Part No. 060207-10, Rev. A
April 2006

OmniSwitch CLI Reference Guide

www.alcatel.com

This user guide documents release 5.4 of the OmniSwitch 6600 Family, OmniSwitch 7700, OmniSwitch 7800, and OmniSwitch 8800.
The functionality described in this guide is subject to change without notice.

Alcatel® and the Alcatel logo are registered trademarks of Alcatel. Xylan®, OmniSwitch®, OmniStack®, and Alcatel OmniVista® are registered trademarks of Alcatel Internetworking, Inc.

OmniAccess™, Omni Switch/Router™, PolicyView™, RouterView™, SwitchManager™, VoiceView™, WebView™, X-Cell™, X-Vision™, and the Xylan logo are trademarks of Alcatel Internetworking, Inc.

This OmniSwitch product contains components which may be covered by one or more of the following U.S. Patents:

- U.S. Patent No. 6,339,830
- U.S. Patent No. 6,070,243
- U.S. Patent No. 6,061,368
- U.S. Patent No. 5,394,402
- U.S. Patent No. 6,047,024
- U.S. Patent No. 6,314,106
- U.S. Patent No. 6,542,507
- U.S. Patent No. 6,874,090

26801 West Agoura Road
Calabasas, CA 91301
(818) 880-3500 FAX (818) 880-3505
info@ind.alcatel.com

US Customer Support—(800) 995-2696
International Customer Support—(818) 878-4507
Internet—http://eservice.ind.alcatel.com

Contents

About This Guide xxvii

Supported Platforms xxvii

Who Should Read this Manual? xxviii

When Should I Read this Manual? xxix

What is in this Manual? xxx

What is Not in this Manual? xxx

How is the Information Organized? xxx

Text Conventions xxxi

Documentation Roadmap xxxii

Related Documentation xxxiii

User Manuals Web Site xxxvi

Technical Support xxxvi

Chapter 1 **CMM Commands** 1-1

- reload 1-2
- reload working 1-4
- copy running-config working 1-6
- write memory 1-8
- copy certified working 1-10
- copy working certified 1-11
- copy flash-synchro 1-13
- takeover 1-14
- debug chassis auto-reboot 1-16
- show running-directory 1-17
- show reload 1-20
- show microcode 1-21
- show microcode history 1-23

Chapter 2 **Chassis Management and Monitoring Commands** 2-1

- system contact 2-3
- system name 2-4
- system location 2-5
- system date 2-6
- system time 2-7
- system time-and-date synchro 2-8
- system timezone 2-9
- system daylight savings time 2-12
- reload ni 2-14
- reload all 2-16

power ni 2-18
temp-threshold 2-20
fabric standby 2-21
power fabric 2-22
show system 2-23
show hardware info 2-25
show chassis 2-28
show cmm 2-30
show ni 2-33
show module 2-36
show module long 2-38
show module status 2-40
show power 2-42
show fan 2-44
show temperature 2-46
show stack topology 2-49
show fabric 2-51

Chapter 3 Chassis MAC Server (CMS) Commands 3-1
mac-range eeprom 3-2
show mac-range 3-4
show mac-range alloc 3-6

Chapter 4 Power over Ethernet (PoE) Commands 4-1
lanpower start 4-3
lanpower stop 4-5
lanpower power 4-6
lanpower maxpower 4-8
lanpower priority 4-10
lanpower priority-disconnect 4-12
lanpower redundant-power 4-14
lanpower capacitor-detection 4-15
show lanpower 4-16
show lanpower capacitor-detection 4-19
show lanpower priority-disconnect 4-20
show lanpower slot-priority 4-21

Chapter 5 Network Time Protocol Commands 5-1
ntp server 5-2
ntp client 5-4
ntp broadcast 5-5
ntp broadcast-delay 5-6
ntp key 5-7
ntp key load 5-9
show ntp client 5-10
show ntp client server-list 5-12
show ntp server status 5-14
show ntp keys 5-16

