------------ ---- ------------ ----------
1/1                      3    listening     root
1/2                      3    listening     root
Console>
```

Related Commands set spantree guard

show spantree mapping

Use the **show spantree mapping** to display VLAN and instance mapping information.

show spantree mapping [**config**]

Syntax Description

config	(Optional) Keyword to display mappings configured on the local switch.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not enter the optional **config** keyword, the mapping information propagated from the root switch in the instance is displayed. This runtime command is available in MISTP or MISTP-PVST+ mode only. If you enter the **config** keyword, the list of mappings configured on the local switch is displayed. It is available in PVST+ mode.

If you enter this command in PVST mode, this message displays:

```
Runtime vlan and instance mapping information is only available in MISTP
or
MISTP-PVST mode. Use 'show spantree mapping config' to view mappings
configured on the local switch.
```

Examples

This example shows how to display runtime VLAN and instance mapping information:

```
Console> (enable) show spantree mapping
Inst Root Mac          Vlans
---- ----------------- ----------------------------------------------------
1    00-50-3e-78-70-00 1
2    00-50-3e-78-70-00 -
3    00-50-3e-78-70-00 -
4    00-50-3e-78-70-00 -
5    00-50-3e-78-70-00 -
6    00-50-3e-78-70-00 -
7    00-50-3e-78-70-00 -
8    00-50-3e-78-70-00 -
9    00-50-3e-78-70-00 -
10   00-50-3e-78-70-00 -
11   00-50-3e-78-70-00 -
12   00-50-3e-78-70-00 -
13   00-50-3e-78-70-00 -
14   00-50-3e-78-70-00 -
15   00-50-3e-78-70-00 -
16   00-50-3e-78-70-00 -
Console> (enable)
```

This example shows how to display mappings configured on the local switch:

```
Console> (enable) show spantree mapping config
Inst Root Mac          Vlans
---- ----------------- ---------------------------------------------------
1    -                 1
2    -                 -
3    -                 -
4    -                 -
5    -                 -
6    -                 -
7    -                 -
8    -                 -
9    -                 -
10   -                 -
11   -                 -
12   -                 -
13   -                 -
14   -                 -
15   -                 -
16   -                 -
Console> (enable)
```

Related Commands set vlan

show spantree mistp-instance

Use the **show spantree mistp-instance** command to display instance information.

show spantree mistp-instance [*instance*] [**active**]

show spantree mistp-instance *mod/port*

Syntax Description

instance	(Optional) Instance number; valid values are from **1** to **16**.
active	(Optional) Keyword to display only active ports.
mod/port	Number of the module and the port on the module.

Defaults

The default instance is 1.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This command is available in MISTP mode only.

If you specify the *mod/port* number only, the VLAN mapping information is not displayed.

Examples

This example shows how to display information regarding active instances only:

```
Console> show spantree mistp-instance active
Instance 1
Spanning tree mode          MISTP
Spanning tree type          ieee
Spanning tree instance enabled

Designated Root             00-d0-00-4c-18-00
Designated Root Priority    32769  (root priority: 32768, sys ID ext: 1)
Designated Root Cost        0
Designated Root Port        none
VLANs mapped:               1
Root Max Age   20 sec   Hello Time 2  sec   Forward Delay 15 sec

Bridge ID MAC ADDR          00-d0-00-4c-18-00
Bridge ID Priority          32769  (bridge priority: 32768, sys ID ext: 1)
VLANs mapped:               1
Bridge Max Age 20 sec   Hello Time 2  sec   Forward Delay 15 sec

Port                      Inst Port-State    Cost      Prio Portfast Channel_id
------------------------- ---- ------------- --------- ---- -------- ----------
 2/3                      1    forwarding       200000   32 disabled 0
 2/12                     1    forwarding       200000   32 disabled
Console>
```

Table 2-87 describes the fields in the **show spantree mistp-instance** command output:

Table 2-87 show spantree mistp-instance Command Output Fields

Field	Description
Instance	Instance for which spanning tree information is shown.
Spanning tree mode	Spanning tree mode.
Spanning tree type	Spanning tree type.
Spanning tree instance	Status of whether spanning tree instance is enabled or disabled.
Designated Root	MAC address of the designated spanning tree root bridge.
Designated Root Priority	Priority of the designated root bridge.
Designated Root Cost	Total path cost to reach the root.
Designated Root Port	Port through which the root bridge can be reached (shown only on nonroot bridges).
VLANs mapped	Number of VLANs mapped.
Root Max Age	Amount of time a BPDU packet should be considered valid.
Hello Time	Number of times the root bridge sends BPDUs.
Forward Delay	Amount of time the port spends in listening or learning mode.
Bridge ID MAC ADDR	Bridge MAC address.
Bridge ID Priority	Part of the bridge identifier and is taken as the most significant part of the bridge ID comparisons.
Bridge Max Age	Bridge maximum age.
Hello Time	Amount of time the bridge sends BPDUs.
Forward Delay	Amount of time the bridge spends in listening or learning mode.
Port	Port number.
Instance	Instance to which the port belongs.
Port-State	Spanning tree port state (disabled, inactive, not-connected, blocking, listening, learning, forwarding, bridging, or type-pvid-inconsistent).
Cost	Cost associated with the port.
Prio	Priority associated with the port.
Portfast	Status of whether the port is configured to use the PortFast feature.
Channel_id	Channel ID number.

Related Commands

set spantree portinstancecost
set spantree portinstancepri

show spantree mst

Use the **show spantree mst** command to display MST information.

show spantree mst [*instance* | *mod/port*]

show spantree mst active

Syntax Description

instance	Number of the instance; valid values are from **0** to **15**.
mod/port	Number of the module and the port on the module.
active	Keyword to display active IST ports only.

Defaults

The default instance is instance 0 (IST).

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

You can use the **show spantree mst** command to display VLAN-specific spanning tree information.

Examples

This example shows how to display MST information:

```
Console> (enable) show spantree mst
Spanning tree mode          MST
Instance                    0
VLANs Mapped:               2-4094

Designated Root             00-04-9b-ba-48-00
Designated Root Priority    32768  (root priority:32768, sys ID ext:0)
Designated Root Cost        2000000
Designated Root Port        7/48
Root Max Age   20 sec   Hello Time 2  sec   Forward Delay 15 sec

IST Master ID MAC ADDR      00-d0-00-b3-68-00
IST Master ID Priority      32768
IST Master Path Cost        0          Remaining Hops 20

Bridge ID MAC ADDR          00-d0-00-b3-68-00
Bridge ID Priority          32768  (bridge priority:32768, sys ID ext:0)
Bridge Max Age 20 sec   Hello Time 2  sec   Forward Delay 15 sec  Max Hops 20

Port                      State         Role Cost     Prio Type
------------------------ ------------- ---- -------- ---- --------------------
 5/1                      forwarding    DESG    20000   32 P2P, Boundary(STP)
 5/2                      forwarding    DESG    20000   32 P2P, Boundary(STP)
 7/48                     forwarding    ROOT  2000000   32 Shared, Boundary
Console> (enable)
```

This example shows how to display MST instance-specific information for instance 1:

```
Console> (enable) show spantree mst 1
Spanning tree mode          MST
Instance                    1
VLANs Mapped:               1

Designated Root             00-d0-00-b3-68-00
Designated Root Priority    32769  (root priority:32768, sys ID ext:1)
Designated Root Cost        0          Remaining Hops 20
Designated Root Port        1/0

Bridge ID MAC ADDR          00-d0-00-b3-68-00
Bridge ID Priority          32769  (bridge priority:32768, sys ID ext:1)

Port                      State         Role Cost     Prio Type
------------------------ ------------- ---- -------- ---- --------------------
 5/1                      forwarding    BDRY    20000   32 P2P, Boundary(STP)
 5/2                      forwarding    BDRY    20000   32 P2P, Boundary(STP)
 7/48                     forwarding    BDRY  2000000   32 Shared, Boundary
Console> (enable)
```

This example shows how to display MST instance-specific information for port 6 on module 3:

```
console> show spantree mst 3/6
       Boundary Port:  Yes (STP)
       Edge Port:      No, (Configured) Default
       Port Guard:         Default
       Link Type:     P2P(Configured) Auto
       Inst State         Role Cost      Prio VLANs
       ---- ------------- ---- --------- ---- --------------------------------
       --
       0    forwarding    ROOT 2000000   32   1
Console>
```

Related Commands

clear spantree mst
set spantree mst config
set spantree mst redetect-protocol
show spantree
show spantree mst config

show spantree mst config

Use the **show spantree mst config** command to display the MST region information present in NVRAM and to display changes that have not been applied to the MST region configuration yet.

show spantree mst config

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the MST region information:

```
Console> show spantree mst config
Currnet (NVRAM) MST Configuration
Configuration Name:Cisco                          Revision: 1
Instance Vlans
-------- ---------------- ----------------------
IST      401-1005,1025-1999,2201-4096
1        1-50
2        51-100
3        101-300
4        -
5        -
6        2000-2200
7        301-400
8        -
9        -
10       -
11       -
12       -
13       -
14       -
15       -
================================================
New MST Region Configuration (Not applied yet)

Region Name:Catalyst                          Revision: 6000
Instance Vlans
-------- ---------------- ----------------------
IST      1-50,401-1005,1025-1999,2201-4096
1        -
2        51-100
3        101-300
4        -
5        -
6        2000-2200
```

```
7        301-400
8        -
9        -
10       -
11       -
12       -
13       -
14       -
15       -
================================================
Edit buffer is locked by: Console
Console> (enable)
```

Related Commands

clear spantree mst
set spantree mst config
set spantree mst redetect-protocol

show spantree portfast

Use the **show spantree portfast** command to display PortFast information.

show spantree portfast [*mod/port*]

Syntax Description

mod/port	(Optional) Number of the module and the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

When you enter the **show spantree portfast** command, if the designation for a port is displayed as an edge port, it is a PortFast port. Refer to Chapter 8, "Configuring Spanning Tree," and Chapter 9, "Configuring Spanning Tree PortFast, UplinkFast, BackboneFast, and Loop Guard," of the *Catalyst 6000 Family Software Configuration Guide* for more information about PortFast.

Examples

This example shows how to display PortFast information:

```
Console> show spantree portfast
Portfast BPDU guard is disabled.
Portfast BPDU filter is disabled.
Console>
```

This example shows how to display PortFast information for a specific module and port:

```
Console> show spantree portfast 3/1
Portfast:    Default
BPDU Filter: Enable
BPDU Guard:  Default
Portfast BPDU guard is disabled.
Portfast BPDU filter is disabled.
Console>
```

Related Commands

set spantree portfast
set spantree portfast bpdu-filter
set spantree portfast bpdu-guard

show spantree portinstancecost

Use the **show spantree portinstancecost** command to show the path cost for the instances on a port.

show spantree portinstancecost *mod/port*

Syntax Description

mod/port	Number of the module and the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the path cost for the MISTP instances on port 1/1:

```
Console> show spantree portinstancecost 1/1
Port 1/1 instances 1-16 have path cost 20000.
Console>
```

Related Commands

clear spantree portinstancecost
set spantree portinstancecost

show spantree portvlancost

Use the **show spantree portvlancost** command to show the path cost for the VLANs or extended-range VLANs.

show spantree portvlancost *mod/port* | **extended-range**

Syntax Description

mod/port	Number of the module and the port on the module.
extended-range	Keyword to specify extended-range VLANs.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This command is valid in PVST+ mode only.

Extended-range VLANs are from 1025 to 4094 and cannot be managed using VTP.

Examples

This example shows how to display the path cost for the VLANs on port 2/12:

```
Console> show spantree portvlancost 2/12
Port 2/12 VLANs 1-1005 have path cost 19.
Console>
```

Related Commands

clear spantree portvlancost
set spantree portvlancost

show spantree statistics

Use the **show spantree statistics** command to show spanning tree statistical information.

show spantree statistics *mod/port* [*vlan*]

show spantree statistics *mod/port* **mistp-instance** [*instance*]

show spantree statistics *mod/port* **mst** [*instance*]

Syntax Description

mod/port	Number of the module and the port on the module.
vlan	(Optional) Number of the VLAN; valid values are from **1** to **1001** and from **1025** to **4094**.
mistp-instance *instance*	Keyword and optional variable to display MISTP instance-specific information; valid values are from **1** to **16**.
mst *instance*	Keyword and optional variable to display MST instance-specific information; valid values are from **0** to **15**.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display statistical information:

```
Console> (enable) show spantree statistics 1/2 1005

SpanningTree enabled for vlanNo = 1005

                BPDU-related parameters
port spanning tree                  enabled
state                               disabled
port_id                             0xcccf
port number                         0x7eb
path cost                           80
message age (port/VLAN)             0(10)
designated_root                     00-10-2f-52-eb-ec
designated_cost                     0
designated_bridge                   00-10-2f-52-eb-ec
designated_port                     0xcccf
top_change_ack                      FALSE
config_pending                      FALSE

                PORT based information & statistics
config bpdu's xmitted (port/VLAN)    0(0)
config bpdu's received (port/VLAN)   0(0)
tcn bpdu's xmitted (port/VLAN)       0(0)
tcn bpdu's received (port/VLAN)      0(0)
```

```
forward trans count                 0

                Status of Port Timers
forward delay timer                 INACTIVE
forward delay timer value           0
message age timer                   INACTIVE
message age timer value             0
topology change timer               INACTIVE
topology change timer value         0
hold timer                          INACTIVE
hold timer value                    0
delay root port timer               INACTIVE
delay root port timer value         0

                VLAN based information & statistics
spanningtree type                   ibm
spanningtree multicast address      c0-00-00-00-01-00
bridge ID priority                          32768 (bridge priority: 32768, sys ID ext:
64)
bridge mac address                  00-10-2f-52-eb-ec
bridge hello time                   2 sec
bridge forward delay                4 sec
topology change initiator:          1/0
topology change                     FALSE
topology change time                14
topology change detected            FALSE
topology change count               0

                Other port-specific info
dynamic max age transitions         0
port bpdu ok count                  0
msg age expiry count                0
link loading                        1
bpdu in processing                  FALSE
num of similar bpdus to process     0
next state                          0
src mac count:                      0
total src mac count                 0
curr_src_mac                        00-00-00-00-00-00
next_src_mac                        00-00-00-00-00-00
channel_src_mac                     00-00-00-00-00-00
channel src count                   0
channel ok count                    0
Console> (enable)
```

This example shows how to display instance-specific information:

```
Console> (enable) show spantree statistics 2 mistp-instance 2
Port  2/1   Instance 2

SpanningTree enabled for instance = 2

                BPDU-related parameters
port spanning tree                  enabled
state                               forwarding
port_id                             0x8041
port number                         0x41
path cost                           20000
message age (port/inst)             1(20)
designated_root                     00-50-3e-8f-8c-00
designated_cost                     0
designated_bridge                   00-50-3e-8f-8c-00
designated_port                     0x8001
top_change_ack                      FALSE
```

```
config_pending                      FALSE
port_inconsistency                  none

               PORT based information & statistics
config bpdu's xmitted (port/inst)   0(0)
config bpdu's received (port/inst)  102(490)
tcn bpdu's xmitted (port/inst)      0(0)
tcn bpdu's received (port/inst)     0(0)
forward trans count                 0
scp failure count                   0

               Status of Port Timers
forward delay timer                 INACTIVE
forward delay timer value           15
message age timer                   ACTIVE
message age timer value             1
topology change timer               INACTIVE
topology change timer value         0
hold timer                          INACTIVE
hold timer value                    0
delay root port timer               INACTIVE
delay root port timer value         0
delay root port timer restarted is  FALSE

               Instance based information & statistics
spanningtree type                   ieee
spanningtree multicast address      01-80-c2-00-00-00
bridge priority                     32770
bridge mac address                  00-d0-00-b3-68-00
bridge hello time                   2 sec
bridge forward delay                15(15) sec
topology change initiator:          15/63
last topology change occured:       Sun Jun 7 2000, 09:00:03
topology change                     FALSE
topology change time                35
topology change detected            FALSE
topology change count               0
topology change last recvd. from    00-00-00-00-00-00

               Other port-specific info
dynamic max age transitions         0
port bpdu ok count                  0
msg age expiry count                0
link loading                        1
bpdu in processing                  FALSE
num of similar bpdus to process     0
received_inferior_bpdu              FALSE
next state                          3
src mac count:                      0
total src mac count                 0
curr_src_mac                        00-00-00-00-00-00
next_src_mac                        00-00-00-00-00-00
channel_src_mac                     00-00-00-00-00-00
channel src count                   0
channel ok count                    0
Console>
```

This example shows how to display MST instance-specific information:

```
Console> show spantree statistics 8/1 mst 0
Port  8/1   Instance 0

SpanningTree enabled for instance = 0

               BPDU-related parameters
port spanning tree                  enabled
state                               forwarding
port_id                             0x81c1
port number                         0x1c1
path cost                           20000
message age (port/VLAN)             0(20)
designated_root                     00-04-9b-ba-48-00
designated_cost                     33920
designated_bridge                   00-10-7b-bb-2f-00
designated_port                     0x81c1
top_change_ack                      FALSE
config_pending                      FALSE
port_inconsistency                  none

               PORT based information & statistics
config bpdu's xmitted (port/inst)   101(212)
config bpdu's received (port/inst)  101(205)
tcn bpdu's xmitted (port/inst)      0(1)
tcn bpdu's received (port/inst)     0(2)
forward trans count                 0
scp failure count                   0
root inc trans count (port/inst)    0(0)
inhibit loopguard                   FALSE
loop inc trans count (port/inst)    0(0)

               Status of Port Timers
forward delay timer                 INACTIVE
forward delay timer value           0
message age timer                   INACTIVE
message age timer value             0
topology change timer               INACTIVE
topology change timer value         0
hold timer                          INACTIVE
hold timer value                    0
delay root port timer               INACTIVE
delay root port timer value         0
delay root port timer restarted is  FALSE

               Vlan based information & statistics
spanningtree type                   ieee
spanningtree multicast address      01-80-c2-00-00-00
bridge priority                     32768
bridge mac address                  00-10-7b-bb-2f-00
bridge hello time                   2 sec
bridge forward delay                15(15) sec
topology change initiator:          1/0
last topology change occured:       Fri Sep 7 2001, 09:52:22
topology change                     FALSE
topology change time                35
topology change detected            FALSE
topology change count               3
topology change last recvd. from    00-00-00-00-00-00

               Other port-specific info
dynamic max age transitions         0
port bpdu ok count                  0
```