Chapter 6 Session Management Commands 6-1
session login-attempt 6-3
session login-timeout 6-4
session banner 6-5
session timeout 6-7
session prompt 6-9
session xon-xoff 6-10
prompt 6-11
show prefix 6-13
alias 6-14
show alias 6-16
user profile save 6-17
user profile reset 6-18
history size 6-19
show history 6-20
! 6-22
command-log 6-24
kill 6-25
exit 6-26
whoami 6-27
who 6-30
show session config 6-32
show session xon-xoff 6-34
more size 6-35
more 6-36
show more 6-37
telnet 6-38
ssh 6-39
show command-log 6-40
show command-log status 6-42

Chapter 7 File Management Commands 7-1
cd 7-3
pwd 7-5
mkdir 7-6
rmdir 7-8
ls 7-10
dir 7-12
rename 7-14
rm 7-16
delete 7-17
cp 7-18
mv 7-20
move 7-22
chmod 7-24
attrib 7-25
freespace 7-26
fsck 7-27
newfs 7-29
rcp 7-30
rrm 7-32
rls 7-34

rdf 7-36
vi 7-38
view 7-39
tty 7-40
show tty 7-42
more 7-43
ftp 7-45
sftp 7-47
rz 7-49
install 7-50

Chapter 8 Web Management Commands 8-1
http server 8-2
http ssl 8-3
debug http sessiondb 8-4
show http 8-6

Chapter 9 Configuration File Manager Commands 9-1
configuration apply 9-2
configuration error-file limit 9-4
show configuration status 9-6
configuration cancel 9-8
configuration syntax check 9-9
configuration snapshot 9-11
show configuration snapshot 9-14
write terminal 9-17

Chapter 10 SNMP Commands 10-1
snmp station 10-3
show snmp station 10-5
snmp community map 10-7
snmp community map mode 10-9
show snmp community map 10-10
snmp security 10-11
show snmp security 10-13
show snmp statistics 10-15
show snmp mib family 10-17
snmp trap absorption 10-19
snmp trap to webview 10-20
snmp trap replay 10-21
snmp trap filter 10-23
snmp authentication trap 10-25
show snmp trap replay 10-26
show snmp trap filter 10-27
show snmp authentication trap 10-29
show snmp trap config 10-30

Chapter 11 Hardware Routing Engine (HRE) Commands 11-1
hre mode configuration 11-2
hre clear changes 11-4
hre apply changes 11-6
show hre changes 11-7
show hre configuration 11-9
show hre pcam utilization 11-11
show hre statistics 11-13
show hre cache utilization 11-15

Chapter 12 DNS Commands 12-1
ip domain-lookup 12-2
ip name-server 12-3
ip domain-name 12-5
show dns 12-6

Chapter 13 Link Aggregation Commands 13-1
static linkagg size 13-3
static linkagg name 13-5
static linkagg admin state 13-6
static agg agg num 13-7
lacp linkagg size 13-9
lacp linkagg name 13-12
lacp linkagg admin state 13-13
lacp linkagg actor admin key 13-15
lacp linkagg actor system priority 13-16
lacp linkagg actor system id 13-17
lacp linkagg partner system id 13-18
lacp linkagg partner system priority 13-20
lacp linkagg partner admin key 13-21
lacp agg actor admin key 13-22
lacp agg actor admin state 13-25
lacp agg actor system id 13-27
lacp agg actor system priority 13-29
lacp agg partner admin state 13-31
lacp agg partner admin system id 13-33
lacp agg partner admin key 13-35
lacp agg partner admin system priority 13-37
lacp agg actor port priority 13-39
lacp agg partner admin port 13-41
lacp agg partner admin port priority 13-43
linkagg slot optimization 13-45
linkagg slot single 13-47
linkagg slot multiple 13-49
show linkagg 13-51
show linkagg port 13-56
show linkagg slot optimization 13-61

Chapter 14 Interswitch Protocol Commands 14-1
amap 14-2
amap discovery time 14-3
amap common time 14-5
show amap 14-7

Chapter 15 802.1Q Commands 15-1
vlan 802.1q 15-2
vlan 802.1q frame type 15-4
vlan 802.1q force tag internal 15-6
debug 802.1q 15-8
show 802.1q 15-10

Chapter 16 Distributed Spanning Tree Commands 16-1
bridge mode 16-4
bridge protocol 16-6
bridge cist protocol 16-8
bridge 1x1 protocol 16-10
bridge mst region name 16-12
bridge mst region revision level 16-14
bridge mst region max hops 16-15
bridge msti 16-17
bridge msti vlan 16-19
bridge priority 16-21
bridge cist priority 16-23
bridge msti priority 16-25
bridge 1x1 priority 16-27
bridge hello time 16-29
bridge cist hello time 16-31
bridge 1x1 hello time 16-33
bridge max age 16-35
bridge cist max age 16-37
bridge 1x1 max age 16-39
bridge forward delay 16-41
bridge cist forward delay 16-43
bridge 1x1 forward delay 16-45
bridge bpdu-switching 16-47
bridge path cost mode 16-49
bridge slot/port 16-51
bridge cist port 16-53
bridge 1x1 port 16-55
bridge slot/port priority 16-57
bridge cist slot/port priority 16-59
bridge msti slot/port priority 16-61
bridge 1x1 slot/port priority 16-63
bridge slot/port path cost 16-65
bridge cist slot/port path cost 16-69
bridge msti slot/port path cost 16-73
bridge 1x1 slot/port path cost 16-76
bridge slot/port mode 16-80
bridge cist slot/port mode 16-82
bridge 1x1 slot/port mode 16-84

bridge slot/port connection 16-86
bridge cist slot/port connection 16-88
bridge 1x1 slot/port connection 16-90
show spantree 16-92
show spantree cist 16-98
show spantree msti 16-102
show spantree 1x1 16-107
show spantree ports 16-111
show spantree cist ports 16-119
show spantree msti ports 16-123
show spantree 1x1 ports 16-128
show spantree mst region 16-133
show spantree msti vlan-map 16-135
show spantree cist vlan-map 16-137
show spantree map-msti 16-139
show spantree mst port 16-140

Chapter 17 Source Learning Commands 17-1
mac-address-table 17-2
mac-address-table static-multicast 17-5
mac-address-table aging-time 17-7
show mac-address-table 17-9
show mac-address-table static-multicast 17-11
show mac-address-table count 17-14
show mac-address-table aging-time 17-16

Chapter 18 Learned Port Security Commands 18-1
port-security 18-2
port-security shutdown 18-4
port security maximum 18-6
port-security mac 18-8
port-security mac-range 18-10
port-security violation 18-12
port-security release 18-14
show port-security 18-16
show port-security shutdown 18-18

Chapter 19 Ethernet Port Commands 19-1
trap port link 19-3
flow 19-5
flow wait time 19-7
interfaces speed 19-9
interfaces autoneg 19-12
interfaces crossover 19-14
interfaces flow 19-16
interfaces duplex 19-18
interfaces admin 19-20
interfaces alias 19-22
interfaces ifg 19-24
interfaces no l2 statistics 19-26
interfaces long 19-28
interfaces max frame 19-30

interfaces runt 19-31
interfaces runtsize 19-33
interfaces flood 19-35
interfaces flood multicast 19-36
interfaces flood rate 19-38
10gig slot 19-40
show interfaces flow control 19-41
show interfaces 19-43
show interfaces capability 19-47
show interfaces accounting 19-49
show interfaces counters 19-52
show interfaces counters errors 19-54
show interfaces collisions 19-56
show interfaces status 19-58
show interfaces port 19-61
show interfaces ifg 19-63
show interfaces flood rate 19-65
show interfaces traffic 19-67
show 10gig 19-69
debug interfaces set backpressure 19-70
debug interfaces backpressure 19-71