```
msg age expiry count                0
link loading                        0
bpdu in processing                  FALSE
num of similar bpdus to process     0
received_inferior_bpdu              FALSE
next state                          3
src mac count:                     0
total src mac count                 0
curr_src_mac                        00-00-00-00-00-00
next_src_mac                        00-00-00-00-00-00
channel_src_mac                     00-00-00-00-00-00
channel src count                   0
channel ok count                    0
Console>
```

Table 2-88 describes the possible fields in the **show spantree statistics** command output.

Table 2-88 show spantree statistics Command Output Fields

Field	Description
BPDU-related parameters	
port spanning tree	Status of whether Spanning Tree Protocol is enabled or disabled on the port.
state	Spanning tree port state (disabled, listening, learning, forwarding, or blocking).
port_id	Port identifier of the associated port.
port number	Port number.
path cost	Contribution of the path through this root port. This applies to the total path cost to the root for this bridge.
message age (port/VLAN)	Age of the received protocol information recorded for a port and the value of the Max Age parameter (shown in parentheses) recorded by the switch.
designated_root	MAC address of the designated spanning tree root bridge.
designated_cost	Cost of the path to the root offered by the designated port on the LAN to which this port is attached.
designated_bridge	Bridge identifier of the bridge assumed to be the designated bridge for the LAN associated with the port.
designated_port	Port identifier of the bridge port assumed to be the designated port for the LAN associated with the port.
top_change_ack	Value of the Topology Change Acknowledgement flag in the next configured BPDU to be transmitted on the associated port. The flag is set in reply to a Topology Change Notification BPDU.
config_pending	Boolean parameter set to record that a configured BPDU should be transmitted on expiration of the hold timer for the associated port.
port_inconsistency	Status of whether the port is in an inconsistent (PVID or port type) state or not.
PORT-based information and statistics	
config bpdu's xmitted (port/VLAN)	Number of BPDUs transmitted from the port. The number in parentheses is the number of configured BPDUs transmitted by the switch for this instance of spanning tree.
config bpdu's received (port/VLAN)	Number of BPDUs received by this port. The number in parentheses is the number of configured BPDUs received by the switch for this instance of spanning tree.
tcn bpdu's xmitted (port/VLAN)	Number of TCN BDPUs transmitted on this port.

Table 2-88 show spantree statistics Command Output Fields (continued)

Field	Description
tcn bpdu's received (port/VLAN)	Number of TCN BPDUs received on this port.
forward trans count	Number of times the port state transitioned to FORWARDing state.
scp failure count	Number of SCP failures.
Status of Port Timers	
forward delay timer	Status of the forward delay timer. This timer monitors the time spent by a port in the listening and learning states.
forward delay timer value	Current value of the forward delay timer.
message age timer	Status of the message age timer. This timer measures the age of the received protocol information recorded for a port.
message age timer value	Current value of the message age timer.
topology change timer	Status of the topology change timer. This timer determines the time period in which configured BPDUs are transmitted with the topology change flag set by the bridge when it is the root following the detection of a topology change.
topology change timer value	Current value of the topology change timer.
hold timer	Status of the hold timer. This timer ensures that configured BPDUs are not transmitted too frequently through any bridge port.
hold timer value	Current value of the hold timer.
delay root port timer	Status of the delay root port timer. This timer enables fast convergence on linkup when the UplinkFast feature is enabled.
delay root port timer value	Current value of the delay root port timer.
VLAN-based information and statistics	
spanningtree type	Type of spanning tree (IEEE, IBM, CISCO).
spanningtree multicast address	Destination address used to send out configured BPDUs on a bridge port.
bridge ID priority	Part of the bridge identifier and is taken as the most significant part bridge ID comparisons.
bridge mac address	Bridge MAC address.
bridge hello time	Value of the Hello Time parameter when the bridge is the root or is attempting to become the root.
bridge forward delay	Value of the Forward Delay parameter when the bridge is the root or is attempting to become the root.
topology change initiator:	Number of the port that caused the topology change.
topology change	Boolean parameter set to record the value of the topology change flag in config BPDUs to be transmitted by the bridge on LANs for which the bridge is the designated bridge.
topology change time	Time period for which BPDUs are transmitted with the topology change flag set by the bridge when it is the root following the detection of a topology change. It is equal to the sum of the bridge's Max Age and Forward Delay parameters.

Table 2-88 show spantree statistics Command Output Fields (continued)

Field	Description
topology change detected	Boolean parameter set to TRUE when a topology change has been detected by or notified to the bridge.
topology change count	Number of times the topology change has occurred.
topology change last recvd. from	MAC address of the bridge that transmitted the last TCN BPDU.
Other port-specific info	
dynamic max age transitions	Number of dynamic max age transitions.
port bpdu ok count	Number of reported port BPDU counts.
msg age expiry count	Number of message age expires.
link loading	Status of whether the link is oversubscribed.
bpdu in processing	Status of whether the BPDU is under processing.
num of similar bpdus to process	Number of similar BPDUs to process that are received on a specific port.
received_inferior_bpdu	Status of whether the port received an inferior BPDU or in response to an RLQ BPDU.
next state	Port state before it is actually set by spanning tree, to faciliate other tasks in using the new value.
src mac count:	Number of BPDUs with the same source MAC address.
total src mac count	Number of BPDUs with all the source MAC addresses.
curr_src_mac	Source MAC address of the configured BPDU received on a particular port. It should always be set to NULL for the Catalyst 6000 family switches.
next_src_mac	MAC address from the different source. It should always be set to NULL for the Catalyst 6000 family switches.
channel_src_mac	Source MAC address of the channel port. It is used to detect channel misconfiguration and avoid spanning tree loops.
channel src count	Number of times channel_src_mac gets changed and if the limit is exceeded, a channel misconfiguration is detected.
channel ok count	Number of times the channel ok condition was detected.

Related Commands **clear spantree statistics**
show spantree

show spantree summary

Use the **show spantree summary** command to display a summary of spanning tree information.

show spantree summary [**novlan**]

show spantree summary {**mistp-instance** | **mst**} [**noinstance**]

Syntax Description

novlan	(Optional) Keyword to display non-VLAN-specific information only.
mistp-instance	Keyword to display MISTP instance-specific information only.
mst	Keyword to display MST instance-specific information only.
noinstance	(Optional) Keyword to display non-instance-specific information only.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If the switch is not the root for any VLANs, “none” is displayed in the “Root switch for vlans” field.

Examples

This example shows how to display a summary of spanning tree information:

```
Console> show spantree summary
MAC address reduction: disabled
Root switch for vlans: none.
BPDU skewing detection disabled for the bridge
BPDU skewed for vlans:  none.
Portfast bpdu-guard disabled for bridge.
Portfast bpdu-filter disabled for bridge.
Uplinkfast disabled for bridge.
Backbonefast disabled for bridge.

Summary of connected spanning tree ports by vlan

VLAN  Blocking Listening Learning Forwarding STP Active
----- -------- --------- -------- ---------- ----------
   1         0         0        0          3          3

      Blocking Listening Learning Forwarding STP Active
----- -------- --------- -------- ---------- ----------
Total        0         0        0          3          3
Console>
```

This example shows how to display non-VLAN-specific information only:

```
Console> (enable) show spantree summary novlan
MAC address reduction:disabled
Root switch for vlans:1-8,10-500,911.
BPDU skewing detection enabled for the bridge
BPDU skewed for vlans:1-8,10-500,911.
Portfast bpdu-guard disabled for bridge.
Portfast bpdu-filter disabled for bridge.
Uplinkfast disabled for bridge.
Backbonefast disabled for bridge.

      Blocking Listening Learning Forwarding STP Active
----- -------- --------- -------- ---------- ----------
Total      506         0        0        506       1012
Console> (enable)
```

This example shows how to display a summary of spanning tree instance information:

```
Console> show spantree summary mistp-instance
MAC address reduction:disabled
Root switch for vlans:1-8,10-500,911.
BPDU skewing detection enabled for the bridge
BPDU skewed for vlans:1-8,10-500,911.
Portfast bpdu-guard disabled for bridge.
Portfast bpdu-filter disabled for bridge.
Uplinkfast disabled for bridge.
Backbonefast disabled for bridge.

Summary of connected spanning tree ports by mistp-instance

Inst  Blocking Listening Learning Forwarding STP Active
----- -------- --------- -------- ---------- ----------
   1         0         0        0          8          0
   2         4         0        0          4          8
   3         4         0        0          4          8
   4         4         0        0          4          8
   5         4         0        0          4          8
   6         4         0        0          4          8
   7         4         0        0          4          8
   8         4         0        0          4          8
   9         4         0        0          4          8
  10         4         0        0          4          8
  11         4         0        0          4          8
  12         4         0        0          4          8
  13         4         0        0          4          8
  14         4         0        0          4          8
  15         4         0        0          4          8
  16         0         0        0          0          0

      Blocking Listening Learning Forwarding STP Active
----- -------- --------- -------- ---------- ----------
Total       56         0        0         64        112
Console>
```

This example shows how to display a summary of spanning tree MST instance information:

```
Console> show spantree summary mst
MAC address reduction:disabled
Root switch for MST instances:none.
Global loopguard is disabled on the switch.
Global portfast is disabled on the switch.
BPDU skewing detection enabled for the bridge.
BPDU skewed for MST instances: none.
Portfast bpdu-guard disabled for bridge.
Portfast bpdu-filter disabled for bridge.

Summary of connected spanning tree ports by MST instances

Inst  Blocking Listening Learning Forwarding STP Active
----- -------- --------- -------- ---------- ----------
   0         0         0        0          3          3
   1         0         0        0          0          0
   2         0         0        0          0          0
   3         0         0        0          0          0
   4         0         0        0          0          0
   5         0         0        0          0          0
   6         0         0        0          0          0
   7         0         0        0          0          0
   8         0         0        0          0          0
   9         0         0        0          0          0
  10         0         0        0          0          0
  11         0         0        0          0          0
  12         0         0        0          0          0
  13         0         0        0          0          0
  14         0         0        0          0          0
  15         0         0        0          0          0

      Blocking Listening Learning Forwarding STP Active
----- -------- --------- -------- ---------- ----------
Total        0         0        0          3          3
Console>
```

This example shows how to display a summary of spanning tree noninstance-specific MST information:

```
Console> show spantree summary mst noinstance
MAC address reduction:disabled
Root switch for MST instances:none.
Global loopguard is disabled on the switch.
Global portfast is disabled on the switch.
BPDU skewing detection enabled for the bridge.
BPDU skewed for MST instances: none.
Portfast bpdu-guard disabled for bridge.
Portfast bpdu-filter disabled for bridge.

      Blocking Listening Learning Forwarding STP Active
----- -------- --------- -------- ---------- ----------
Total        0         0        0          3          3
Console>
```

Related Commands show spantree

show spantree uplinkfast

Use the **show spantree uplinkfast** command to show the UplinkFast feature settings.

show spantree uplinkfast [{**mistp-instance** [*instances*]} | *vlans*]

Syntax Description

mistp-instance *instances*	(Optional) Keyword and (optional) variable to display instance-specific information; valid values are from **1** to **16**.
vlans	(Optional) Number of the VLAN; valid values are from **1** to **1005** and from **1025** to **4094**.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The **mistp-instance** *instances* keyword and optional variable are available in MISTP or MISTP/PVST+ mode only.

The *vlans* variable is available in PVST+ mode only.

You can enter a single VLAN or instance or a range of VLANs or instances separated by commas.

If you do not specify a VLAN or instance, all VLANs or instances are displayed.

This command is not available in MST mode.

Examples

This example shows how to display the UplinkFast feature settings for all VLANs:

```
Console> show spantree uplinkfast
Station update rate set to 15 packets/100ms.
uplinkfast all-protocols field set to off.
VLAN port list
-------------------------------------------------
1-20   1/1(fwd),1/2-1/5
21-50  1/9(fwd), 1/6-1/8, 1/10-1/12
51-100 2/1(fwd), 2/12
Console>
```

This example shows how to display the UplinkFast feature settings for a specific instance:

```
Console> show spantree uplinkfast mistp-instance 1
Station update rate set to 15 packets/100ms.
uplinkfast all-protocols field set to off.
Inst   port list
------------------------------------------------
1      4/1(fwd)
Console>
```

Related Commands clear spantree uplinkfast
set spantree uplinkfast

show startup-config

Use the **show startup-config** command to display the startup configuration file contained in NVRAM or specified by the CONFIG_FILE environment variable.

show startup-config

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

To view specific information within the **show startup-config** output, if you enter /*text* and press the **Return** key at the --More-- prompt, the display starts two lines above the line containing the *text* string. If the text string is not found, "Pattern Not Found" is displayed. You can also enter "**n**" at the --More-- prompt to search for the last entered *text* string.

Examples

This example shows how to display the switch startup configuration:

```
Console> (enable) show startup-config
This command shows non-default configurations only.
Use 'show config all' to show both default and non-default configurations.
..............

..................
..................

..

begin
!
# ***** NON-DEFAULT CONFIGURATION *****
!
!
#time: Mon Jun 11 2001, 06:56:10
!
#version 6.3(0.56)PAN
!

!
#!
```

```
#vtp
set vtp domain dan
set vtp mode transparent
set vlan 1 name default type ethernet mtu 1500 said 100001 state active
set vlan 1002 name fddi-default type fddi mtu 1500 said 101002 state active
set vlan 1004 name fddinet-default type fddinet mtu 1500 said 101004 state acti
e stp ieee
set vlan 1005 name trnet-default type trbrf mtu 1500 said 101005 state active s
p ibm
set vlan 2,10-11
set vlan 1003 name token-ring-default type trcrf mtu 1500 said 101003 state act
ve mode srb aremaxhop 7 stemaxhop 7 backupcrf off
!
#ip
set interface sc0 1 172.20.52.19/255.255.255.224 172.20.52.31

set ip route 0.0.0.0/0.0.0.0         172.20.52.1
!
#set boot command
set boot config-register 0x10f
set boot system flash bootflash:cat6000-sup2-d.6-3-0-56-PAN.bin
set boot system flash bootflash:cat6000-sup2-d.6-3-0-54-PAN.bin
set boot system flash bootflash:cat6000-sup2-d.6-3-0-46-PAN.bin
set boot system flash bootflash:cat6000-sup2-d.6-3-0-44-PAN.bin
set boot system flash bootflash:
!
#qos
set qos wred 1p2q2t tx queue 1 60:80 80:100
set qos wred 1p2q2t tx queue 2 60:80 80:100
set qos wred 1p3q1t tx queue 1 80:100
set qos wred 1p3q1t tx queue 2 80:100
set qos wred 1p3q1t tx queue 3 80:100
!
#mmls nonrpf
set mmls nonrpf timer 0
!
#security ACLs
clear security acl all
#pbf set
set pbf mac 00-01-64-61-39-c3
#adj set
set security acl adjacency ADJ2 10 00-00-00-00-00-0a 00-00-00-00-00-0b mtu 9600
#
commit security acl all
!
# default port status is enable
!
!
#module 1 empty
!
#module 2 : 2-port 1000BaseX Supervisor
!
#module 3 : 48-port 10/100BaseTX Ethernet
set vlan 10   3/1
set vlan 11   3/2
!
#module 4 empty
!
#module 5 : 0-port Switch Fabric Module
!
#module 6 empty
!
#module 7 empty
!
```

```
#module 8 empty
!
#module 9 empty
!
#module 15 empty
!
#module 16 empty
end
Console> (enable)
```

Related Commands **show running-config**

show summertime

Use the **show summertime** command to display the current status of the **summertime** feature.

show summertime

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the current status of the **summertime** feature:

```
Console> show summertime
Summertime is disabled and set to ''
Start : Thu Apr 13 2000, 04:30:00
End   : Mon Jan 21 2002, 05:30:00
Offset: 1440 minutes (1 day)
Recurring: no
Console>
```

Related Commands

set summertime

show system

Use the **show system** command to display system information.

show system

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The switching bus traffic values displayed apply to a single bus.

Examples

This example shows how to display system information:

```
Console> show system
PS1-Status PS2-Status
---------- ----------
none       ok

Fan-Status Temp-Alarm Sys-Status Uptime d,h:m:s Logout
---------- ---------- ---------- -------------- ---------
ok         off        ok         1,22:38:21     20 min

PS1-Type             PS2-Type
-------------------- --------------------
none                 WS-CAC-1300W
Modem   Baud  Traffic Peak Peak-Time
------- ----- ------- ---- -------------------------
disable  9600   0%      0% Mon Jan 10 2000, 15:23:31

PS1 Capacity: 1153.32 Watts (27.46 Amps @42V)

System Name              System Location          System Contact           CC
------------------------ ------------------------ ------------------------ ---
Information Systems      Closet 230 4/F           Xena ext. 24
Console>
```

This example shows how to display system information on a system configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2):

```
Console> show system
PS1-Status PS2-Status
---------- ----------
none       ok

Fan-Status Temp-Alarm Sys-Status Uptime d,h:m:s Logout
---------- ---------- ---------- -------------- ---------
ok         off        ok         0,00:02:52     20 min

PS1-Type             PS2-Type
-------------------- --------------------
none                 WS-CAC-1300W
Modem   Baud  Backplane-Traffic Peak Peak-Time
------- ----- ----------------- ---- -------------------------
disable  9600   0%                0% Thu Jul 27 2000, 14:03:27

PS1 Capacity:852.60 Watts (20.30 Amps @42V)

System Name              System Location          System Contact           CC
------------------------ ------------------------ ------------------------ ---


Fab Chan Input Output
-------- ----- ------
       0    0%     0%
       1    0%     0%
       2    0%     0%
       3    0%     0%
       4    0%     0%
       5    0%     0%
       6    0%     0%
       7    0%     0%
       8    0%     0%
       9    0%     0%
      10    0%     0%
      11    0%     0%
      12    0%     0%
      13    0%     0%
      14    0%     0%
      15    0%     0%
      16    0%     0%
      17    0%     0%
Console>
```

Table 2-89 describes the fields in the **show system** command output.

Table 2-89 show system Command Output Fields

Field	Description
PS1-Status	Status of power supply 1 (ok, fan failed, faulty, or none).
PS2-Status	Status of power supply 2 (ok, fan failed, faulty, or none).
Fan-Status	Status of the fan (ok, faulty, or other).
Temp-Alarm	Status of whether the temperature alarm is off or on.
Sys-Status	System status (ok or faulty). Corresponds to system LED status.

Table 2-89 show system Command Output Fields (continued)

Field	Description
Uptime d, h:m:s	Amount of time in days, hours, minutes, and seconds, that the system has been up and running.
Logout	Amount of time after which an idle session is disconnected.
PS1-Type	Part number of the power supply.
PS2-Type	Part number of the redundant power supply, if present.
Modem	Status of the modem status (enable or disable).
Baud	Baud rate to which the modem is set.
Traffic	Current traffic percentage.
Peak	Peak percentage of traffic on the backplane.
Peak-Time	Time stamp when peak percentage was recorded.
PS1 Capacity	Power supply 1 maximum capacity.
PS2 Capacity	Power supply 2 maximum capacity.
PS Configuration	Power supply configuration.
System Name	System name.
System Location	System location.
System Contact	System contact information.
CC	Country code string.
Backplane-Traffic	Current traffic percentage.
Fabric Chan	Number of the fabric channel.
Input	Percentage of fabric channel utilization for input.
Output	Percentage of fabric channel utilization for output.

Related Commands

set system baud
set system contact
set system location
set system modem
set system name

show system highavailability

Use the **show system highavailability** command to display the system high-availability configuration settings.

show system highavailability

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the system high-availability configuration settings:

```
Console> (enable) show system highavailability
Highavailability:disabled
Highavailability versioning:disabled
Highavailability Operational-status:OFF(high-availability-not-enabled)
Console> (enable)
```

Related Commands

set system highavailability
set system highavailability versioning

show system switchmode

Use the **show system switchmode** command to display the system switching mode setting.

show system switchmode

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the system switching mode:

```
Console> show system switchmode
Switching-mode allow:truncated
Switching-mode threshold:2
Console>
```

Related Commands

set system switchmode

show tacacs

Use the **show tacacs** command to display the TACACS+ protocol configuration.

show tacacs [**noalias**]

Syntax Description

noalias	(Optional) Keyword to force the display to show IP addresses, not IP aliases.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the TACACS+ protocol configuration:

```
Console> show tacacs
Login Authentication: Console Session   Telnet Session
---------------------  ----------------  ----------------
tacacs                 disabled          disabled
local                  enabled(primary)  enabled(primary)

Enable Authentication:Console Session   Telnet Session
---------------------- ----------------- ----------------
tacacs                 disabled          disabled
local                  enabled(primary)  enabled(primary)