Chapter 20 Port Mobility Commands 20-1
vlan dhcp mac 20-2
vlan dhcp mac range 20-4
vlan dhcp port 20-6
vlan dhcp generic 20-8
vlan binding mac-ip-port 20-10
vlan binding mac-port-protocol 20-12
vlan binding mac-port 20-14
vlan binding mac-ip 20-16
vlan binding ip-port 20-18
vlan binding port-protocol 20-20
vlan mac 20-22
vlan mac range 20-24
vlan ip 20-26
vlan ipx 20-28
vlan protocol 20-30
vlan user 20-32
vlan port 20-34
vlan port mobile 20-36
vlan port default vlan restore 20-38
vlan port default vlan 20-40
vlan port authenticate 20-42
vlan port 802.1x 20-43
show vlan rules 20-45
show vlan port mobile 20-47

Chapter 21 VLAN Management Commands 21-1
vlan 21-2
vlan stp 21-4
vlan mobile-tag 21-6
vlan authentication 21-8
vlan router ipx 21-9
vlan router mac multiple 21-11
vlan port default 21-13
show vlan 21-15
show vlan port 21-18
show vlan router mac status 21-21

Chapter 22 Port Mapping Commands 22-1
port mapping user-port network-port 22-2
port mapping 22-4
port mapping 22-6
show port mapping status 22-8
show port mapping 22-10

Chapter 23 IP Commands 23-1
ip interface 23-4
ip router primary-address 23-7
ip router router-id 23-8
ip static-route 23-9
ip route-pref 23-11
ip default-ttl 23-13
ping 23-14
traceroute 23-16
ip directed-broadcast 23-18
ip service 23-19
arp 23-21
clear arp-cache 23-23
arp filter 23-24
clear arp filter 23-26
icmp type 23-27
icmp unreachable 23-30
icmp echo 23-32
icmp timestamp 23-34
icmp addr-mask 23-36
icmp messages 23-38
ip dos scan close-port-penalty 23-39
ip dos scan tcp open-port-penalty 23-40
ip dos scan udp open-port-penalty 23-41
ip dos scan threshold 23-42
ip dos trap 23-44
ip dos scan decay 23-45
show ip traffic 23-46
show ip interface 23-49
show ip route 23-53
show ip route-pref 23-55
show ip router database 23-57
show ip emp-route 23-60

show ip config 23-62
show ip protocols 23-63
show ip service 23-65
show arp 23-67
show arp filter 23-69
show icmp control 23-71
show icmp statistics 23-73
show tcp statistics 23-75
show tcp ports 23-77
show udp statistics 23-79
show udp ports 23-80
show ip dos config 23-81
show ip dos statistics 23-83
debug ip packet 23-85
debug ip level 23-88
debug ip packet default 23-89
debug ip packet 23-90

Chapter 24 IPv6 Commands 24-1
ipv6 interface 24-3
ipv6 address 24-6
ipv6 interface tunnel source destination 24-8
ipv6 dad-check 24-9
ipv6 hop-limit 24-10
ipv6 pmtu-lifetime 24-11
ipv6 host 24-12
ipv6 neighbor 24-13
ipv6 prefix 24-14
ipv6 route 24-16
ping6 24-17
traceroute6 24-19
debug ipv6 packet 24-21
debug ipv6 trace-category 24-24
show ipv6 hosts 24-26
show ipv6 icmp statistics 24-27
show ipv6 interface 24-30
show ipv6 pmtu table 24-35
clear ipv6 pmtu table 24-37
show ipv6 neighbors 24-38
clear ipv6 neighbors 24-40
show ipv6 prefixes 24-41
show ipv6 routes 24-43
show ipv6 tcp ports 24-45
show ipv6 traffic 24-47
clear ipv6 traffic 24-50
show ipv6 tunnel 24-51
show ipv6 udp ports 24-53
ipv6 load rip 24-55
ipv6 rip status 24-56
ipv6 rip invalid-timer 24-57
ipv6 rip garbage-timer 24-58
ipv6 rip holddown-timer 24-59

ipv6 rip jitter 24-60
ipv6 rip route-tag 24-61
ipv6 rip update-interval 24-62
ipv6 rip triggered-sends 24-63
ipv6 rip interface 24-64
ipv6 rip interface metric 24-66
ipv6 rip interface recv-status 24-67
ipv6 rip interface send-status 24-68
ipv6 rip interface horizon 24-69
ipv6 rip debug-level 24-70
ipv6 rip debug-type 24-71
show ipv6 rip 24-73
show ipv6 rip interface 24-75
show ipv6 rip peer 24-78
show ipv6 rip routes 24-80
show ipv6 rip debug 24-83