Tacacs login attempts:3
Tacacs timeout:5 seconds
Tacacs direct request:disabled

Tacacs-Server                             Status
----------------------------------------   -------
171.69.193.114                            primary
Console>
```

Table 2-90 describes the fields in the **show tacacs** command output.

Table 2-90 show tacacs Command Output Fields

Field	Description
Login authentication	Display of the login authentication types.
Console Session	Status of whether the console session is enabled or disabled.
Telnet Session	Status of whether the Telnet session is enabled or disabled.
Enable Authentication	Display of the enable authentication types.
Tacacs login attempts	Number of failed login attempts allowed.

Table 2-90 show tacacs Command Output Fields (continued)

Field	Description
Tacacs timeout	Time in seconds to wait for a response from the TACACS+ server.
Tacacs direct request	Status of whether TACACS+ directed-request option is enabled or disabled.
Tacacs-Server	IP addresses or IP aliases of configured TACACS+ servers.
Status	Primary TACACS+ server.

Related Commands

set tacacs attempts
set tacacs directedrequest
set tacacs key
set tacacs server
set tacacs timeout

show tech-support

Use the **show tech-support** command to display system and configuration information you can provide to the Cisco Technical Assistance Center when reporting a problem.

show tech-support [{**module** *mod*} | {**port** *mod/port*}] [**vlan** *vlan*] [**mistp-instance** *instance*] [**mst** *instance*] [**memory**] [**config**]

Syntax Description

module *mod*	(Optional) Keyword and variable to specify the module number of the switch ports.
port *mod/port*	(Optional) Keyword and variable to specify the module and port number of the switch ports.
vlan *vlan*	(Optional) Keyword and variable to specify the VLAN; valid values are from **1** to **1001** and from **1025** to **4094**.
mistp-instance *instance*	(Optional) Keyword and variable to specify the MISTP instance number; valid values are from **1** to **16**.
mst *instance*	(Optional) Keyword and variable to specify the MST instance number; valid values are from **0** to **15**.
memory	(Optional) Keyword to display memory and processor state data.
config	(Optional) Keyword to display switch configuration.

Defaults

By default, this command displays the output for technical-support-related **show** commands. Use keywords to specify the type of information to be displayed. If you do not specify any parameters, the system displays all configuration, memory, module, port, instance, and VLAN data.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

Caution Avoid running multiple **show tech-support** commands on a switch or multiple switches on the network segment. Doing so may cause spanning tree instability.

The **show tech-support** command may time out if the configuration file output takes longer to display than the configured session timeout time. If this happens, enter a **set logout** *timeout* value of 0 to disable automatic disconnection of idle sessions or enter a longer *timeout* value.

The **show tech-support** command output is continuous; it does not display one screen at a time. To interrupt the output, press **Ctrl-C**.

If you specify the **config** keyword, the **show tech-support** command displays the output of these commands:

- **show config**
- **show flash**
- **show log**
- **show microcode**
- **show module**
- **show port**
- **show spantree active**
- **show spantree summary**
- **show system**
- **show test**
- **show trunk**
- **show version**
- **show vlan**

Note If MISTP is running, the output from the **show spantree mistp-instance active** and **show spantree summary mistp-instance** commands are displayed instead of the output from the **show spantree active** and **show spantree summary** commands.

Note If MST is running, the output from the **show spantree mst** and **show spantree summary mst** commands are displayed instead of the output from the **show spantree active** and **show spantree summary** commands.

If you specify the **memory** keyword, the **show tech-support** command displays the output of these commands:

- **ps**
- **ps -c**
- **show cam static**
- **show cam system**
- **show flash**
- **show memory buffers**
- **show microcode**
- **show module**
- **show proc**
- **show proc mem**
- **show proc cpu**
- **show system**
- **show spantree active**

- **show version**

If you specify a module, port, or VLAN number, the system displays general system information and information for the component you specified.

Related Commands See the commands listed in the "Usage Guidelines" section.

show test

Use the **show test** command to display the errors reported from the diagnostic tests and the diagnostic level.

show test [*mod*]

show test [**diaglevel**]

Syntax Description

mod	(Optional) Number of the module. If you do not specify a number, test statistics are given for the general system as well as for the supervisor engine.
diaglevel	(Optional) Keyword to display the diagnostic level.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

Only error conditions are displayed. If there are no errors, PASS is displayed in the Line Card Status field.

Examples

This example shows the error display for module 2:

```
Console> show test 2

Module 2 : 2-port 1000BaseX Supervisor
Network Management Processor (NMP) Status: (. = Pass, F = Fail, U = Unknown)
  ROM:  .   Flash-EEPROM: .   Ser-EEPROM: .   NVRAM: .   EOBC Comm: .

Line Card Status for Module 2 : PASS

Port Status :
  Ports 1  2
  -----------
        .  .

Line Card Diag Status for Module 2  (. = Pass, F = Fail, N = N/A)

 Module 2
  Cafe II Status :
        NewLearnTest:            .
        IndexLearnTest:          .
        DontForwardTest:         .
        DontLearnTest:           .
        ConditionalLearnTest:    .
        BadBpduTest:             .
        TrapTest:                .
```

```
 Loopback Status [Reported by Module 2] :
  Ports 1  2
  -----------
        .  .

 Channel Status :
  Ports 1  2
  -----------
        .  .
```

This example shows the error display for module 3:

```
Console> show test 3

Module 3 : 12-port 1000BaseX Ethernet

Line Card Status for Module 3 : PASS

Port Status :
  Ports 1  2  3  4  5  6  7  8  9  10 11 12
  ---------------------------------------
        .  .  .  .  .  .  .  .  .  .  .  .
Line Card Diag Status for Module 3  (. = Pass, F = Fail, N = N/A)
 Loopback Status [Reported by Module 3] :
  Ports 1  2  3  4  5  6  7  8  9  10 11 12
  ---------------------------------------
        .  .  .  .  .  .  .  .  .  .  .  .

 Channel Status :
  Ports 1  2  3  4  5  6  7  8  9  10 11 12
  ---------------------------------------
        .  .  .  .  .  .  .  .  .  .  .  .
```

This example shows the display when errors are reported by the LCP for module 3:

```
Console> show test 3

Module 3 : 12-port 1000BaseX Ethernet

Line Card Status for Module 3 : FAIL
 Error                                                      Device Number
 ---------------------------------------------------------  ------------------------
 Port asic error                                            1,2,5,12
 CPU error                                                  0
Line Card Diag Status for Module 3  (. = Pass, F = Fail, N = N/A)
 Loopback Status [Reported by Module 1] :
  Ports 1  2  3  4  5  6  7  8  9  10 11 12
  ---------------------------------------
        .  .  .  .  .  .  .  .  .  .  .  .

 Channel Status :
  Ports 1  2  3  4  5  6  7  8  9  10 11 12
  ---------------------------------------
        .  .  .  .  .  .  .  .  .  .  .  .
```

This example shows the display if you do not specify a module:

```
Console> show test

Environmental Status (. = Pass, F = Fail, U = Unknown, N = Not Present)
  PS1:.     PS2:N     PS1 Fan:.     PS2 Fan:N
  Chassis-Ser-EEPROM:.     Fan:.
  Clock(A/B):A         Clock A:.     Clock B:.
  VTT1:.    VTT2:.    VTT3:.

Module 1 :2-port 1000BaseX Supervisor
Network Management Processor (NMP) Status:(. = Pass, F = Fail, U =
Unknown)
  ROM: .   Flash-EEPROM:.   Ser-EEPROM:.   NVRAM:.   EOBC Comm:.

Line Card Status for Module 1 :PASS

Port Status :
  Ports 1  2
  -----------
        .  .

Line Card Diag Status for Module 1  (. = Pass, F = Fail, N = N/A)

Module 1
  Earl IV Status :
        NewLearnTest:           .
        IndexLearnTest:         .
        DontForwardTest:        .
        DontLearnTest:          .
        ConditionalLearnTest:   .
        BadBpduTest:            .
        TrapTest:               .
        MatchTest:              .
        SpanTest:               .
        CaptureTest:            .
Loopback Status [Reported by Module 1] :
  Ports 1  2
  -----------
        .  .

Channel Status :
  Ports 1  2
  -----------
        .  .
```

This example shows how to display diagnostic level status:

```
Console> (enable) show test diaglevel
Diagnostic mode at last bootup : minimal
Diagnostic mode at next reset  : bypass
Console> (enable)
```

Table 2-91 describes the possible fields in the **show test** command output. The fields shown depend on the module type queried.

Table 2-91 show test Command Output Fields

Field	Description
Environmental Status	Test results that apply to the general system environment.
PS (3.3V)	Test results for the 3.3V power supply.
PS (12V)	Test results for the 12V power supply.
PS (24V)	Test results for the 24V power supply.
PS1	Test results for power supply 1.
PS2	Test results for power supply 2.
Temperature	Test results for the temperature.
Fan	Test results for the fan.
Module #	Test results that apply to the module #. The module type is indicated as well.
Network Management Processor (NMP) Status	Test results that apply to the NMP on the supervisor engine module.
ROM	Test results for the ROM.
Flash-EEPROM	Test results for the Flash EEPROM.
Ser-EEPROM	Test results for the serial EEPROM.
NVRAM	Test results for the NVRAM.
EARL Status	Fields that display the EARL status information.
NewLearnTest	Test results for the NewLearn test (EARL).
IndexLearnTest	Test results for the IndexLearn test (EARL).
DontForwardTest	Test results for the DontForward test (EARL).
MonitorTest	Test results for the Monitor test (EARL).
DontLearn	Test results for the DontLearn test (EARL).
FlushPacket	Test results for the FlushPacket test (EARL).
ConditionalLearn	Test results for the ConditionalLearn test (EARL).
EarlLearnDiscard	Test results for the EarlLearnDiscard test (EARL).
EarlTrapTest	Test results for the EarlTrap test (EARL).
LCP Diag Status for Module 1	Test results for the specified module.
CPU	Test results for the CPU.
Sprom	Test results for the serial PROM.
Bootcsum	Test results for the Boot ROM checksum.
Archsum	Test results for the archive Flash checksum.
RAM	Test results for the RAM.
LTL	Test results for the local-target logic.
CBL	Test results for the color-blocking logic.

Table 2-91 show test Command Output Fields (continued)

Field	Description
DPRAM	Test results for the dual-port RAM.
SAMBA	Test results for the SAMBA chip.
Saints	Test results for the SAINT chips.
Pkt Bufs	Test results for the packet buffers.
Repeater	Test results for the repeater module.
FLASH	Test results for the Flash memory.
EOBC	Channel through which a module exchanges control messages with the other modules in the system.
Local Power	Status of the DC converter on a module that supplies power to the entire module except the power management block on the module.
Phoenix	Test results for the Phoenix.
TrafficMeter	Test results for the TrafficMeter.
UplinkSprom	Test results for the Uplink SPROM.
PhoenixSprom	Test results for the Phoenix SPROM.
MII Status	Test results for the MII ports.
SAINT/SAGE Status	Test results for the individual SAINT/SAGE chip.
Phoenix Port Status	Test results for the Phoenix ports.
Packet Buffer Status	Test results for the individual packet buffer.
Phoenix Packet Buffer Status	Test results for the Phoenix packet buffer.
Loopback Status	Test results for the loopback test.
Channel Status	Test results for the channel test.

Related Commands **set test diaglevel**

show time

Use the **show time** command to display the current time of day in the system clock.

show time

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the current time:

```
Console> show time
Wed Jan 12 2000, 14:18:52
Console>
```

The output shows the day of the week, month, day, year, hour, minutes, and seconds.

Related Commands

set time

show timezone

Use the **show timezone** command to display the current time zone and offset.

show timezone

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the current time zone and offset:

```
Console> show timezone
Timezone set to 'pst', offset from UTC is -8 hours
Console>
```

Related Commands

clear timezone
set timezone

show top

Use the **show top** command to start the TopN process.

show top [*N*] [*metric*] [**interval** *interval*] [*port_type*] [**background**]

Syntax Description

N	(Optional) Number of ports displayed; valid values are **1** to a maximum number of physical ports.
metric	(Optional) Port statistic to sort on; valid values are as follows: **util**—utilization **bytes**—in/out bytes **pkts**—in/out packets **bcst**—in/out broadcast packets **mcst**—in/out multicast packets **errors**—in errors **overflow**—buffer overflow
interval	(Optional) Keyword to specify duration of sample (in seconds).
interval	(Optional) Number of seconds for sample; valid values are **0** and from **10** to **999** seconds. If the value is 0, the N topmost ports by absolute counter values are displayed.
port_type	(Optional) Type of switch ports to use for report; valid values are as follows: **all**—All port types are used **eth**—All Ethernet port types are used **10e**—10-Mbps Ethernet ports types are used **fe**—Fast Ethernet port types are used **ge**—Gigabit Ethernet port types are used **10ge**—10-Gigabit Ethernet port types are used
background	(Optional) Keyword to specify the TopN report not to print to the screen when the task is done. Instead, a notification is sent out when the reports are ready.

Defaults

The defaults are as follows:

- Number of ports displayed is **20**.
- Port statistics to report on is **util**.
- Sample duration is **30** seconds.
- Switch port type is **all**.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

You can terminate TopN processes with the **background** option specified only by using the **clear top** [*report_num*] command.

TopN reports with the **background** option specified are not displayed on the screen unless you enter a **show top report** [*report_num*] command.

If you do not specify the **background** option, the output TopN results are dumped to the screen when the task is done, and the results are printed one time only and are not saved.

You can terminate TopN processes (without the **background** option) by pressing **Ctrl-C** in the same Telnet/console session, or by entering a **clear top** [*report_num*] command from a separate Telnet/console session. The prompt is not printed before the TopN report completely displays. Other commands are blocked until the report has displayed.

Examples

This example shows how to start the TopN process with the **background** option:

```
Console> show top 10 util interval 600 background
03/09/2000,14:05:38:MGMT-5: TopN report 2 started by telnet/172.20.22.7/.
Console>
03/09/2000,14:15:38:MGMT-5: TopN report 2 available.
```

This example shows how to start the TopN process without the **background** option:

```
Console> show top 10 util interval 600
Start Time:      03/19/2000,12:04:16
End Time:        03/19/2000,12:14:18
PortType:        all
Metric:          util
Port  Band- Uti Tx/Rx-bytes          Tx/Rx-pkts Tx/Rx-bcst Tx/Rx-mcst In-  Buf-
      width  %                                                      err  Ovflw
----- ----- --- -------------------- ---------- ---------- ---------- ---- -----
 1/1  100     0 65433                824         0          719        0     0
 5/48 10   0 3543              45      0        34       0    0
 5/47 10   0 45367           124      0        219      0    0
 5/46 10   0 23456           49       0        108      0    0
Console>
```

This example shows how to start the TopN process for a specific port type:

```
Console> show top 5 10e interval 0
Start Time:    03/09/2000,11:03:21
End Time:      03/09/2000,11:03:21
PortType:      10Mbps Ethernet
Metric:        util
Port  Band- Uti Bytes               Pkts       Bcst       Mcst       Error Over
      width  %  (Tx + Rx)           (Tx + Rx)  (Tx + Rx)  (Tx + Rx)  (Rx)  flow
----- ----- --- -------------------- ---------- ---------- ---------- ----- ----
2/1     10   0                    0          0          0          0     0    0
3/12  auto   0                    0          0          0          0     0    0
3/11  auto   0                    0          0          0          0     0    0
3/10  auto   0                    0          0          0          0     0    0
3/9   auto   0                    0          0          0          0     0    0
Console>
```

Related Commands

clear top
show top report

show top report

Use the **show top report** command to list all TopN processes and specific TopN reports.

show top report [*report_num*]

Syntax Description

report_num	(Optional) TopN report number for each process.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify *report_num*, this command lists all the active TopN processes and all the available TopN reports for the switch. Each process is associated with a unique report number. All TopN processes (both with and without a background option) are shown in the list.

An asterisk displayed after the pending status field indicates that it is not a background TopN and the results are not saved.

Examples

This example shows how to display all the active TopN processes and all the available TopN reports for the switch:

```
Console> show top report
Rpt  Start time          Int N   Metric      Status   Owner (type/machine/user)
---  ------------------- --- --- ----------  -------- ------------------------
  1  03/09/2000,11:34:00 60  20  Tx/Rx-Bytes done     telnet/172.20.22.7/
  2  03/09/2000,11:34:08 600 10  Util        done     telnet/172.34.39.6/
  4  03/09/2000,11:35:17 300 20  In-Errors   pending  Console//
  5  03/09/2000,11:34:26 60  20  In-Errors   pending* Console//
Console>
```

This example shows an attempt to display a TopN report 5 (shown in the first example) that is still in pending status:

```
Console> show top report 5
Rpt  Start time          Int N   Metric     Status   Owner (type/machine/user)
---  ------------------- --- --- ---------- -------- ------------------------
  5  03/09/2000,11:34:26 60  20  In-Errors   pending* Console//
Console>
```

This example shows how to display the available TopN report 2 (shown in the first example) for the switch:

```
Console> show top report 2
Start Time:     03/09/2000,11:34:00
End Time:       03/09/2000,11:34:33
PortType:       all
Metric:         util
Port  Band-  Uti Tx/Rx-bytes          Tx/Rx-pkts Tx/Rx-bcst Tx/Rx-mcst In-  Buf-
      width  %                                                        err  Ovflw
----- ----- --- -------------------- ---------- ---------- ---------- ---- -----
 /15  100   88  98765432109876543210 9876543210 98765      12345      123  321
 5/48 10    75  44532                5389       87         2          0    0
 5/47 10    67  5432                 398        87         2          0    0
 5/46 10    56  1432                 398        87         2          0    0
 5/45 10    54  432                  398        87         2          0    0
 5/44 10    48  3210                 65         10         10         15   5
 5/43 10    45  432                  5398       87         2          2    0
 5/42 10    37  5432                 398        87         2          0    0
 5/41 10    36  1432                 398        87         2          0    0
 5/40 10    14  2732                 398        87         2          0    0
Console>
```

Related Commands

clear top
show top

show traffic

Use the **show traffic** command to display traffic and peak information.

show traffic

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows the traffic and peak information display on a system configured with the Supervisor Engine 1 with Layer 3 Switching Engine WS-F6K-PFC:

```
Console> (enable) show traffic
Threshold: 100%
Traffic Peak Peak-Time
------- ---- -------------------------
  0%      0% Tue Apr 25 2000, 12:07:32
Console> (enable)
```

This example shows the traffic and peak information display on a system configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC II):

```
Console> (enable) show traffic
Threshold:100%
Backplane-Traffic Peak Peak-Time
----------------- ---- -------------------------
  0%                0% Thu Jul 27 2000, 14:03:27

Fab Chan Input Output
-------- ----- ------
       0    0%     0%
       1    0%     0%
       2    0%     0%
       3    0%     0%
       4    0%     0%
.
.
.
      14    0%     0%
      15    0%     0%
      16    0%     0%
      17    0%     0%
```

Related Commands

show system

show trunk

Use the **show trunk** command to display trunking information for the switch.

show trunk [*mod*[*/port*]] [**detail**] [**extended-range**]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.
detail	(Optional) Keyword to show detailed information about the specified trunk port.
extended-range	(Optional) Keyword to show trunking information for extended-range VLANs.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

Entering the **show trunk** command without specifying a module or port number displays only the actively trunking ports. To display the trunking configuration for a port that is not actively trunking, specify the module and port number of the port you want to display.The MSM port displays as a port that is always trunking, with allowed and active VLANs for each VLAN configured on the MSM.

Entering the **show trunk** command displays untagged traffic received over the dot1q trunk. For ISL trunks, packets are tagged on all VLANs (including native VLANs).

In the **show trunk detail** command output, the Peer-Port field displays either the module and port number of the peer connection or multiple or unknown. Multiple is displayed if connected to shared media, and unknown is displayed if DTP is not running on the other side.

If you enter the **show trunk** command on a trunk where a VTP domain mismatch exists, an asterisk is displayed after the trunk status and this message appears:

```
* - indicates vtp domain mismatch.
```

In the **show trunk** command output, the ports and VLANs listed in the spanning tree forward state and not pruned fields are the same regardless of whether or not VTP or GVRP is running.

Examples

This example shows how to display trunking information for the switch:

```
Console> (enable) show trunk
* - indicates vtp domain mismatch
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
15/1      nonegotiate  isl            trunking      1

Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------------
15/1      1-1005,1025-4094

Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------------
15/1

Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------------
15/1
Console> (enable)
```

This example shows how to display detailed information about the specified trunk port:

```
Console> (enable) show trunk 1/1 detail
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 1/1      auto         negotiate      not-trunking  1

Port      Peer-Port  Mode         Encapsulation  Status
--------  ---------  -----------  -------------  ------------
 1/1      2/3        auto         n-isl          not-trunking

Port      TrunkFramesTx         TrunkFramesRx         WrongEncap
--------  --------------------  --------------------  ----------
 1/1                       0                     0           0

Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------------
 1/1      1-1005

Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------------
 1/1      1

Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------------
 1/1
Console> (enable)
```

This example shows how to display detailed information about the specified trunk port that has a VTP domain mismatch:

```
Console> (enable) show trunk 3/1 detail
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 3/1      auto         negotiate      not-trunking*  1

Port      Peer-Port  Mode         Encapsulation  Status
--------  ---------  -----------  -------------  ------------
 3/1      2/3        auto         n-isl          not-trunking

Port      TrunkFramesTx         TrunkFramesRx         WrongEncap
--------  --------------------  --------------------  ----------
 3/1                       0                     0           0

Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------------
 3/1      1-1005

Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------------
 3/1      2

Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------------
 3/1
Console> (enable)
```

This example shows how to include information about extended-range VLANs:

```
Console> (enable) show trunk extended-range
Port       Status            Vlans allowed on trunk
--------   --------------    ------------------------------------
1/2         Trunking          1-1005, 2000-4094
2/2         Trunking          1-1005, 2100-4094
2/3         Non-Trunking      1-1005, 1025-2000, 3001-4094
.............
Console> (enable)
```

Table 2-92 describes the fields in the **show trunk** command outputs.

Table 2-92 show trunk Command Output Fields

Field	Description
Port	Module and port numbers.
Mode	Trunk administrative status of the port (on, off, auto, desirable, or nonegotiate).
Encapsulation	Trunking type configured by administration.
Status	Status of whether the port is trunking or nontrunking.
Native vlan	Number of the native VLAN for the trunk link (the VLAN for which untagged traffic can be transmitted and received over the dot1q trunk).
Vlans allowed on trunk	Range of VLANs allowed to go on the trunk (default is 1 to 1000).
Vlans allowed and active in management domain	Range of active VLANs within the allowed range.

Table 2-92 show trunk Command Output Fields (continued)

Field	Description
Vlans in spanning tree forwarding state and not pruned	Range of VLANs that actually go on the trunk with Spanning Tree Protocol forwarding state.
Peer-Port	Peer connection information (module and port number of peer connection, multiple, or unknown).
TrunkFramesTx	Number of ISL/802.1Q frames transmitted on a port.
TrunkFramesRx	Number of ISL/802.1Q frames received on a port.
WrongEncap	Number of frames with the wrong encapsulation received on a port.

Related Commands set trunk

show udld

Use the **show udld** command to display UDLD information.

show udld

show udld port [*mod*[*/port*]]

Syntax Description

port	Keyword to specify module and ports or just modules.
mod	(Optional) Number of the module for which UDLD information is displayed.
port	(Optional) Number of the port for which UDLD information is displayed.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to find out whether or not UDLD is enabled:

```
Console> show udld
UDLD      : enabled
Message Interval  :15 seconds
Console>
```

This example shows how to display UDLD information for a specific module and port:

```
Console> show udld port 2/1
UDLD              :enabled
Message Interval  :15 seconds
Port      Admin Status  Aggressive Mode  Link State
--------  ------------  ---------------  ----------------
 2/1      enabled       disabled         undertermined
Console>
```

This example shows how to display UDLD information for all ports on a specific module:

```
Console> (enable) show udld port 1
UDLD              :enabled
Message Interval  :15 seconds
Port      Admin Status  Aggressive Mode  Link State
--------  ------------  ---------------  ----------------
1/1       disabled      disabled         not applicable
1/2       disabled      enabled          not applicable
Console>
```

Table 2-93 describes the fields in the **show udld** command output.

Table 2-93 show udld Command Output Fields

Field	Description
UDLD	Status of whether UDLD is enabled or disabled.
Port	Module and port numbers.
Admin Status	Status of whether administration status is enabled or disabled.
Aggressive Mode	Status of whether aggressive mode is enabled or disabled.
Link State	Status of the link: undetermined (detection in progress, UDLD has been disabled on the neighbors), not applicable (UDLD is not supported on the port, UDLD has been disabled on the port, or the port is disabled), shutdown (unidirectional link has been detected and the port disabled), bidirectional (bidirectional link has been detected).

Related Commands

set udld
set udld aggressive-mode
set udld interval

show users

Use the **show users** command to show if the console port is active and to list all active Telnet sessions with the IP address or IP alias of the originating host.

show users [**noalias**]

Syntax Description

noalias	(Optional) Keyword to force the display to show IP addresses, not IP aliases.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the users of the active Telnet sessions:

```
Console> show users
Console Port
------------
Active

Telnet Sessions                          User
---------------------------------------  ------------------------------
172.16.10.75
172.16.10.75
171.31.1.203
Console>
```

Related Commands

disconnect

show version

Use the **show version** command to display software, hardware, and web interface version information.

show version [*mod*]

Syntax Description

mod	(Optional) Number of the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the software and hardware versions on systems configured with the Supervisor Engine 1 with Layer 3 Switching Engine WS-F6K-PFC:

```
Console> show version
WS-C6009 Software, Version NmpSW: 6.2(0.11)KEY
Copyright (c) 1995-2000 by Cisco Systems
NMP S/W compiled on Oct  5 2000, 01:18:33

System Bootstrap Version: 5.2(1)

Hardware Version: 1.0  Model: WS-C6009  Serial #: SCA030900JA

Mod Port Model               Serial #    Versions
--- ---- ------------------- ----------- -------------------------------------
1   2    WS-X6K-SUP1A-2GE    SAD03392376 Hw : 1.0
                                         Fw : 5.2(1)
                                         Fw1: 5.1(1)CSX
                                         Sw : 6.2(0.11)KEY
                                         Sw1: 6.2(0.11)KEY
         L3 Switching Engine SAD03365068 Hw: 1.0
3   2    WS-X6380-NAM        JAB0343055Y Hw : 0.201
                                         Fw : 4B4LZ0XA
                                         Fw1: 4.2(0.24)DAY68
                                         Sw : 1.1(0.20)
                                         Sw1: 6.2(0.11)KEY
5   48   WS-X6248-RJ-45      SAD03181291 Hw : 1.0
                                         Fw : 4.2(0.24)VAI78
                                         Sw : 6.2(0.11)KEY
15  1    WS-F6K-MSFC         SAD03366264 Hw : 1.2
                                         Fw : 12.1(2)E,
                                         Sw : 12.1(2)E,

       DRAM                    FLASH                   NVRAM
Module Total   Used    Free    Total   Used    Free    Total Used  Free
------ ------- ------- ------- ------- ------- ------- ----- ----- -----
1       65408K  45402K  20006K  16384K   8683K   7701K  512K  253K  259K
```

```
Uptime is 1 day, 19 hours, 54 minutes
Console> (enable)
```

This example shows how to display version information for a specific module:

```
Console> (enable) show version 3
Mod Port Model               Serial #    Versions
--- ---- ------------------- ----------- -------------------------------------
3   2    WS-X6380-NAM        JAB0343055Y Hw : 0.201
                                         Fw : 4B4LZ0XA
                                         Fw1: 4.2(0.24)DAY68
                                         Sw : 1.1(0.20)
                                         Sw1: 6.2(0.11)KEY

Console> (enable)
```

This example shows how to display the software and hardware versions on systems configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2):

```
Console> show version
WS-C6506 Software, Version NmpSW:6.1(0.142-Eng)
Copyright (c) 1995-2000 by Cisco Systems
NMP S/W compiled on Jul 27 2000, 18:36:52

System Bootstrap Version:6.1(194)

Hardware Version:2.0  Model:WS-C6506  Serial #:TBA04140397

Mod Port Model               Serial #    Versions
--- ---- ------------------- ----------- -------------------------------------
2   2    WS-X6K-SUP2-2GE     SAD041104M3 Hw :0.212
                                         Fw :6.1(194)
                                         Fw1:4.2(0.24)DAY84-Eng
                                         Sw :6.1(0.142-Eng)
                                         Sw1:6.1(0.142)
         L3 Switching Engine SAD04130E6X Hw :0.303
3   48   WS-X6248-RJ-45      SAD04140BZ1 Hw :1.2
                                         Fw :5.1(1)CSX
                                         Sw :6.1(0.142)
16  1    WS-F6K-MSFC2        SAD04040BP6 Hw :0.201
                                         Fw :12.1(0.11)EP1(0.43)
                                         Sw :12.1(0.11)EP1(0.43)

       DRAM                    FLASH                   NVRAM
Module Total   Used    Free    Total   Used    Free    Total Used  Free
------ ------- ------- ------- ------- ------- ------- ----- ----- -----
2      130944K  57916K  73028K  16384K  12003K   4381K  512K  257K  255K

Uptime is 0 day, 0 hour, 34 minutes
Console>
```

Table 2-94 describes the fields in the **show version** command output.

Table 2-94 show version Command Output Fields

Field	Description
NmpSW	Version number of the NMP software.
NMP S/W compiled on	Date and time that the NMP software was compiled.
System Bootstrap Version	System bootstrap version number.

Table 2-94 show version Command Output Fields (continued)

Field	Description
Web Interface Version	Web interface version number.
Hardware Version	Hardware version number.
Model	Switch model number.
Serial #	Switch serial number.
Module	Module number.
Port	Number of ports on the module.
Model	Model number of the module.
Serial #	Serial number of the module.
Versions	Hardware, software, and firmware versions of the module.
Hw	Hardware version of the module.
Fw	Version of the boot code (for switching modules) or bootstrap (for the supervisor engine).
Fw1	Version of the firmware boot code (on the supervisor engine).
Sw	Version of the firmware runtime installed (on the switching module) or the software version (on the supervisor engine).
Sw1	Version of the firmware runtime (on the supervisor engine).
DRAM Total	Total dynamic RAM installed on the module.
Used	Amount of DRAM in use.
Free	Amount of available DRAM.
FLASH Total	Total Flash memory installed on the module.
Used	Amount of Flash memory in use.
Free	Amount of available Flash memory.
NVRAM Total	Total NVRAM installed on the module.
Used	Amount of NVRAM in use.
Free	Amount of available NVRAM.
Uptime is	Number of uninterrupted days, hours, minutes, and seconds the system has been up and running.

show vlan

Use the **show vlan** command to display VLAN information.

show vlan [**trunk**]

show vlan *vlans* [**notrunk**]

show vlan mapping

show vlan *type*

Syntax Description

trunk	(Optional) Keyword to force the display to show information only on trunk ports.
vlans	Number or range of VLANs; valid values are from **1** to **1000** and from **1025** to **4094**.
notrunk	(Optional) Keyword to force the display to show information only on nontrunk ports.
mapping	Keyword to display VLAN mapping table information.
type	Type of the VLAN; valid values are **ethernet**, **fddi**, **fddinet**, **trbrf**, or **trcrf**.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

Each Ethernet switch port and Ethernet repeater group belong to only one VLAN. Trunk ports can be on multiple VLANs.

If you do not specify the VLAN number, all VLANs are displayed.

Examples

This example shows how to display information for all VLAN trunks:

```
Console> show vlan trunk
VLAN Name                             Status    IfIndex Mod/Ports, Vlans
---- -------------------------------- --------- ------- -----------------------
1    default                          active    5       2/1-2
                                                        6/4-8
10   VLAN0010                         active    18      6/1,6/3
11   VLAN0011                         active    19      6/2
20   VLAN0020                         active    20
21   VLAN0021                         active    21
```

```
30   VLAN0030                         active    22
31   VLAN0031                         active    23
1002 fddi-default                     active    6
1003 token-ring-default               active    9
1004 fddinet-default                  active    7
1005 trnet-default                    active    8       8

VLAN Type  SAID       MTU   Parent RingNo BrdgNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ ------ ---- -------- ------ ------
1    enet  100001     1500  -      -      -      -    -        0      0
10   enet  100010     1500  -      -      -      -    -        0      0
11   enet  100011     1500  -      -      -      -    -        0      0
20   enet  100020     1500  -      -      -      -    -        0      0
21   enet  100021     1500  -      -      -      -    -        0      0
30   enet  100030     1500  -      -      -      -    -        0      0
31   enet  100031     1500  -      -      -      -    -        0      0
1002 fddi  101002     1500  -      -      -      -    -        0      0
1003 trcrf 101003     1500  0      0x0    -      -    -        0      0
1004 fdnet 101004     1500  -      -      0x0    ieee -        0      0
1005 trbrf 101005     1500  -      -      0x0    ibm  -        0      0


VLAN Inst DynCreated  RSPAN
---- ---- ---------- --------
1    1    static     disabled
10        static     disabled
11        static     disabled
20        static     disabled
21        static     disabled
30        static     disabled
31        static     disabled
1002 -    static     disabled
1003 1    static     disabled
1004 2    static     disabled
1005 -    static     disabled


VLAN AREHops STEHops Backup CRF 1q VLAN
---- ------- ------- ---------- -------
1003 7       7       off


Primary Secondary Secondary-Type Ports
------- --------- -------------- ------------
10      20        isolated       6/1,6/3
11      21        isolated       6/2
30      -         -
-       31        isolated
```

This example shows how to display the VLAN mapping table information:

```
Console> show vlan mapping
802.1q vlan     ISL vlan        Effective
-----------------------------------------
3000            300             true
Console>
```

This example shows how to display information for a specific VLAN and type:

```
Console> show vlan 2 fddi
VLAN Name                             Status    IfIndex Mod/Ports, Vlans
---- -------------------------------- --------- ------- ------------------------
1002 fddi-default                     active    6


VLAN Type  SAID       MTU   Parent RingNo BrdgNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ ------ ---- -------- ------ ------
2    fddi  101002     1500  -      -      -      -    -        0      0

VLAN Inst DynCreated  RSPAN
---- ---- ---------- --------
2    -    static     disabled
Console>
```

This example shows how to display information for nontrunk ports only on a specific VLAN:

```
Console> (enable) show vlan 2 notrunk
VLAN Name                             Status    IfIndex Mod/Ports, Vlans
---- -------------------------------- --------- ------- ------------------------
2    VLAN0002                         active    60


VLAN Type  SAID       MTU   Parent RingNo BrdgNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ ------ ---- -------- ------ ------
2    enet  100002     1500  -      -      -      -    -        0      0


VLAN Inst DynCreated  RSPAN
---- ---- ---------- --------
2    -    static     disabled


VLAN AREHops STEHops Backup CRF 1q VLAN
---- ------- ------- ---------- -------

Console>
```

This example shows how to display extended-range VLANs:

```
Console> (enable) show vlan 4000
VLAN Name                             Status    IfIndex Mod/Ports, Vlans
---- -------------------------------- --------- ------- ------------------------
Unable to access VTP Vlan 4000 information.


VLAN Type  SAID       MTU   Parent RingNo BrdgNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ ------ ---- -------- ------ ------
Unable to access VTP Vlan 4000 information.


VLAN Inst DynCreated  RSPAN
---- ---- ---------- --------
Unable to access VTP Vlan 4000 information.


VLAN AREHops STEHops Backup CRF 1q VLAN
---- ------- ------- ---------- -------

Console> (enable)
```

Table 2-95 describes the fields in the **show vlan** command output.

Table 2-95 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).
IfIndex	Number of the ifIndex.
Mod/Ports, VLANs	Ports that belong to the VLAN.
Type	Media type of the VLAN.
SAID	Security association ID value for the VLAN.
MTU	Maximum transmission unit size for the VLAN.
Parent	Parent VLAN, if one exists.
RingNo	Ring number for the VLAN, if applicable.
BrdgNo	Bridge number for the VLAN, if applicable.
Stp	Spanning Tree Protocol type used on the VLAN.
BrdgMode	Bridging mode for this VLAN. Possible values are SRB and SRT; the default is SRB.
Inst	Instance number.
DynCreated	Status of whether the VLAN is created statically or dynamically.
RSPAN	Status of whether RSPAN is enabled or disabled.
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.
802.1Q Vlan	Number of the 802.1Q VLAN.
ISL Vlan	Number of the ISL VLAN.
Effective	Status of the VLAN. If the VLAN is active and its type is Ethernet, true is displayed; if not, false is displayed.
Primary	Number of the primary VLAN in a private VLAN.
Secondary	Number of the secondary VLAN in a private VLAN.
Secondary-Type	Type of secondary VLAN port. Possible values are isolated, community, or -.
Ports	Number of the module and ports associated to a specific private VLAN pair.

Related Commands

- set trunk
- set vlan
- show trunk

show vlan counters

Use the **show vlan counters** command to display counters for all VLANs or a range of VLANs:

show vlan counters [*vlans*]

Syntax Description

vlans	Number or range of VLANs; valid values are from **1** to **1005** and from **1025** to **4094**.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display counters for VLAN 1:

```
Console> show vlan counters 1

Vlan    :1
L2-Unicast-Pkts                              :3081
L3-In-Unicast-Pkts                           :0
L3-Out-Unicast-Pkts                          :0
L2-NonUnicast-Pkts + L3-In-NonUnicast-Pkts   :4021
L3-Out-NonUnicast-Pkts                       :0
L2-Unicast-Octets                            :238081
L3-In-Unicast-Octets                         :0
L3-Out-Unicast-Octets                        :0
L2-NonUnicast-Octets + L3-In-NonUnicast-Octets  :273025
L3-Out-NonUnicast-Octets                     :0
Console>
```

Table 2-96 describes the fields in the **show vlan counters** command output.

Table 2-96 show vlan counters Output Fields

Field	Description
L2-Unicast-Pkts	Layer 2 unicast packets forwarded per VLAN.
L3-In-Unicast-Pkts	Layer 3 unicast packets forwarded per input VLAN.
L3-Out-Unicast-Pkts	Layer 3 unicast packets forwarded per output VLAN.
L2-NonUnicast-Pkts + L3-In-NonUnicast-Pkts	Layer 2 nonunicast packets forwarded per VLAN and Layer 3 nonunicast packets forwarded per input VLAN.

Table 2-96 show vlan counters Output Fields (continued)

Field	Description
L3-Out-NonUnicast-Pkts	Layer 3 nonunicast packets forwarded per output VLAN.
L2-Unicast-Octets	Layer 2 unicast octets per VLAN.
L3-In-Unicast-Octets	Layer 3 unicast octets per input VLAN.
L3-Out-Unicast-Octets	Layer 3 unicast octets per output VLAN.
L2-NonUnicast-Octets + L3-In-NonUnicast-Octets	Layer 2 nonunicast octets per VLAN and Layer 3 nonunicast octets per input VLAN.
L3-Out-NonUnicast-Octets	Layer 3 nonunicast octets per output VLAN.

Related Commands **clear vlan counters**

show vmps

Use the **show vmps** command to display VMPS configuration information.

show vmps [**noalias**]

Syntax Description

noalias	(Optional) Keyword to force the display to show IP addresses, not IP aliases.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display VMPS configuration information:

```
Console> show vmps
VMPS Server Status:
-------------------
Management Domain:    (null)
State:                disabled
Operational Status:   inactive
TFTP Server:          default
TFTP File:            vmps-config-database.1
Fallback VLAN:        (null)
Secure Mode:          open
VMPS No Domain Req:   allow

VMPS Client Status:
---------------------
VMPS VQP Version:     1
Reconfirm Interval:   60 min
Server Retry Count:   3
VMPS domain server:

No dynamic ports configured.
Console>

No dynamic ports configured.
Console>
```

Table 2-97 describes the fields in the **show vmps** command output.

Table 2-97 show vmps Command Output Fields

Field	Description
VMPS Server Status	Status of VMPS server.
Management Domain	Management domain supported by this server.
State	Status on whether VMPS is enabled or disabled.
Operational Status	VMPS status (active, inactive, or downloading).
TFTP Server	IP address of the VMPS server.
TFTP File	VMPS configuration filename.
Fallback VLAN	VLAN assigned if a VLAN is not assigned to a MAC address in the database.
Secure Mode	Secure mode status (open or secure).
VMPS No Domain Req	Status on whether the server accepts requests from clients with no domain name.
VMPS Client Status	Status of the VMPS client.
VMPS VQP Version	Version of VMPS VQP.
VMPS domain server	VMPS domain server name.

Related Commands

download
set vmps server
set vmps state

show vmps mac

Use the **show vmps mac** command to display the MAC-address-to-VLAN mapping table.

show vmps mac [*mac_addr*]

Syntax Description

mac_addr	(Optional) MAC address that allows you to see mapping information.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a MAC address, the entire mapping table is displayed.

Examples

This example shows the entire MAC-address-to-VLAN mapping table:

```
Console> show vmps mac
MAC Address       VLAN Name Last Requestor  Port ID Last Accessed Last Response
----------------- --------- --------------- ------- ------------- -------------
00-00-c0-23-c8-34 Hardware  198.4.222.111   3/5     0, 01:25:30   Success
00-00-c0-25-c9-42 --NONE--  198.4.222.111   2/1     0, 05:20:00   Denied
Console>
```

Table 2-98 describes the fields in the **show vmps mac** command output.

Table 2-98 show vmps mac Command Output Fields

Field	Description
MAC Address	MAC address.
VLAN Name	VLAN name assigned to the MAC address.
Last Requestor	IP address of the client that last requested a VLAN assignment for this MAC address.
Port ID	Port ID in the last request.
Last Accessed	Time when the last request was processed for this MAC address.
Last Response	Response sent by the server for the last request.

Related Commands

show vmps

show vmps statistics

Use the **show vmps statistics** command to display the VMPS statistics.

show vmps statistics

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The statistics shown are based on the results of the **reconfirm vmps** command.

Examples

This example shows how to display the VMPS statistics:

```
Console> show vmps statistics
VMPS Statistics:
Last Enabled At:                  2,01:30:05
Config Requests:                  20
Invalid Requests:                 0
Status 'Error' Responses:         0
Status 'Deny' Responses:          5
MAC Address of Last Failed Request: 00-60-00-cc-01-02
Console>
```

Table 2-99 describes the fields in the **show vmps statistics** command output.

Table 2-99 show vmps statistics Command Output Fields

Field	Description
Last Enabled At	Time when the VMPS was enabled.
Config Requests	Number of configuration requests.
Invalid Requests	Number of invalid requests.
Status ‘Error’ Responses	Number of error responses.
Status ‘Deny’ Responses	Number of “Access Denied” and “Port Shutdown” responses.
MAC Address of Last Failed Request	MAC address of the last request for which the response was not successful.

Related Commands

clear vmps statistics

show vmps vlan

Use the **show vmps vlan** command to display all the MAC addresses assigned to a VLAN in the VMPS table.

show vmps vlan *vlan_name*

Syntax Description

vlan_name	Name or number of the VLAN.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display all MAC addresses assigned to the VLAN named Hardware:

```
Console> show vmps vlan Hardware

MAC Address       VLAN Name Last Requestor  Port ID Last Accessed Last Response
----------------- --------- --------------- ------- ------------- -------------
00-00-c0-23-c8-34 Hardware  198.4.222.111   3/5     0, 01:25:30   Success
Console>
```

Table 2-100 describes the fields in the **show vmps vlan** command output.

Table 2-100 show vmps vlan Command Output Fields

Field	Description
MAC Address	MAC address.
VLAN Name	VLAN name assigned to the MAC address.
Last Requestor	IP address of the client that last requested a VLAN assignment for this MAC address.
Port ID	Port ID in the last request.
Last Accessed	Time when the last request was processed for this MAC address.
Last Response	Response sent by the server for the last request.

Related Commands

show vmps

show vtp domain

Use the **show vtp domain** command to display VTP domain information.

show vtp domain

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display VTP domain information:

```
Console> show vtp domain
Domain Name                      Domain Index VTP Version Local Mode  Password
-------------------------------- ------------ ----------- ----------- ----------
                                 1            2           server      -

Vlan-count Max-vlan-storage Config Revision Notifications
---------- ---------------- --------------- -------------
15         1023             5               disabled

Last Updater    V2 Mode Pruning  PruneEligible on Vlans
--------------- ------- -------- -------------------------
172.20.44.30    enabled disabled 2-1000
Console>
```

Table 2-101 describes the fields in the **show vtp domain** command output.

Table 2-101 show vtp domain Command Output Fields

Field	Description
Domain Name	Name of the VTP domain.
Domain Index	Domain index number of the domain.
VTP Version	VTP version number.
Local Mode	VTP mode (server, client, or transparent).
Password	Password required or not.

Table 2-101 show vtp domain Command Output Fields (continued)

Field	Description
Vlan-count	Total number of VLANs in the domain.
Max-vlan-storage	Maximum number of VLANs allowed on the device.
Config Revision	VTP revision number used to exchange VLAN information.
Notifications	Notifications to SNMP (enabled or disabled).
Last Updater	IP address through which VTP was last updated.
V2 Mode	Status on whether VTP V2 mode is enabled or disabled.
Pruning	Status on whether VTP pruning is enabled or disabled.
PruneEligible on Vlans	VLANs on which pruning is allowed.

Related Commands

set vtp
show vtp statistics

show vtp statistics

Use the **show vtp statistics** command to display VTP statistics.

show vtp statistics

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display VTP statistics:

```
Console> show vtp statistics
VTP statistics:
summary advts received          0
subset  advts received          0
request advts received          0
summary advts transmitted       72
subset  advts transmitted       7
request advts transmitted       0
No of config revision errors    0
No of config digest errors      0

VTP pruning statistics:

Trunk    Join Transmitted Join Received Summary advts received from GVRP PDU
                                        non-pruning-capable device  Received
-------- ---------------- ------------- --------------------------- ----------
4/2       0               0             0                           0
```

Table 2-102 describes the fields in the **show vtp statistics** command output.

Table 2-102 show vtp statistics Command Output Fields

Field	Description
summary advts received	Total number of summary advts received.
subset advts received	Total number of subset advts received.
request advts received	Total number of request advts received.
summary advts transmitted	Total number of summary advts transmitted.
subset advts transmitted	Total number of subset advts transmitted.
request advts transmitted	Total number of request advts transmitted.

Table 2-102 show vtp statistics Command Output Fields (continued)

Field	Description
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 transmitted.
Join Received	Number of VTP-Pruning Joins received.
Summary advts received from nonpruning-capable device	Number of Summary advts received from nonpruning-capable devices.
GVRP PDU Received	Number of GVRP messages received on VTP trunks.

Related Commands

clear vtp statistics
set vtp

slip

Use the **slip** command to attach or detach SLIP for the console port.

slip {**attach** | **detach**}

Syntax Description

attach	Keyword to activate SLIP for the console port.
detach	Keyword to deactivate SLIP for the console port.

Defaults

The default is SLIP is not active (detached).

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can use the **slip** command from a console port session or a Telnet session.

Examples

This example shows how to enable SLIP for a console port during a console port session:

```
Console> (enable) slip attach
Console port now running SLIP.
<console port running SLIP>
```

This example shows how to disable SLIP for a console port during a Telnet session:

```
Console> (enable) slip detach
SLIP detached on Console port.
<console port back to RS-232 Console>
Console> (enable)
```

Related Commands

set interface

squeeze

Use the **squeeze** command to delete Flash files permanently.

squeeze [*m/*]*device***:**

Syntax Description

m/	(Optional) Module number of the supervisor engine containing the Flash device.
*device***:**	Device where the Flash resides.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

A colon (:) is required after the specified device.

Examples

These examples show how to use the **squeeze** command to delete the slot0 Flash files and then use the **show flash** command to confirm the deletion:

```
Console> squeeze slot0:
All deleted files will be removed, proceed (y/n) [n]?y
Squeeze operation may take a while, proceed (y/n) [n]?y
.....................................................
Console> show flash
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
  1 .. 2        f3a3e7c1  607f80   24  6061822 Mar 31 2000 15:42:49 cat6000-sup.
5-5-1.bin
7336000 bytes available (1052608 bytes used)
Console>
```

Related Commands

dir—switch
show flash
undelete

stack

Use the **stack** command to dump a stack trace of frames.

stack [**-d** | **-m**] [*num*]

Syntax Description

-d	(Optional) Keyword to dump the ROM monitor stack.
-m	(Optional) Keyword to specify addresses to dump.
num	(Optional) Number of frames.

Defaults

The default for *num* is five frames.

Command Types

ROM monitor command.

Command Modes

Normal.

Usage Guidelines

The frames are dumped from the kernel stack and the process stack (if one is available) of a booted image. Use the **frame** command to display an individual stack frame.

The minus sign (-) is required with the **-d** and **-m** options.

Examples

This example shows how to use the **stack** command to dump a stack trace of eight frames:

```
rommon 5 > stack 8
Kernel Level Stack Trace:
Initial SP = 0x60276a98, Initial PC = 0x60033054, RA = 0x6006d380
Frame 0 : FP= 0x60276a98, PC= 0x60033054,   0 bytes
Frame 1 : FP= 0x60276a98, PC= 0x6006d380,  24 bytes
Frame 2 : FP= 0x60276ab0, PC= 0x600e5218,  40 bytes
Frame 3 : FP= 0x60276ad8, PC= 0x600dcd48,  32 bytes
Frame 4 : FP= 0x60276af8, PC= 0x60033fdc,   0 bytes

Process Level Stack Trace:
Initial SP = 0x80007ce8, Initial PC = 0x600dfd38, RA = 0x600dfd20
Frame 0 : FP= 0x80007ce8, PC= 0x600dfd38,  24 bytes
Frame 1 : FP= 0x80007d00, PC= 0x6005b260,  32 bytes
Frame 2 : FP= 0x80007d20, PC= 0x6005c05c, 192 bytes
Frame 3 : FP= 0x80007de0, PC= 0x6005b54c,  24 bytes
Frame 4 : FP= 0x80007df8, PC= 0x600e82e0,  56 bytes
Frame 5 : FP= 0x80007e30, PC= 0x600e9484,  40 bytes
Frame 6 : FP= 0x80007e58, PC= 0x600e8b28,  24 bytes
Frame 7 : FP= 0x80007e70, PC= 0x600de224,  72 bytes
```

Related Commands

frame

switch

Use the **switch** command to switch the clock from the supervisor clock to the internal clock or from the active supervisor engine to the standby supervisor engine.

switch {**clock** | **supervisor**}

Syntax Description

clock	Keyword to switch the clock from the supervisor clock to the internal clock.
supervisor	Keyword to switch from the active supervisor engine to the standby supervisor engine.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to switch the clock:

```
Console> (enable) switch clock
This command will reset system and force a clock switch-over.
Do you want to continue (y/n) [n]?
Console> (enable)
```

This example shows how to switch to the standby supervisor engine:

```
Console> (enable) switch supervisor
This command will force a switch-over to the standby Supervisor module.
Do you want to continue (y/n) [n]?
Console> (enable)
```

switch console

Use the **switch console** command to switch the console connection physically to the MSFC on the active supervisor engine.

switch console [*mNo*]

Syntax Description

mNo	(Optional) Module number.

Defaults

The default is supervisor engine console.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported on Telnet sessions.

The **switch console** command allows you to change to the MSFC that shares the slot with the active supervisor engine. To use this command, it is necessary to have active and standby supervisor engine consoles. Otherwise, you cannot use the **switch console** command to switch to the console of the MSFC placed in the standby supervisor engine slot.

If you place the MSFC on a supervisor engine installed in slot 1, the MSFC is recognized as module 15. If you install the supervisor engine in slot 2, the MSFC is recognized as module 16. If the optional argument *mNo* is excluded, the console will switch to MSFC on the active supervisor engine.

To exit from the router CLI back to the switch CLI, press **Ctrl-C** three times at the Router> prompt.

Examples

This example shows how to switch the console connection to the MSFC on the active supervisor engine:

```
Console> (enable) switch console 15
Trying Router-15...
Connected to Router-15.
Type ^C^C^C to switch back...
```

switch fabric

Use the **switch fabric** command to reset the active Switch Fabric Module and allow the standby Switch Fabric Module to take over.

switch fabric [*mNo*]

Syntax Description

mNo	(Optional) Switch Fabric Module number.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported on Telnet sessions.

Examples

This example shows how to reset the active Switch Fabric Module:

```
Console> (enable) switch fabric
This command will force a switch-over to the standby fabric module.
Do you want to continue (y/n) [n]?
Console> (enable)
```

sync

Use the **sync** command to write the working in-core copy of environment variables and the aliases out to NVRAM so they are read on the next reset.

sync

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

ROM monitor command.

Command Modes

Normal.

Examples

This example shows how to use the **sync** command:

```
rommon 10 > sync
rommon 11 >
```

sysret

Use the **sysret** command to display the return information from the last booted system image.

sysret

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

ROM monitor command.

Command Modes

Normal.

Usage Guidelines

The stack dump information displayed has a maximum of eight frames.

Examples

This example shows how to use the **sysret** command to display the return information from the last booted system image:

```
rommon 8 > sysret
System Return Info:
count: 19,  reason: user break
pc:0x60043754,  error address: 0x0
Stack Trace:
FP: 0x80007e78, PC: 0x60043754
FP: 0x80007ed8, PC: 0x6001540c
FP: 0x80007ef8, PC: 0x600087f0
FP: 0x80007f18, PC: 0x80008734
```

telnet

Use the **telnet** command to start a Telnet connection to a remote host.

telnet *host* [*port*]

Syntax Description

host	Name or IP address of the remote host to which you want to connect.
port	(Optional) Specific port connection on the remote host.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to open and close a Telnet session with the host elvis:

```
Console> (enable) telnet elvis
Trying 192.122.174.11...
Connected to elvis.
Escape character is '^]'.

UNIX(r) System V Release 4.0 (elvis)

login: fred
Password:
Last login: Thu Oct 15 09:25:01 from forster.cisc.rum
Sun Microsystems Inc.   SunOS 5.4       Generic July 1994
You have new mail.
% logout

Console> (enable)
```

Related Commands

disconnect

test snmp trap

Use the **test snmp trap** command to send an SNMP trap message to the trap receivers.

test snmp trap *trap_num* [*specific_num*]

Syntax Description

trap_num	Number of the trap.
specific_num	(Optional) Number of a predefined trap.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to run trap 0:

```
Console> (enable) test snmp trap 0
SNMP trap message sent. (4)
Console> (enable)
```

Related Commands

set snmp trap
show snmp

traceroute

Use the **traceroute** command to display a hop-by-hop path through an IP network from the Catalyst 6000 family switch to a specific destination host.

traceroute [**-n**] [**-w** *wait_time*] [**-i** *initial_ttl*] [**-m** *max_ttl*] [**-p** *dest_port*] [**-q** *nqueries*] [**-t** *tos*] *host* [*data_size*]

Syntax Description

-n	(Optional) Option that prevents **traceroute** from performing a DNS lookup for each hop on the path. Only numerical IP addresses are printed.
-w *wait_time*	(Optional) Option used to specify the amount of time (in seconds) that **traceroute** will wait for an ICMP response message. The allowed range for *wait_time* is from **1** to **300** seconds.
-i *initial_ttl*	(Optional) Option that causes **traceroute** to send ICMP datagrams with a TTL value equal to *initial_ttl* instead of the default TTL of 1. This causes **traceroute** to skip processing for hosts that are less than *initial_ttl* hops away.
-m *max_ttl*	(Optional) Option used to specify the maximum TTL value for outgoing ICMP datagrams. The allowed range for *max_ttl* is from **1** to **255**.
-p *dest_port*	(Optional) Option used to specify the base UDP destination port number used in **traceroute** datagrams. This value is incremented each time a datagram is sent. The allowed range for *dest_port* is from **1** to **65535**. Use this option in the unlikely event that the destination host is listening to a port in the default traceroute port range.
-q *nqueries*	(Optional) Option used to specify the number of datagrams to send for each TTL value. The allowed range for *nqueries* is from **1** to **1000**.
-t *tos*	(Optional) Option used to specify the ToS to be set in the IP header of the outgoing datagrams. The allowed range for *tos* is from **0** to **255**.
host	IP alias or IP address in dot notation (*a.b.c.d*) of the destination host.
data_size	(Optional) Number of bytes, in addition to the default of 40 bytes, of the outgoing datagrams. The allowed range is from **0** to **1420**.

Defaults

Entering the **traceroute** *host* command without options sends three 40-byte ICMP datagrams with an initial TTL of 1, a maximum TTL of 30, a timeout period of 5 seconds, and a ToS specification of 0 to destination UDP port number 33434. For each host in the processed path, the initial TTL for each host and the destination UDP port number for each packet sent are incremented by one.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

To interrupt **traceroute** after the command has been issued, press **Ctrl-C**.

The **traceroute** command uses the TTL field in the IP header to cause routers and servers to generate specific return messages. Traceroute starts by sending a UDP datagram to the destination host with the TTL field set to 1. If a router finds a TTL value of 1 or 0, it drops the datagram and sends back an ICMP "time-exceeded" message to the sender. The traceroute facility determines the address of the first hop by examining the source address field of the ICMP time-exceeded message.

To identify the next hop, traceroute again sends a UDP packet but this time with a TTL value of 2. The first router decrements the TTL field by 1 and sends the datagram to the next router. The second router sees a TTL value of 1, discards the datagram, and returns the time-exceeded message to the source. This process continues until the TTL is incremented to a value large enough for the datagram to reach the destination host (or until the maximum TTL is reached).

To determine when a datagram has reached its destination, traceroute sets the UDP destination port in the datagram to a very large value that the destination host is unlikely to be using. When a host receives a datagram with an unrecognized port number, it sends an ICMP "port unreachable" error to the source. This message indicates to the traceroute facility that it has reached the destination.

Catalyst 6000 family switches can participate as the source or destination of the **traceroute** command. However, because they are Layer 2 devices, Catalyst 6000 family switches do not examine the TTL field in the IP header and do not decrement the TTL field or send ICMP time-exceeded messages. Thus, a Catalyst 6000 family switch does not appear as a hop in the **traceroute** command output.

Use the *tos* option to see if different types of service cause routes to change.

Examples

This example shows how to use the **traceroute** command to determine the path from the source to the destination host server10:

```
Console> (enable) traceroute server10
traceroute to server10.company.com (172.16.22.7), 30 hops max, 40 byte packets
 1  engineering-1.company.com (172.31.192.206)  2 ms  1 ms  1 ms
 2  engineering-2.company.com (172.31.196.204)  2 ms  3 ms  2 ms
 3  gateway_a.company.com (172.16.1.201)  6 ms  3 ms  3 ms
 4  server10.company.com (172.16.22.7)  3 ms  *  2 ms
Console> (enable)
```

Table 2-103 describes the fields in the **traceroute** command output.

Table 2-103 traceroute Command Output Fields

Field	Description
30 hops max, 40 byte packets	Maximum TTL value and the size of the ICMP datagrams being sent.
2 ms 1 ms 1 ms	Total time (in milliseconds) for each ICMP datagram to reach the router or host plus the time it took for the ICMP time-exceeded message to return to the host. An exclamation point following any of these values (for example, 20 ms !) indicates that the port-unreachable message returned by the destination had a TTL of 0 or 1. Typically, this occurs when the destination uses the TTL value from the arriving datagram as the TTL in its ICMP reply. The reply does not arrive at the source until the destination receives a traceroute datagram with a TTL equal to the number of hops between the source and destination.
3 ms * 2 ms	"*" indicates that the timeout period (default of 5 seconds) expired before an ICMP time-exceeded message was received for the datagram.

If **traceroute** receives an ICMP error message other than a time-exceeded or port-unreachable message, it prints one of the error codes shown in Table 2-104 instead of the round-trip time or an asterisk (*).

Table 2-104 traceroute Error Messages

ICMP Error Code	Meaning
!N	No route to host. The network is unreachable.
!H	No route to host. The host is unreachable.
!P	Connection refused. The protocol is unreachable.
!F	Fragmentation needed but do not fragment (DF) bit was set.
!S	Source route failed.
!A	Communication administratively prohibited.
?	Unknown error occurred.

Related Commands **ping**

unalias

Use the **unalias** command to remove the alias name and associated value from the alias list.

unalias *name*

Syntax Description

name	Name of the alias.

Defaults

This command has no default settings.

Command Types

ROM monitor command.

Command Modes

Normal.

Usage Guidelines

You must issue a **sync** command to save your change. Otherwise, the change is not saved and the **reset—ROM monitor** command removes your change.

Examples

This example shows how to use the **unalias** command to remove the **s** alias and then check to ensure it was removed:

```
rommon 5 > alias
r=repeat
h=history
?=help
b=boot
ls=dir
i=reset
k=stack
s=set
rommon 6 > unalias s
rommon 7 > alias
r=repeat
h=history
?=help
b=boot
ls=dir
i=reset
k=stack
rmmon 8 > s
monitor: command "s" not found
================================================================================
```

Related Commands

alias

undelete

Use the **undelete** command to recover a deleted file on a Flash memory device. The deleted file can be recovered using its index (because there could be multiple deleted files with the same name).

undelete *index* [[*m/*]*device***:**]

Syntax Description

index	Index number of the deleted file.
m/	(Optional) Module number of the supervisor engine containing the Flash device.
*device***:**	(Optional) Device where the Flash resides.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

A colon (:) is required after the specified device. See the **dir—switch** command to learn the index number of the file to be undeleted. A file cannot be undeleted if a valid file with the same name exists. You must delete the existing file before you can undelete the target file. A file can be deleted and undeleted up to 15 times. To delete all deleted files permanently on a device, use the **squeeze** command.

Examples

This example shows how to recover the deleted file with index 1 and use the **show flash** command to confirm:

```
Console> (enable) undelete 1 bootflash:
Console> (enable)
Console> (enable) show flash
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
  1 .. ffffffff fec05d7a  4b3a4c   25  4667849 Mar 03 2000 08:52:09 cat6000-sup.
5-3-4-CSX.bin
  2 .. ffffffff 4e5efc31  c0fadc   30  7716879 May 19 2000 06:50:55 cat6000-sup-
d.6-1-0.bin

3605796 bytes available (12384988 bytes used)
Console> (enable)
```

Related Commands

delete
show flash
squeeze

unset=varname

Use the **unset=***varname* command to remove a variable name from the variable list.

unset=*varname*

Syntax Description

varname	Name of the variable.

Defaults

This command has no default settings.

Command Types

ROM monitor command.

Command Modes

Normal.

Usage Guidelines

You must enter the **sync** command to save your change to NVRAM. Otherwise, the change is not saved and a **reset** removes your change.

Examples

This example shows how to use the **set** command to display the variable list, remove a variable name from the variable list, and then display the variable list to verify:

```
rommon 2 > set
PS1=rommon ! >
BOOT=
?=0
rommon 3 > unset=0
rommon 4 > set
PS1=rommon ! >
BOOT=
```

Related Commands

varname=

varname=

Use the *varname=* command to set the variable *VARNAME* to *varvalue*. Note that the syntax *varname=* sets the variable to a NULL string.

varname=value

Syntax Description

varname=	Name of the variable.
value	Any ROM monitor command.

Defaults

This command has no default settings.

Command Types

ROM monitor command.

Command Modes

Normal.

Usage Guidelines

Do not put a space before or after the equal (=) sign. If there are spaces, you must place the *value* in quotes. Spell out variable names in uppercase letters to make them conspicuous.

Examples

This example shows how to assign a variable name to a value:

```
rommon 1 > s=set
rommon 2 > s
PS1=rommon ! >
BOOT=
?=0
```

Related Commands

unset=varname

verify

Use the **verify** command to confirm the checksum of a file on a Flash device.

verify [[*m/*]*device***:**] *filename*

Syntax Description

m/	(Optional) Module number of the supervisor engine containing the Flash device.
device:	(Optional) Device where the Flash resides.
filename	Name of the configuration file.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

A colon (:) is required after the specified device.

Examples

This example shows how to use the **verify** command:

```
Console> verify cat6k_r47_1.cbi
.....................................................
File cat6k_r47_1.cbi verified OK.
```

wait

Use the **wait** command to cause the CLI to pause for a specified number of seconds before executing the next command. This command might be included in a configuration file.

wait *seconds*

Syntax Description

seconds	Number of seconds for the CLI to wait before executing the next command.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to pause the CLI for 5 seconds:

```
Console> wait 5


Console>
```

whichboot

Use the **whichboot** command to determine which file booted.

whichboot

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to use the **whichboot** command:

```
Console> whichboot
Boot image name is 'slot0:cat6000-sup.6-1-1.bin'.
Console>
```

write

Use the **write** command to upload the current configuration to the network or display the configuration information currently in running memory.

write network [**all**]

write terminal [**all**]

write {*host file*} [**all**] [**rcp**]

write memory

Syntax Description

network	Keyword to specify interactive prompting for the IP address or IP alias of the host and the filename to upload.
all	(Optional) Keyword to specify default and nondefault configuration settings.
terminal	Keyword to display the nondefault configuration file on the terminal.
host	IP address or IP alias of the host.
file	Name of the configuration file.
rcp	(Optional) Keyword to upload a software image to a host using rcp.
memory	Keyword that specifies to upload the current configuration to a specified location.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **write terminal** command is exactly the same as the **show config** command. The **write** *host file* command is a shorthand version of the **write network** command.

You cannot use the **write network** command to upload software to the ATM module.

With the **write network** command, the file must already exist on the host (use the UNIX **touch** *filename* command to create it).

Before you can enter the **write memory** command, you must enter text configuration mode. Enter text configuration mode by entering the **set config mode text** command.

Examples

This example shows how to upload the system5.cfg file to the mercury host:

```
Console> (enable) write network
IP address or name of host? mercury
Name of configuration file to write? system5.cfg
Upload configuration to system5.cfg on mercury (y/n) [y]? y
/
Done.  Finished Network Upload.  (9003 bytes)
Console> (enable)
```

This example shows how to upload the system5.cfg file to the mercury host:

```
Console> (enable) write mercury system5.cfg
Upload configuration to system5.cfg on mercury (y/n) [y]? y
/
Done.  Finished Network Upload.  (9003 bytes)
Console> (enable)
```

This example shows how to display the configuration file on the terminal (partial display):

```
Console> (enable) write terminal
!
....
............


............

............



begin
!
#version 4.2(0.24)VAI58 set password $1$FMFQ$HfZR5DUszVHIRhrz4h6V70
set enablepass $1$FMFQ$HfZR5DUszVHIRhrz4h6V70
set prompt Console>
set length 24 default
set logout 20
set banner motd ^C^C
!
#system
set system baud  9600
set system modem disable
set system name
set system location
set system contact
!
#power
set power redundancy enable
!
#snmp
set snmp community read-only      public
set snmp community read-write     private
set snmp community read-write-all secret
set snmp rmon disable
set snmp trap disable module

...
<<<< output truncated >>>>
```

This example shows how to upload the running system configuration to a prespecified location:

```
Console> (enable) write memory
Upload configuration to bootflash:switch.cfg
7165844 bytes available on device bootflash, proceed (y/n) [n]? y
Console> (enable)
```

Related Commands

copy
set config mode
show config

write tech-support

Use the **write tech-support** command to generate a report that contains status information about your switch or upload the output of the command to a TFTP server, where you can send it to the Technical Assistance Center.

write tech-support *host file* [**module** *mod*] [**vlan** *vlan*] [**mistp-instance** *instance*] [**mst** *instance*] [**memory**] [**config**]

write tech-support *host file* [**port** *mod/port*] [**vlan** *vlan*] [**mistp-instanc**e *instance*] [**mst** *instance*] [**memory**] [**config**]

Syntax Description

host	IP address or IP alias of the host.
file	Name of the configuration file.
module *mod*	(Optional) Keyword and variable to specify the module number.
vlan *vlan*	(Optional) Keyword and variable to specify the VLAN; valid values are from **1** to **1001** and from **1025** to **4094**.
port *mod/port*	(Optional) Keyword and variables to specify the module and port on the module.
mistp-instance *instance*	(Optional) Keyword and variable to specify the MISTP instance number; valid values are from **1** to **16**.
mst *instance*	(Optional) Keyword and variable to specify the MST instance number; valid values are from **0** to **15**.
memory	(Optional) Keyword to specify memory and processor state information.
config	(Optional) Keyword to specify switch configuration information.

Defaults

By default, this command displays the output for technical-support-related **show** commands. Use keywords to specify the type of information to be displayed. If you do not specify any parameters, the system displays all configuration, memory, module, port, instance, and VLAN data.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Caution Avoid running multiple **write tech-support** commands on a switch or multiple switches on the network segment. Doing so may cause spanning tree instability.

Note If you press **Ctrl-C** while the **write tech-support** is outputting, the output file to the TFTP server might be incomplete.

Note If you are uploading the information to a file, make sure the file already exists in the TFTP server, the file has appropriate permissions, and the network connections are good before you issue the **write tech-support** command.

If you specify the **config** keyword, the **write tech-support** command displays the output of these commands:

- **show config**
- **show flash**
- **show log**
- **show microcode**
- **show module**
- **show port**
- **show spantree active**
- **show spantree summary**
- **show system**
- **show test**
- **show trunk**
- **show version**
- **show vlan**

Note If MISTP is running, the output from the **show spantree mistp-instance active** and **show spantree summary mistp-instance** commands are displayed instead of the output from the **show spantree active** and **show spantree summary** commands.

Note If MST is running, the output from the **show spantree mst** and **show spantree summary mst** commands are displayed instead of the output from the **show spantree active** and **show spantree summary** commands.

If you specify the **memory** keyword, the **write tech-support** command displays the output of these commands:

- **ps**
- **ps -c**
- **show cam static**
- **show cam system**
- **show flash**
- **show memory buffers**

- **show microcode**
- **show module**
- **show proc**
- **show proc mem**
- **show proc cpu**
- **show system**
- **show spantree active**
- **show version**

If you specify a module, port, or VLAN number, the system displays general system information and information for the component you specified.

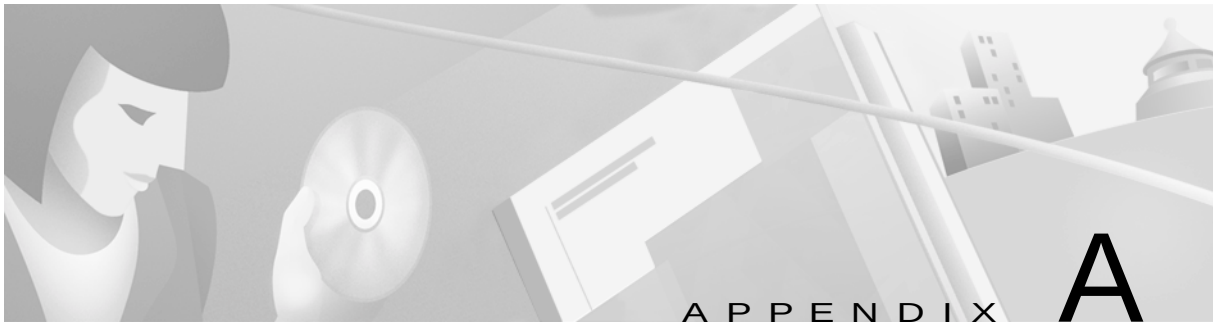
Examples

This example shows how to upload the technical report:

```
Console> (enable) write tech-support 172.20.32.10 tech.txt
Upload tech-report to tech.txt on 172.20.32.10 (y/n) [n]? y
/
Finished network upload.  (67784 bytes)
Console> (enable)
```

Related Commands

show tech-support
See the commands listed in the “Usage Guidelines” section.



Acronyms

Table A-1 defines the acronyms used in this publication.

Table A-1 List of Acronyms

Acronym	Expansion
AAA	authentication, authorization, accounting
AAL	ATM adaptation layer
ACE	access control entry
ACL	access control list
AFI	authority and format identifier
AMP	active monitor present
APaRT	automated packet recognition and translation
ARP	Address Resolution Protocol
ASLB	accelerated server load balancing
ATM	Asynchronous Transfer Mode
BDD	binary decision diagram
BES	bursty errored seconds
BIA	bottom interface adapter
BPDU	bridge protocol data unit
BRF	bridge relay function
BUS	broadcast and unknown server
CAM	content-addressable memory
CDP	Cisco Discovery Protocol
CEF	Cisco Express Forwarding
CLI	command-line interface
COPS	Common Open Policy Service
COPS-DS	COPS Differentiated Services
COPS-PR	COPS for Provisioning
CoS	class of service
CPLD	Complex Programmable Logic Device

Table A-1 List of Acronyms (continued)

Acronym	Expansion
CRC	cyclic redundancy check
CRF	concentrator relay function
DCC	Data Country Code
DEC	Digital Equipment Corporation
DFI	Domain-Specific Part Format Identifier
DHCP	Dynamic Host Configuration Protocol
DISL	Dynamic Inter-Switch Link
DMP	data movement processor
DNS	Domain Name System
DRAM	dynamic RAM
DRiP	Dual Ring Protocol
DSAP	destination service access point
DSBM	Designated Subnet Bandwidth Manager
DSCP	differentiated services code point
DSP	digital signal processing or processor
DTP	Dynamic Trunking Protocol
EAP	Extensible Authentication Protocol
EARL	Enhanced Address Recognition Logic
EEPROM	electrically erasable programmable read-only memory
ESI	end-system identifier
FCS	frame check sequence
FEFI	far end fault indication
GARP	General Attribute Registration Protocol
GBIC	Gigabit Interface Converter
GMRP	GARP Multicast Registration Protocol
GSR	Gigabit Switch Router
GVRP	GARP VLAN Registration Protocol
HCRMON	High Capacity RMON
HDD	hard disk drive driver
HTTP	HyperText Transfer Protocol
ICD	International Code Designator
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IDP	initial domain part
IDSM	Intrusion Detection System Module
IGMP	Internet Group Management Protocol

Table A-1 List of Acronyms (continued)

Acronym	Expansion
ILMI	Integrated Local Management Interface
IP	Internet Protocol
IPC	interprocessor communication
IPX	Internetwork Packet Exchange
ISL	Inter-Switch Link
ISO	International Organization of Standardization
KDC	Key Distribution Center
LACP	Link Aggregation Control Protocol
LAN	local-area network
LANE	LAN Emulation
LCP	Link Control Protocol
LCV	line code violation seconds
LD	LocalDirector
LEC	LAN Emulation Client
LECS	LAN Emulation Configuration Server
LEM	link error monitor
LER	link error rate
LES	LAN Emulation Server or line errored seconds
LLC	logical link control
MAC	Media Access Control
MDG	multiple default gateway
MIB	Management Information Base
MII	media-independent interface
MISTP	Multi-Instance Spanning Tree Protocol
MLS	Multilayer Switching
MMLS	Multicast Multilayer Switching
MOP	Maintenance Operation Protocol
MOTD	message-of-the-day
MSFC	Multilayer Switch Feature Card
MSM	Multilayer Switch Module
MST	Multiple Spanning Tree
MTP	Media Termination Point
MTU	maximum transmission unit
MVAP	multiple VLAN access port
NAM	Network Analysis Module
NDE	NetFlow Data Export

Table A-1 List of Acronyms (continued)

Acronym	Expansion
NMP	Network Management Processor
NSAP	network service access point
NTP	Network Time Protocol
NVRAM	nonvolatile RAM
OAM	Operation, Administration, and Maintenance
ODM	order dependent merge
OSI	Open System Interconnection
OUI	organizational unique identifier
PAE	port access entity
PAgP	Port Aggregation Protocol
PBF	policy-based forwarding
PCM	pulse code modulation
PCR	peak cell rate
PDP	policy decision point
PDU	protocol data unit
PEP	policy enforcement point
PFC	Policy Feature Card
PHY	physical sublayer
PIB	policy information base
PPP	Point-to-Point Protocol
PRID	policy rule identifiers
PROM	programmable read-only memory
PVID	port VLAN identifier
PVST+	per VLAN spanning tree
QoS	quality of service
RADIUS	Remote Access Dial-In User Service
RAM	random-access memory
rcp	Remote Copy Protocol
RGMP	Router-Ports Group Management Protocol
RIF	Routing Information Field
RMON	Remote Monitoring
ROM	read-only memory
RSA	Rivest, Shamir, and Adleman (a public-key cryptographic system)
RSPAN	remote SPAN
RST	reset
RSVP	ReSerVation Protocol

Table A-1 List of Acronyms (continued)

Acronym	Expansion
SAID	Security Association Identifier
SAP	service access point
SIMM	single in-line memory module
SLCP	Supervisor Line-Card Processor
SLIP	Serial Line Internet Protocol
SMP	standby monitor present
SMT	station management
SNAP	Subnetwork Access Protocol
SNMP	Simple Network Management Protocol
SPAN	Switched Port Analyzer
SRB	source-route bridging
SRT	source-route transparent bridging
SSH	Secure Shell
STE	Spanning Tree Explorer
STP	Spanning Tree Protocol
SVC	switched virtual circuit
TAC	Technical Assistance Center (Cisco)
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
TGT	ticket granting ticket
TOS	type of service
TLV	type-length-value
TrBRF	Token Ring Bridge Relay Function
TrCRF	Token Ring Concentrator Relay Function
TTL	time to live
UART	Universal Asynchronous Receiver/Transmitter
UDLD	UniDirectional Link Detection
UDLP	UniDirectional Link Protocol
UDP	User Datagram Protocol
UNI	User-Network Interface
UTC	Coordinated Universal Time
VACL	VLAN access control list
VCC	virtual channel connection (in ATM technology), virtual channel circuit
VCI	virtual circuit identifier
VCR	virtual configuration register

Table A-1 List of Acronyms (continued)

Acronym	Expansion
VIP	virtual IP address
VLAN	virtual LAN
VMPS	VLAN Membership Policy Server
VoIP	Voice over IP
VTP	VLAN Trunk Protocol
VID	VLAN ID
VVID	voice VLAN identifier
WRED	weighted random early detection
WRR	weighted round-robin

Symbols

?
- command completion 1-11
- displaying matches 1-11

? (help)
- switch CLI 1-9

? (question mark) 1-11

Numerics

3DES key
- defining 2-288
- removing 2-36

802.1x
- configuring on a port 2-353
- displaying authenticator information 2-787
- displaying backend authenticator information 2-787
- displaying system capabilities and protocol version 2-640
- displaying timer values 2-640
- initializing on port 2-353
- manually initiating reauthentication 2-353
- setting number of frame 2-234
- setting retransmission authentication time 2-234
- setting retransmission time 2-234
- specifying port control type
  - auto 2-353
  - force-authorized 2-353
  - force-unauthorized 2-353

A

access control
- entries
  - See QoS ACL
  - See security ACL
  - See VACL
- lists
  - See QoS ACL
  - See security ACL
  - See VACL

accounting
- RADIUS
  - disabling accounting of normal login session 2-183
  - disabling accounting of system events 2-186
  - enabling accounting of normal login session 2-183
  - enabling accounting of system events 2-186
- TACACS+
  - disabling accounting of normal login session 2-183
  - disabling accounting of system events 2-186
  - disabling suppression of accounting information 2-185
  - enabling accounting of normal login session 2-183
  - enabling accounting of outbound connection events 2-182
  - enabling accounting of system events 2-186
  - enabling command event accounting 2-181
  - enabling suppression of accounting information 2-185
  - setting accounting update frequency 2-188

acronyms, list of A-1

adding to permit list 2-274

Address Recognition Protocol
- See ARP table

adjacency
displaying PBF information 2-755
aggregate rate limit
clearing 2-78
alias
clearing 2-6
defining 2-191
displaying 2-592
ARP
displaying table 2-593
ARP table
adding entries 2-192
adding IP address-to-MAC address mapping entries 2-192
clearing entries 2-7
displaying table 2-593
setting aging time 2-192
setting ARP agingtime 2-192
ASLB
configuring ASLB information 2-291
displaying ASLB information 2-686
removing ASLB MLS entries 2-38
removing MAC address entries 2-38
saving ASLB configuration to NVRAM 2-129
authentication
specifying lockout time 2-194
specifying number of connection attempts 2-194
specifying primary login method 2-196
specifying primary method 2-194
authorization
TACACS+
disabling 2-198
disabling authorization of privileged mode events 2-200
enabling 2-198
enabling authorization of EXEC mode events 2-202
enabling authorization of normal login mode 2-202
enabling authorization of privileged mode events 2-200
enabling authorization of session events 2-202
auto-config
synchronizing 2-210, 2-215
auto-config file
configuring 2-210, 2-215
auxiliary VLAN
configuring ports 2-340
displaying port status 2-766

B

banner
clearing MOTD banner 2-8
configuring LCD banner 2-204
configuring message-of-the-day banner 2-205
displaying LCD banner 2-596
displaying MOTD banner 2-596
baud rate
setting console port baud rate 2-543
bidirectional VLAN
grouping ports 2-574
mapping 2-574
setting type 2-574
boot
clearing NAM boot string 2-10
configuring auto-config file 2-210
displaying NAM boot string 2-598
setting IDS environment 2-213
setting NAM environment 2-213
synchronizing auto-config file 2-215
boot configuration register
setting 2-207
BOOT environment variable
clearing 2-11
displaying contents 2-597
setting 2-216
boot file
determining which file booted 2-1013
bootflash
displaying information 2-652

broadcast/multicast suppression
disabling 2-61
displaying information 2-768
broadcast suppression
setting 2-342

C

CAM table
adding entries 2-217
clearing entries 2-12
configuring traffic filtering 2-217
deleting entry 2-12
displaying 2-598
aging time information 2-601
number of entries 2-602
router MAC-VLAN entries 2-603
displaying entries 2-599
setting
aging time 2-217
setting agingtime 2-217
capture port list
removing entry 2-86
CDP
configuring hold time 2-219
configuring message interval 2-219
disabling 2-219
displaying information 2-604
displaying port CDP state and message interval 2-773
enabling 2-219
selecting version 2-219
setting device-ID TLV format 2-219
CEF
clearing adjacencies associated with CEF entries 2-49
clearing statistics summary 2-46
displaying
adjacencies 2-715
entry information 2-715
interfaces 2-703
MAC addresses 2-705
displaying CEF table information 2-707
channel
displaying channel port utilization based on MAC counters 2-619
displaying EtherChannel group status information 2-612
displaying port or module information 2-775
display MAC information 2-617
setting channel path cost 2-221
setting channel VLAN cost 2-223
channel hash
displaying hash information 2-616
clear 2-46
CLI
exiting session 2-167
pausing CLI for specified number of seconds 2-1012
ROM monitor CLI
accessing 1-13
operating 1-13
switch CLI
accessing 1-1
command aliases 1-8
command help 1-9
command-line processing 1-3
command modes 1-3
console port 1-2
ending session 2-167
IP addresses 1-11
IP aliases 1-11
IPX addresses 1-11
MAC addresses 1-11
operating 1-3
Telnet 1-2
clock
displaying summertime status 2-945
setting 2-334, 2-541
closing active console 2-148
command accounting

clearing command log entries 2-41
displaying command log entries 2-692
command alias
clearing 2-6
displaying 2-2
removing alias name and value 2-1007
setting 2-2
command completion
keyword lookup
keyword lookup 1-11
partial keyword lookup 1-11
self-repeat function 1-11
command history, switch CLI 1-8
command history buffer
displaying contents 2-158
command history log
clearing 2-41
displaying 2-692
command-line editing 1-4
completing partial command 1-4
controlling capitalization 1-7
deleting entries 1-6
designating keystroke as command entry 1-7
editing wrapping command lines 1-5
moving around 1-4
pasting in buffer entries 1-5
redisplaying current command line 1-7
scrolling down line or screen 1-6
scrolling to specified text 1-6
transposing mistyped characters 1-7
command-line-interface
See CLI
command logging
clearing log entry table 2-41
displaying command log entries 2-692
command modes
switch CLI, normal mode 1-3
switch CLI, privileged mode 1-3
top-level, normal mode 1-9
top-level, privileged mode 1-9
command shorthands
clearing 2-6
displaying 2-2
setting 2-2
common access policy
displaying group name 2-892
displaying user collection 2-892
Common Open Policy Service
See COPS
community and associated access types
defining 2-469
completing command or keyword
using Tab key 1-12
configuration file
clearing contents 2-9
deleting 2-142
specifying file to use 2-206
configuration register setting
displaying 2-597
setting 2-11
configuration register utility
configuring 2-132
configuring 2-204
console
setting port baud rate 2-543
switching console connection physically to MSFC on active supervisor engine 2-998
contact person 2-544
content-addressable memory
See CAM table
context-sensitive help 1-10
COPS
clearing domain name 2-17
clearing port roles 2-63
clearing roles 2-17
clearing servers 2-17
configuring
domain name 2-227

policy server names 2-227
creating port roles 2-347
displaying COPS information 2-781
displaying COPS information for RSVP 2-628
displaying policy tree information 2-628
displaying ports assigned to each role 2-628
setting
connection retry interval 2-227
memory usage 2-227
core dump file
disabling 2-545
enabling 2-545
naming 2-547
CoS-to-DSCP map
clearing 2-71
counters
clearing
MAC counters 2-19
port counters 2-19
displaying hardware counters 2-631
displaying port counters 2-783
restoring
MAC counters 2-177
port counters 2-177
country code
setting 2-548
CPU
displaying information 2-823
crossbar fabric
selecting fallback action 2-549

D

data export
disabling globally 2-431
disabling on aggregate policer 2-432
disabling on port 2-435
enabling globally 2-431
enabling on aggregate policer 2-432
enabling on port 2-435
setting export destination 2-433
daylight saving time
displaying clock 2-945
setting clock 2-334, 2-541
default IP gateway
specifying 2-277
default port status
displaying 2-638
setting 2-231
deleted file
recovering 2-1008
designating ports 1-10
designating VLANs 1-10
DHCP
configuring interfaces 2-264
diagnostic tests
errors 2-956
level 2-956
module 2-956
setting level 2-563
system 2-956
disabling module 2-321
disabling UDLD information display 2-570
displaying 2-596
displaying configuration information 2-1014
displaying current cd command setting 2-166
displaying Layer 2 path 2-159
displaying setting 2-800
displaying system information 2-946
DNS
defining IP address of DNS server 2-270
defining server as primary 2-270
disabling 2-268
enabling 2-268
setting default DNS domain name 2-269
documentation
audience xxiii
conventions xxiv

organization xxiii
domain naming service
See DNS
dot1q
configuring tagging mode 2-232
configuring tunneling mode 2-351
displaying tagging mode status 2-639
displaying tunneling mode status 2-786
dot1x
clearing configuration 2-21
configuring on a port 2-353
configuring on a system 2-234
disabling authentication 2-234
disabling reauthentication 2-234
displaying authenticator information 2-787
displaying backend authenticator information 2-787
displaying system capabilities and protocol version 2-640
displaying timer values 2-640
enabling authentication 2-234
enabling reauthentication 2-234
initializing on port 2-353
manually initiating reauthentication 2-353
setting idle time 2-234
setting number of frame retransmissions 2-234
setting retransmission authentication time 2-234
setting retransmission time 2-234
specifying port control type
auto 2-353
force-authorized 2-353
force-unauthorized 2-353
downloading
forcing module to accept SCP download 2-169
rcp configuration file 2-130
downloading image 2-149
DSCP-to-CoS map
clearing 2-72
dump log
clearing 2-40
displaying 2-690
DVLAN
displaying statistics 2-641

E

EAP
configuring dot1x 2-234
enabling module 2-321
entries
See security ACL
environment
displaying inline power status 2-642
displaying system status information 2-642
error detection
disabling 2-240
displaying settings 2-647
enabling 2-240
inband 2-240
memory 2-240
port counter 2-240
error disable
configuring timeout for ports in errdisable state 2-238
displaying configuration and status information 2-646
EtherChannel
displaying channel information 2-607
exiting CLI session 2-167
Extensible Authentication Protocol
See EAP

F

fabric
resetting active module and allowing standby fabric to take over 2-999
fabric channel
displaying utilization 2-946
Flash configuration file
appending 2-210

overwriting 2-210
recurrence 2-210
Flash device
confirming checksum of file on Flash device 2-1011
recovering deleted file 2-1008
setting system default Flash device 2-5
Flash files
deleting 2-995
Flash memory
copying image from host 2-149
displaying contents of file saved to Flash memory 2-651
Flash PC card
displaying information 2-652
formatting 2-154
flow control
configuring ports 2-357
port guidelines 2-357

G

GARP
displaying timer values 2-655
setting timers 2-244
GARP Multicast Registration Protocol
See GMRP
GARP VLAN Registration Protocol
See GVRP
General Attribute Registration Protocol
See GARP, setting timers
GMRP
clearing statistics information 2-22
disabling Forward All 2-246
disabling in all VLANs 2-245
disabling on specified ports 2-360
displaying configuration information 2-656
displaying statistical information 2-657
displaying timer values 2-658
enabling Forward All 2-246
enabling in all VLANs 2-245
enabling on specified ports 2-360
setting registration type 2-247
setting timers 2-248
GVRP
clearing statistics information 2-23
disabling dynamic VLAN creation 2-252
disabling globally 2-250
disabling on port 2-250
disabling on specified ports 2-361
displaying configuration information 2-659
displaying statistics 2-661
enabling dynamic VLAN creation 2-252
enabling globally 2-250
enabling on port 2-250
enabling on specified ports 2-361
setting administrative control 2-253
setting timers 2-255
VLAN declaration 2-251

H

hardware
displaying versions 2-975
high availability
disabling 2-550
disabling versioning 2-551
displaying configuration settings 2-949
enabling 2-550
enabling versioning 2-551
hop-by-hop path
displaying 2-1004

I

ICMP
disabling redirect messages 2-276
disabling unreachable messages 2-279

enabling redirect messages 2-276
enabling unreachable messages 2-279
sending echo-request packets
configuring ping 2-163
identifying
2-544
idle session timeout
setting 2-307
idling
timeout 2-307
ifIndex
displaying information 2-663
IGMP
clearing statistics information 2-24
disabling fastleave processing 2-258
disabling rate limiting 2-261
disabling snooping 2-257
displaying IGMP mode 2-664
displaying IGMP rate limit information 2-665
displaying IGMP statistics 2-666
enabling fastleave processing 2-258
enabling rate limiting 2-261
enabling snooping 2-257
setting IGMP snooping mode 2-259
setting rate limit for snooping packets 2-261
in-band interfaces
configuring 2-264
inline power
displaying status 2-642
instances
assigning port path cost 2-526
displaying BPDU skew status 2-912
displaying information summary 2-937
displaying instance information 2-921
displaying list of MAC addresses, instance numbers, and timers 2-914
displaying MAC address of root switch 2-914
displaying only blocked ports 2-911
displaying path cost 2-928
displaying portfast information 2-927
displaying spanning tree guard information 2-917
displaying statistics information 2-930
displaying time remaining before VLAN joins instance 2-914
resetting port instance priority 2-103
restoring default path cost 2-101
setting bridge forward delay 2-501
setting bridge hello time 2-507
setting bridge maximum aging time 2-510
setting bridge priority 2-534
setting port priority 2-528
setting primary root 2-536
setting secondary root 2-536
Internet Group Management Protocol
See IGMP
Internet Protocol
See IP addresses
IP addresses 2-274
clearing 2-28
designating in CLI 1-11
IP alias
adding 2-267
clearing 2-25
designating in CLI 1-11
displaying 2-671
IP DNS
clearing default DNS domain name 2-26
defining IP address of DNS server 2-270
displaying DNS domain name 2-672
displaying DNS name server 2-672
displaying DNS name servers 2-671
removing DNS server 2-27
IP fragmentation
disabling 2-271
enabling 2-271
IP permit list
clearing IP address and mask 2-28
disabling 2-274

displaying 2-675
enabling 2-274
IP precedence-to-DSCP map
clearing 2-73
IP routing table
adding IP addresses 2-277
adding IP aliases 2-277
deleting entries 2-30
displaying entries 2-677
specifying default IP gateway 2-277
IP subnet address
format guidelines 2-48, 2-56
IPX address
format guidelines 2-47, 2-56
IPX addresses, designating in CLI 1-11

J

jumbo frames
displaying settings 2-792
enabling 2-365
port guidelines 2-365
setting MTU size
contacting TAC 2-365

K

Kerberos
authenticating users 2-282
clearing Kerberos realm to DNS domain name map 2-34
clearing secret key 2-36
clearing specific Kerberos entry 2-35
defining secret key 2-288
deleting all Kerberos credentials 2-33
disabling credentials forwarding 2-32
disabling mandatory authentication 2-31
displaying configuration information 2-679
displaying credentials information 2-679
enabling authentication 2-194
enabling mandatory authentication 2-280
enabling primary authentication login method 2-196
entering SRVTAB file from command line 2-285
forwarding user credentials 2-281
mapping realm to DNS domain name 2-283
providing file containing secret key 2-287
specifying which KDC to use 2-284

L

l2trace 2-159
Layer 2
displaying path 2-159
LCD banner 2-204, 2-596
LCP
configuring error action 2-290
displaying error action 2-685
LDA
configuring ASLB information 2-291
Link Control Protocol
See LCP
link negotiation protocol 2-800
disabling on port 2-371
listing Flash memory device files 2-145
local command accounting
clearing command log entries 2-41
displaying command log entries 2-692
local director
See LDA
local engine ID
displaying 2-891
login password
changing 2-337
limiting console login attempts 2-196
limiting Telnet login attempts 2-196
loop guard
disabling 2-505
displaying information 2-917

enabling 2-505

M

MAC addresses
clearing from secure MAC addresses list 2-66
clearing MAC address from list of secure MAC addresses 2-66
designating in CLI 1-11
displaying port MAC counter information 2-796
MAC counters
displaying 2-696
MDG
disabling
enabling
membership assignments
reconfirming 2-168
memory allocation
displaying information 2-823
message log
setting size of syslog table 2-297
message-of-the-day banner
clearing 2-8
messages
disabling logging 2-303
disabling logging on Telnet sessions 2-304
enabling logging 2-303
enabling logging on Telnet sessions 2-304
sending logging messages to current login session 2-303
sending logging messages to new Telnet sessions 2-304
MIB
displaying CISCO-IMAGE-MIB information 2-668
MIB view entry
removing 2-98
microcode
displaying version 2-699
microflow policing rule
clearing 2-78
MISTP
clearing statistical information 2-110
disabling 2-497
displaying information summary 2-937
displaying instance information 2-921
displaying spanning tree guard information 2-917
displaying statistics information 2-930
enabling 2-499
mapping VLANs 2-574
setting 2-512
setting bridge forward delay 2-501
setting bridge hello time 2-507
setting bridge maximum aging time 2-510
setting bridge priority 2-534
setting primary root 2-536
setting secondary root 2-536
MISTP-PVST
setting 2-512
MLS
adding protocols to protocol statistics list 2-318
clearing excluded protocol port 2-50, 2-51
clearing IP MLS cache entries 2-47, 2-55
clearing IP MLS statistics 2-47, 2-53
clearing IPX MLS cache entries 2-47, 2-55
clearing IPX MLS statistics 2-47, 2-53
clearing MLS statistics from MSFC 2-51
configuring NDE flow 2-314
disabling NDE 2-314
displaying configuration of packet checking 2-732
displaying excluded protocols 2-721
displaying IP MLS state information 2-709
displaying IP MLS statistics information 2-729
displaying IP multicast MLS information 2-722
displaying IPX MLS statistics information 2-729
displaying IPX state information 2-709
displaying MLS Layer 3 packet information 2-700, 2-728
displaying MLS state information 2-709
displaying MLS statistics information 2-729
displaying MSFC MLS statistics information 2-729

displaying NDE information 2-700, 2-727, 2-728
displaying router processor MLS information 2-709
displaying summaries from ACL routing information 2-702
enabling NDE 2-314
enabling or disabling packet checking 2-319
resetting NDE filter 2-52
setting MLS aging time 2-308
setting MLS fast aging time 2-308
specifying collector 2-314
specifying minimum flow mask used 2-312
specifying NDE version 2-314
specifying protocol port to be excluded from being shortcut 2-311
module configuration
displaying nondefault configuration 2-620
module error log
clearing 2-40
modules
disabling 2-321
displaying contents of system module initiation log 2-736
displaying status and information 2-733
enabling 2-321
naming 2-323
shutting down NAM and IDS modules 2-325
turning off power to module 2-324
turning on power to module 2-324
monitoring traffic
configuring threshold 2-566
MSFC
disabling auto state 2-326
disabling line protocol state 2-326
displaying auto state status 2-738
displaying interface state status 2-738