Chapter 25 RDP Commands 25-1
ip router-discovery 25-2
ip router-discovery interface 25-3
ip router-discovery interface advertisement-address 25-5
ip router-discovery interface max-advertisement-interval 25-7
ip router-discovery interface min-advertisement-interval 25-9
ip router-discovery interface advertisement-lifetime 25-11
ip router-discovery interface preference-level 25-13
show ip router-discovery 25-15
show ip router-discovery interface 25-17

Chapter 26 DHCP Relay Commands 26-1
ip helper address 26-2
ip helper address vlan 26-4
ip helper standard 26-6
ip helper avlan only 26-7
ip helper per-vlan only 26-9
ip helper forward delay 26-11
ip helper maximum hops 26-13
ip helper agent-information 26-15
ip helper agent-information policy 26-17
ip helper dhcp-snooping 26-19
ip helper dhcp-snooping mac-address verification 26-20
ip helper dhcp-snooping option-82 data-insertion 26-21
ip helper dhcp-snooping vlan 26-23
ip helper dhcp-snooping port 26-25
ip helper dhcp-snooping binding 26-27
ip helper dhcp-snooping binding timeout 26-29
ip helper dhcp-snooping binding action 26-30
ip helper boot-up 26-31
ip helper boot-up enable 26-32
ip udp relay 26-33
ip udp relay vlan 26-35
show ip helper 26-37
show ip helper stats 26-40

show ip helper dhcp-snooping vlan 26-42
show ip helper dhcp-snooping port 26-44
show ip helper dhcp-snooping binding 26-46
show ip udp relay service 26-48
show ip udp relay statistics 26-50
show ip udp relay destination 26-52

Chapter 27 RIP Commands 27-1
ip load rip 27-3
ip rip status 27-4
ip rip interface 27-5
ip rip interface status 27-7
ip rip interface metric 27-8
ip rip interface send-version 27-9
ip rip interface recv-version 27-11
ip rip force-holddowntimer 27-13
ip rip host-route 27-15
ip rip route-tag 27-16
ip rip redist status 27-17
ip rip redist 27-18
ip rip redist metric 27-20
ip rip redist-filter 27-22
ip rip redist-filter effect 27-24
ip rip redist-filter metric 27-26
ip rip redist-filter route-tag 27-28
ip rip redist-filter redist-control 27-29
ip rip interface auth-type 27-31
ip rip interface auth-key 27-32
ip rip debug-type 27-33
ip rip debug-level 27-35
show ip rip 27-36
show ip rip routes 27-38
show ip rip interface 27-40
show ip rip peer 27-42
show ip rip redist 27-44
show ip rip redist-filter 27-46
show ip rip debug 27-48

Chapter 28 IPX Commands 28-1
ipx routing 28-2
ipx default-route 28-3
ipx route 28-5
clear ipx route 28-7
ping ipx 28-9
ipx filter rip 28-11
ipx filter sap 28-13
ipx filter gns 28-16
ipx type-20-propagation 28-18
ipx packet-extension 28-20
ipx timers 28-22
show ipx interface 28-24
show ipx traffic 28-28

show ipx default-route 28-32
show ipx route 28-34
show ipx servers 28-36
show ipx filter 28-38
show ipx type-20-propagation 28-40
show ipx packet-extension 28-41
show ipx timers 28-42