enabling auto state 2-326
enabling line protocol state 2-326
MSM
accessing MSM 2-179
disabling line protocol state 2-328
displaying current status of line protocol state determination of MSM 2-739
displaying line protocol state 2-739
enabling line protocol state 2-328
MST
clearing mapping of VLANs 2-99
detecting legacy bridges and boundary ports 2-518
displaying MST configuration 2-925
displaying MST information 2-923
displaying system and configuration information when in MST mode 2-953
setting mapping of VLANs 2-519
setting maximum number of hops 2-517
setting MST region information 2-514
setting port link type 2-516
multicast
displaying multicast protocols status 2-743
multicast group
displaying configuration 2-740
displaying total count of multicast addresses (groups) in VLAN 2-742
multicast router
clearing port list 2-58
configuring port 2-329
displaying ports with IGMP-capable routers 2-744
multicast suppression
setting 2-342
Multi-Instance Spanning Tree Protocol
See MISTP
Multilayer Switch Module
See MSM A-3
multiple default gateway
See MDG

N

NAM
clearing NAM boot string 2-10
clearing password 2-57

disabling SNMP extended RMON support 2-471
displaying NAM boot string 2-598
enabling SNMP extended RMON support 2-471
setting boot environment 2-213
shutting down module 2-325
naming module 2-323
naming system 2-555
NDE
displaying information
displaying MLS Layer 3 packet information 2-728
NDE filter
resetting 2-52
NetFlow Data Export
See NDE
network interfaces
displaying information 2-669
network statistics
displaying 2-746
normal mode
returning from privileged mode 2-147
NTP
configuring IP address of NTP server 2-333
configuring server authentication key 2-333
configuring time-adjustment factor 2-331
disabling switch as NTP client 2-332
displaying current NTP status 2-753
enabling switch as NTP client 2-332
removing servers from table 2-59
removing server table entry 2-59
returning to default time zone 2-60
setting daylight saving time 2-334
NVRAM
clearing stored module configuration information 2-14
clearing stored system configuration information 2-14
committing ACEs 2-127
committing ASLB configuration 2-129
copying ACL configuration from DRAM back into NVRAM 2-225

O

oops
recovering deleted file 2-1008
opening module session 2-179

P

PAgP
clearing statistical information 2-13
configuring ports 2-344
displaying port or module information 2-775
displaying port statistics 2-607
partial keyword lookup 1-11
password
changing 2-337
setting password for privileged level 2-237
PBF
clearing MAC address 2-61
configuring MAC address 2-338
displaying adjacency information 2-755
displaying adjacency map 2-755
displaying statistical information 2-755
peak
displaying information 2-967
per port utilization
disabling statistics data export 2-432
displaying packet and byte rates 2-696
enabling statistics data export 2-432
policed-dscp table
resetting to default 2-77
policy-based forwarding
See PBF
Port Aggregation Protocol
See PAgP
port mapping
clearing 2-16
port name
setting 2-370

port roles
clearing 2-63
creating 2-347
ports
clearing MAC addresses from secure MAC addresses list 2-66
clearing port configuration for optimizing host connection 2-64
configuring access port on Cisco IP phone 2-381
configuring dot1q tunnel mode 2-351
configuring duplex mode 2-355
configuring flow control
pause frames 2-357
configuring port security 2-383
configuring speed 2-385
creating EtherChannel port bundles 2-344
defining EtherChannel administrative groups 2-344
disabling 2-350
disabling link negotiation protocol 2-371
disabling protocol membership 2-372
disabling standard SNMP link trap 2-387
displaying flow control information 2-789
displaying information 2-811
displaying link negotiation protocol setting 2-800
displaying MAC counter information 2-796
displaying port capabilities 2-769
displaying port security configuration 2-805
displaying port status 2-758
displaying protocol filters configured on EtherChannel ports 2-801
displaying status 2-808
displaying trap status information 2-810
enabling 2-356
enabling jumbo frames 2-365
enabling link negotiation protocol 2-371
enabling or disabling GMRP 2-360
enabling or disabling GVRP on specified ports 2-361
enabling protocol membership 2-372
enabling standard SNMP link trap 2-387
optimizing port configuration for host connection 2-363
returning to factory-set default for all packets arriving through untrusted port 2-65
setting default value for packets arriving through untrusted port 2-376
setting inline power mode 2-364
setting interface interpretation as physical port 2-374
setting interface interpretation as VLAN 2-374
setting port name 2-370
setting trusted state 2-379
setting VLAN membership assignment 2-368
specifying frame-distribution method for switch 2-344
port security
clearing MAC addresses from secure MAC addresses list 2-66
configuring 2-383
port speed
configuring 2-385
powering module 2-324
power redundancy
turning redundancy between power supplies on or off 2-390
power supplies
turning redundancy on or off 2-390
private VLAN
See PVLAN
privileged level
setting password 2-237
privileged mode
activating 2-153
returning to normal mode 2-147
process utilization
displaying information 2-823
prompt
changing 2-391
protocol filtering
activating 2-392
deactivating 2-392
displaying status 2-827

protocol membership
disabling on port 2-372
enabling on port 2-372
pruning
disabling VTP pruning 2-585
enabling VTP pruning 2-585
specifying pruning-eligible VTP domain VLANs 2-587
PVLAN
bidirectional VLAN 2-574
binding port to private VLAN 2-393
binding VLAN to primary VLAN 2-393
clearing configuration 2-16
deleting mapping 2-67
determining PVLAN capability 2-830
displaying configuration 2-828
displaying mapping configuration 2-832
grouping ports 2-574
mapping 2-574
mapping VLAN to primary VLAN 2-395
setting type 2-574
PVST
setting 2-512

Q

QoS
clearing changes from edit buffer 2-178
clearing CoS-to-DSCP map 2-71
clearing DSCP-to-CoS map 2-72
clearing IP precedence-to-DSCP map 2-73
clearing mac-cos values 2-74
clearing map values 2-75
clearing statistic counters 2-80
configuring access port 2-381
configuring transmit and drop thresholds 2-414
deleting CoS assigned to MAC addresses 2-70
displaying counters 2-856
displaying current information for MAC address and VLAN pair 2-846
displaying information for MAC address and VLAN pair 2-846
displaying information on per-port basis 2-802
displaying map information 2-848
displaying policy source information 2-853
displaying related information 2-841
displaying status 2-859
enabling microflow policing
disabling microflow policing 2-412
mapping CoS values 2-420
mapping IP precedence-to-DSCP 2-417
returning to factory-set CoS defaults 2-65
returning to factory-set default for all packets arriving through untrusted port 2-65
returning to factory-set default values 2-70
returning to factory-set threshold, queue, and threshold map defaults 2-70
setting CoS values 2-419
setting default for all packets arriving through untrusted port 2-376
setting DSCP-to-CoS map 2-416
setting packet buffer memory 2-430, 2-436
setting packet value 2-376
setting policy source to COPS-PR 2-426
setting policy source to local NVRAM 2-426
setting port policy source 2-374
setting port policy source to COPS 2-377
setting port policy source to local NVRAM 2-377
setting switch to participate in DSBM election 2-382
setting trusted state 2-379
specifying CoS-to-DSCP map 2-413
specifying interface as port or VLAN 2-374
specifying WRED threshold 2-437
specifying WRR weights 2-439
turning off 2-397
turning on 2-397
turning QoS on 2-397
turning QoS RSVP off 2-428
turning QoS RSVP on 2-428
QoS access lists

attaching to interface 2-410
defining IP access lists 2-400
defining IPX access lists 2-405
defining MAC access lists 2-408
QoS ACL
attaching ACL to interface 2-410
clearing changes to ACL edit buffer 2-178
committing to NVRAM 2-127
defining default action 2-398
defining IP access lists 2-400
defining IPX access lists 2-405
defining MAC access lists 2-408
detaching ACL 2-68
displaying ACL management information 2-839
displaying ACL names in edit buffer 2-834
displaying committed access lists 2-627
displaying configuration file location 2-620
displaying configured ACE information 2-835
displaying default action 2-835
displaying QoS ACL mapping 2-837
displaying running configuration 2-868
displaying runtime ACE information 2-835
displaying VLAN-bridged packet-policing status 2-840
removing ACE 2-68
removing default actions 2-68
removing IP ACE default actions 2-68
removing IPX ACE default actions 2-68
removing MAC-layer ACE default actions 2-68
QoS policing
clearing aggregate rate limit 2-78
clearing microflow policing rule 2-78
displaying policing information 2-851
mapping in-profile DSCPs changes when policed 2-423
resetting policed-dscp table to default 2-77
specifying microflow policing rule 2-424

R

RADIUS
clearing RADIUS server table 2-81
clearing RADIUS shared key 2-81
disabling accounting of normal login session 2-183
disabling accounting of system events 2-186
displaying RADIUS configuration parameters 2-860
enabling accounting of normal login session 2-183
enabling accounting of system events 2-186
enabling authentication 2-194
enabling primary authentication login method 2-196
setting deadtime 2-441
setting encryption and authentication 2-442
setting time between retransmissions 2-446
setting up RADIUS server 2-444
specifying RADIUS retransmit times 2-443
rcp
clearing information 2-82
copying software image to Flash memory 2-149
deleting user name 2-122
downloading configuration file 2-130
downloading Flash image or switch configuration 2-136
setting username 2-447
uploading Flash image or switch configuration 2-136
Remote Copy Protocol
See rcp
remote span
creating remote SPAN sessions 2-449
displaying remote SPAN configuration 2-866
repeating command 2-170
reset
cancel 2-173
displaying scheduled reset information 2-863
module 2-173
schedule reset 2-173
switch 2-173
restoring factory-set defaults 2-112
return information
displaying information from last booted system image 2-1001

RGMP
clearing statistics information 2-83
disabling 2-448
displaying multicast group count 2-864
displaying multicast groups 2-864
displaying statistics information 2-865
enabling 2-448
ROM monitor
booting up external process 2-4
configuring configuration register utility 2-132
displaying command aliases 2-2
displaying context of loaded image 2-134
displaying main memory information 2-162
displaying NVRAM information 2-162
displaying packet memory information 2-162
displaying supported DRAM configurations 2-162
displaying variable names 2-180
dumping stack trace of frames 2-996
listing available device IDs 2-143
listing device files 2-144
performing soft reset 2-172
repeating command 2-170
setting ROM monitor variable name values 2-180
soft reset 2-172
writing environment variables and aliases to NVRAM 2-1000
ROM monitor CLI
accessing 1-13
operating 1-13
root guard
disabling 2-505
displaying information 2-917
enabling 2-505
RSA
configuring key pair 2-229
displaying key pair information 2-637
generating key pair 2-229
removing key pairs 2-20
RSVP
displaying COPS information 2-628
displaying port information 2-804
displaying switch information 2-854
setting switch to participate in DSBM election 2-382
turning QoS RSVP off 2-428

S

security access lists
See security ACL
security ACL
clearing changes from edit buffer 2-178
committing to NVRAM 2-127
configuring adjacency 2-452
configuring log table 2-462
creating new entry in non-IP VACL 2-463
creating new entry in non-IPX VACL 2-463
creating new entry in standard IPX VACL 2-459
displaying ACL management information 2-839
displaying capture port list entries 2-874
displaying committed ACL 2-871
displaying configuration file location 2-620
displaying current configuration 2-871
displaying mapped ACL 2-878
displaying running configuration 2-868
displaying VACL log information 2-875
displaying VACL management information 2-879
mapping existing VACL-to-VLAN 2-465
removing all ACEs from VACL 2-84
removing entry from capture port list 2-86
removing VACL from editbuffer 2-84
removing VACL-to-VLAN mapping 2-88
setting ports to capture traffic 2-453
setting security ACL
security ACL log table
clearing 2-87
self-repeat function 1-11
server table
clearing RADIUS server table 2-81

setting VARNAME variable 2-1010
shared key
clearing 2-81
SLIP
attaching 2-994
configuring interfaces 2-264
detaching 2-994
SNMP
adding trap receiver table entry 2-480
clearing community mapping 2-91
clearing SNMP trap receiver entry 2-96
clearing target parameters 2-95
configuring MIB view 2-485
configuring new user 2-483
configuring target address entry 2-476
configuring target parameters 2-478
defining access rights for specific context string 2-467
defining access rights for specific security type 2-467
defining community and associated access types 2-469
defining group access rights 2-467
disabling extendedrmon 2-471
disabling RMON support 2-474
disabling standard SNMP link trap 2-387
disabling traps 2-480
displaying access information 2-882
displaying community information 2-884
displaying context information 2-886
displaying counter information 2-887
displaying group or users with common access policy 2-892
displaying information 2-880
displaying information for specific user 2-901
displaying local engine ID 2-891
displaying MIB view configuration 2-903
displaying snmpNotifyTable configuration 2-894
displaying target address entries 2-897
displaying target parameter entries 2-899
enabling extendedrmon 2-471
enabling of standard SNMP link trap 2-387
enabling RMON support 2-474
enabling traps 2-480
establishing relationship between group and user 2-472
removing access rights for specific context string 2-90
removing access rights for specific security type 2-90
removing group access rights 2-90
removing individual user 2-97
removing MIB view entry 2-98
removing notifyname 2-93
removing SNMP user from SNMP group 2-92
removing target address entry 2-94
setting notifyname entry 2-473
setting notifytag entry 2-473
SNMP group
defining access rights for specific context string 2-467
defining access rights for specific security type 2-467
defining group access rights 2-467
removing access rights for specific context string 2-90
removing access rights for specific security type 2-90
removing group access rights 2-90
removing user 2-92
SNMP permit list
adding 2-274
clearing 2-28
SNMP trap receiver table
removing entry 2-96
sending message 2-1003
soft reset 2-172
software
displaying versions 2-975
SPAN
configuring 2-487
disabling 2-487
displaying information 2-905
enabling 2-487
spanning tree
assigning path cost 2-531
assigning port path cost for instances 2-526
clearing statistics 2-110

disabling 2-497
disabling BackboneFast 2-490
disabling BPDU packet filtering 2-524
disabling BPDU skewing 2-491
disabling instance 2-497
disabling MAC address reduction 2-509
disabling PortFast BPDU guard feature 2-525
disabling PortFast-start feature 2-522
disabling UplinkFast 2-539
display BackboneFast convergence status 2-910
displaying BPDU skew status 2-912
displaying current default port cost mode 2-916
displaying information summary 2-937
displaying instance-based guard information 2-917
displaying instance information 2-921
displaying list of instance numbers 2-914
displaying list of MAC addresses 2-914
displaying list of timers 2-914
displaying only blocked ports 2-911
displaying path cost for instances 2-928
displaying portfast information 2-927
displaying port information 2-807, 2-907
displaying statistics information 2-930
displaying time left before entry expires 2-914
displaying UplinkFast settings 2-940
displaying VLAN and instance mapping information 2-919
displaying VLAN-based guard information 2-917
displaying VLAN information 2-907
displaying VLAN path cost 2-929
enabling 2-499
enabling BackboneFast 2-490
enabling BPDU packet filtering 2-524
enabling BPDU skewing 2-491
enabling instance 2-499
enabling MAC address reduction 2-509
enabling PortFast BPDU guard feature 2-525
enabling PortFast-start feature 2-522
enabling UplinkFast 2-539
loop guard
  disabling 2-505
  enabling 2-505
resetting port instance priority 2-103
resetting port VLAN priority 2-107
restoring default bridge priority 2-108
restoring default forward delay 2-108
restoring default hello time 2-108
restoring default maxage 2-108
restoring default path cost 2-105
restoring default path cost to instance 2-101
restoring factory-set defaults 2-108
root guard
  disabling 2-505
  enabling 2-505
setting bridge forward delay 2-501
setting bridge hello time 2-507
setting bridge maximum aging time 2-510
setting instance bridge priority 2-534
setting mode 2-512
setting port bridge priority 2-530
setting port cost mode 2-495
setting port path cost 2-520
setting port priority 2-533
setting port priority for instances 2-528
setting primary root 2-536
setting secondary root 2-536
setting VLAN bridge priority 2-534
turning off UplinkFast 2-112
SSH permit list
  adding 2-274
  clearing 2-28
stack frame
  displaying 2-156
standby clock
  switching 2-997
statistics data export
  disabling globally 2-431
  disabling on aggregate policer 2-432

disabling on port 2-435
displaying configuration and status information 2-858
enabling globally 2-431
enabling on aggregate policer 2-432
enabling on port 2-435
setting export destination 2-433
setting export interval 2-434
summertime
displaying status 2-945
setting daylight saving time 2-334, 2-541
switch CLI
accessing 1-1
aliases 1-8
categories, definition 1-10
command aliases 1-8
command help 1-9
command-line editing features 1-4
command-line processing 1-3
command modes 1-3
console port 1-2
designating modules 1-10
help
switch CLI 1-9
history substitution 1-8
IP addresses 1-11
IP aliases 1-11
MAC addresses 1-11
operating 1-3
Telnet 1-2
switch fabric channel
displaying counter information 2-648
displaying switch mode and status 2-648
displaying utilization 2-648
Switch Fabric Module
configuring LCD banner 2-204
displaying LCD banner 2-596
switching
from active supervisor engine to standby supervisor engine 2-997
from clock from supervisor engine to internal clock 2-997
physically to MSFC on active supervisor engine 2-998
switching mode
setting system mode 2-950
syslog server
adding 2-301
system
displaying information 2-946
system clock
changing 2-564
displaying current time of day 2-961
system configuration
displaying nondefault configuration 2-620
displaying the system configuration mode 2-626
system contact
identifying 2-544
system disconnect
idle session timeout 2-307
system error log
clearing 2-40
system location
identifying 2-553
setting 2-548
system log
clearing buffer 2-42
displaying 2-690
displaying logging buffer 2-695
displaying system log configuration 2-690
system logging messages
disabling 2-301
disabling time-stamp display 2-305
enabling 2-301
enabling time-stamp display 2-305
sending to console 2-296
system logging server
deleting 2-45
displaying 2-693
system messages

setting facility level 2-298
setting severity level 2-298
system modem
disabling 2-554
enabling 2-554
system name
configuring 2-555
system switching mode
setting 2-556

T

TAC
displaying system and configuration information 2-953
TACACS+
configuring maximum number of login attempts 2-558
defining TACACS+ server 2-561
disabling accounting of normal login session 2-183
disabling accounting of system events 2-186
disabling authorization 2-198
disabling authorization of privileged mode events 2-200
disabling suppression of accounting information 2-185
disabling TACACS+ directed-request option 2-559
displaying accounting information 2-588
displaying authorization information 2-595
displaying protocol configuration 2-951
enabling accounting of normal login session 2-183
enabling accounting of outbound connection events 2-182
enabling accounting of system events 2-186
enabling authentication 2-194
enabling authorization 2-198
enabling authorization of EXEC mode events 2-202
enabling authorization of normal login mode 2-202
enabling authorization of privileged mode events 2-200
enabling authorization of session events 2-202
enabling command event accounting 2-181
enabling primary authentication login method 2-196
enabling suppression of accounting information 2-185
enabling TACACS+ directed-request option 2-559
removing host 2-114
removing key setting 2-113
setting accounting update frequency 2-188
setting authentication and encryption key 2-560
setting response timeout interval 2-562
TACACS, RADIUS, KERBEROS, HTTP
displaying authentication information 2-594
target address entry
removing 2-94
technical support
displaying system and configuration information 2-953
Telnet
closing session 2-148
connecting 2-1002
disconnecting 2-148
limiting login attempts 2-196
listing all active Telnet sessions 2-974
specifying authentication login method
disabling authentication 2-196
specifying authentication method 2-194
Telnet permit list
adding 2-274
clearing 2-28
temperature
displaying system status information 2-642
Terminal Access Controller Access Control System Plus
See TACACS+
terminal display
setting default number of lines on screen 2-294
setting number of lines on screen 2-294
text mode
configuring text mode 2-226
displaying text mode 2-626
time-stamp display
disabling on system logging messages 2-305
enabling on system logging messages 2-305
time zone

displaying 2-962
returning to default, UTC 2-115
setting 2-565
TopN
displaying all TopN processes and specific TopN reports 2-965
starting 2-963
stopping process 2-116
traffic
displaying information 2-967
traffic log
configuring threshold 2-566
traps
displaying status information 2-810
trunk
clearing VLAN from allowed VLAN list 2-117
displaying information 2-968
displaying port information 2-811
restoring trunk port to default trunk type and mode 2-117
trunk ports
adding VLANs 2-567
configuring 2-567
two-way community
configuring PVLANs 2-574
configuring VLAN 2-574
displaying PVLAN configuration 2-828

U

UDLD
disabling aggressive mode 2-572
displaying information 2-972
enabling aggressive mode 2-572
enabling UDLD information display 2-570
setting message interval 2-573
unicast suppression
setting 2-342
UniDirectional Link Detection Protocol
See UDLD
UplinkFast
displaying settings 2-940
uploading current configuration 2-1014
uploading current configuration to file 2-1017

V

VACL
creating new entry in non-IP VACL 2-463
creating new entry in non-IPX VACL 2-463
creating new entry in standard IP VACL 2-454
creating new entry in standard IPX VACL 2-459
displaying ACL management information 2-839
displaying capture port list entries 2-874
displaying configuration file location 2-620
displaying current configuration 2-871
displaying VACL management information 2-879
displaying VACL-to-VLAN mapping 2-878
mapping existing VACL-to-VLAN 2-465
removing all ACEs from VACL 2-84
removing entry from capture port list 2-86
removing VACL from editbuffer 2-84
removing VACL-to-VLAN mapping 2-88
setting ports to capture traffic 2-453
VACL logging
clearing all flows in log table 2-87
configuring log table 2-462
displaying log information 2-875
VACL-to-VLAN mapping
removing 2-88
variable name
removing 2-1009
VLAN
deleting 2-118
deleting reserved mapping 2-120
deleting VLAN-mapped pairs 2-120
displaying nontrunk port information 2-978
displaying trunk port information 2-978

displaying VLAN information 2-978
displaying VLAN mapping table information 2-978
grouping ports into VLAN
mapping 802.1Q VLANs to ISL VLANs 2-578
mapping reserved VLANs to nonreserved VLANs 2-578
VTP configuration caution 2-118
VLAN ACL
See VACL
VLAN membership
setting assignment to port 2-368
VLAN path cost
displaying 2-929
VLANs
mapping instances 2-574
VMPS
configuring server 2-582
deleting rcp user name 2-122
deleting server 2-123
deleting statistics 2-124
disabling 2-584
displaying configuration information 2-985
displaying MAC addresses in VLAN 2-989
displaying MAC-address-to-VLAN mapping table 2-987
displaying statistics 2-988
enabling 2-584
reconfirming membership assignments 2-168
specifying download method 2-580
specifying server 2-581
voice
configuring access port on Cisco IP phone 2-381
displaying active call information 2-816
displaying FDL information 2-820
displaying inline power status 2-642
displaying port voice information 2-813
displaying port voice interface 2-822
displaying power administration status 2-791
displaying power operational status 2-791
setting default power allocation 2-263
setting inline power mode 2-364
setting port voice interface
DHCP server 2-388
DNS server 2-388
TFTP server 2-388
VTP
clearing statistics 2-126
defining VTP password 2-585
disabling VTP pruning 2-585
displaying VTP domain information 2-990
displaying VTP statistics 2-992
enabling VTP pruning 2-585
setting options 2-585
setting version 2 mode 2-585
setting VTP domain name 2-585
setting VTP mode 2-585
specifying pruning-eligible VTP domain VLANs 2-587
specifying pruning-ineligible VTP domain VLANs 2-125

W

web interface
configuring TCP port number 2-272
disabling HTTP server 2-273
displaying HTTP configuration 2-673
displaying version information 2-975
enabling HTTP server 2-273
WRED
configuring threshold values 2-437
mapping guidelines 2-421
port type description 2-421
setting amount of packet buffer memory 2-430
WRR
specifying weights 2-439