Chapter 29 VRRP Commands 29-1
vrrp 29-2
vrrp ip 29-5
vrrp trap 29-6
vrrp delay 29-7
vrrp track 29-8
vrrp track-association 29-10
show vrrp 29-11
show vrrp statistics 29-14
show vrrp track 29-17
show vrrp track-association 29-19

Chapter 30 OSPF Commands 30-1
ip ospf status 30-3
ip load ospf 30-4
ip ospf asbr 30-5
ip ospf exit-overflow-interval 30-6
ip ospf extlsdb-limit 30-7
ip ospf host 30-8
ip ospf mtu-checking 30-10
ip ospf redist-filter 30-11
ip ospf redist status 30-13
ip ospf redist 30-14
ip ospf route-tag 30-16
ip ospf spf-timer 30-17
ip ospf virtual-link 30-19
ip ospf neighbor 30-22
ip ospf debug-level 30-24
ip ospf debug-type 30-25
ip ospf area 30-28
ip ospf area status 30-30
ip ospf area default-metric 30-31
ip ospf area range 30-33
ip ospf interface 30-35
ip ospf interface status 30-36
ip ospf interface area 30-38
ip ospf interface auth-key 30-39
ip ospf interface auth-type 30-40
ip ospf interface dead-interval 30-42
ip ospf interface hello-interval 30-44
ip ospf interface md5 30-45
ip ospf interface md5 key 30-47
ip ospf interface type 30-49
ip ospf interface cost 30-51

ip ospf interface poll-interval 30-52
ip ospf interface priority 30-53
ip ospf interface retrans-interval 30-54
ip ospf interface transit-delay 30-55
ip ospf restart-support 30-56
ip ospf restart-interval 30-57
ip ospf restart-helper status 30-58
ip ospf restart-helper strict-lsa-checking-status 30-60
ip ospf restart initiate 30-62
show ip ospf 30-63
show ip ospf border-routers 30-66
show ip ospf ext-lsdb 30-68
show ip ospf host 30-70
show ip ospf lsdb 30-72
show ip ospf neighbor 30-74
show ip ospf redist-filter 30-77
show ip ospf redist 30-79
show ip ospf routes 30-81
show ip ospf virtual-link 30-83
show ip ospf virtual-neighbor 30-85
show ip ospf area 30-88
show ip ospf area range 30-91
show ip ospf area stub 30-93
show ip ospf interface 30-95
show ip ospf restart 30-101
show ip ospf debug 30-103

Chapter 31 BGP Commands 31-1
ip load bgp 31-4
ip bgp status 31-5
ip bgp autonomous-system 31-6
ip bgp bestpath as-path ignore 31-7
ip bgp cluster-id 31-9
ip bgp default local-preference 31-10
ip bgp fast-external-failover 31-12
ip bgp always-compare-med 31-14
ip bgp bestpath med missing-as-worst 31-15
ip bgp client-to-client reflection 31-16
ip bgp as-origin-interval 31-18
ip bgp synchronization 31-19
ip bgp confederation identifier 31-21
ip bgp maximum-paths 31-22
ip bgp log-neighbor-changes 31-23
ip bgp dampening 31-24
ip bgp dampening clear 31-27
ip bgp debug-type 31-28
ip bgp debug-level 31-30
ip bgp aggregate-address 31-31
ip bgp aggregate-address status 31-33
ip bgp aggregate-address as-set 31-35
ip bgp aggregate-address community 31-37
ip bgp aggregate-address local-preference 31-39

ip bgp aggregate-address metric 31-41
ip bgp aggregate-address summary-only 31-43
ip bgp network 31-45
ip bgp network status 31-47
ip bgp network community 31-49
ip bgp network local-preference 31-50
ip bgp network metric 31-52
ip bgp neighbor 31-54
ip bgp neighbor status 31-55
ip bgp neighbor advertisement-interval 31-56
ip bgp neighbor clear 31-57
ip bgp neighbor route-reflector-client 31-59
ip bgp neighbor default-originate 31-60
ip bgp neighbor timers 31-61
ip bgp neighbor conn-retry-interval 31-63
ip bgp neighbor auto-restart 31-65
ip bgp neighbor maximum-prefix 31-67
ip bgp neighbor md5 key 31-69
ip bgp neighbor ebgp-multihop 31-71
ip bgp neighbor description 31-73
ip bgp neighbor next-hop-self 31-74
ip bgp neighbor passive 31-76
ip bgp neighbor remote-as 31-77
ip bgp neighbor remove-private-as 31-79
ip bgp neighbor soft-reconfiguration 31-80
ip bgp neighbor stats-clear 31-82
ip bgp confederation neighbor 31-83
ip bgp neighbor update-source 31-84
ip bgp neighbor in-aspathlist 31-86
ip bgp neighbor in-communitylist 31-87
ip bgp neighbor in-prefixlist 31-88
ip bgp neighbor out-aspathlist 31-89
ip bgp neighbor out-communitylist 31-90
ip bgp neighbor out-prefixlist 31-91
ip bgp neighbor route-map 31-92
ip bgp neighbor clear soft 31-94
ip bgp policy aspath-list 31-95
ip bgp policy aspath-list action 31-97
ip bgp policy aspath-list priority 31-99
ip bgp policy community-list 31-101
ip bgp policy community-list action 31-103
ip bgp policy community-list match-type 31-105
ip bgp policy community-list priority 31-107
ip bgp policy prefix-list 31-109
ip bgp policy prefix-list action 31-111
ip bgp policy prefix-list ge 31-112
ip bgp policy prefix-list le 31-114
ip bgp policy route-map 31-116
ip bgp policy route-map action 31-118
ip bgp policy route-map aspath-list 31-119
ip bgp policy route-map asprepend 31-120
ip bgp policy route-map community 31-121

ip bgp policy route-map community-list 31-123
ip bgp policy route-map community-mode 31-124
ip bgp policy route-map lpref 31-125
ip bgp policy route-map lpref-mode 31-126
ip bgp policy route-map match-community 31-128
ip bgp policy route-map match-mask 31-130
ip bgp policy route-map match-prefix 31-131
ip bgp policy route-map match-regexp 31-132
ip bgp policy route-map med 31-134
ip bgp policy route-map med-mode 31-135
ip bgp policy route-map origin 31-137
ip bgp policy route-map prefix-list 31-139
ip bgp policy route-map weight 31-141
ip bgp policy route-map community-strip 31-142
ip bgp redist-filter 31-143
ip bgp redist-filter community 31-145
ip bgp redist-filter effect 31-147
ip bgp redist-filter local-preference 31-149
ip bgp redist-filter metric 31-151
ip bgp redist-filter subnets 31-153
show ip bgp 31-155
show ip bgp statistics 31-158
show ip bgp dampening 31-160
show ip bgp dampening-stats 31-162
show ip bgp path 31-164
show ip bgp routes 31-168
show ip bgp debug 31-170
show ip bgp aggregate-address 31-173
show ip bgp network 31-175
show ip bgp neighbors 31-177
show ip bgp neighbors policy 31-181
show ip bgp neighbors timer 31-183
show ip bgp neighbors statistics 31-185
show ip bgp policy aspath-list 31-190
show ip bgp policy community-list 31-192
show ip bgp policy prefix-list 31-194
show ip bgp policy route-map 31-196
show ip bgp redist-filter 31-199

Chapter 32 PIM-SM Commands 32-1
ip load pimsm 32-3
ip pimsm status 32-4
ip pimsm cbsr-masklength 32-5
ip pimsm static-rp status 32-6
ip pimsm static-rp 32-8
ip pimsm rp-candidate 32-10
ip pimsm rp-threshold 32-12
ip pimsm crp-address 32-13
ip pimsm crp-expirytime 32-14
ip pimsm crp-holdtime 32-15
ip pimsm crp-interval 32-16
ip pimsm crp-priority 32-17

ip pimsm data-timeout 32-18
ip pimsm joinprune-interval 32-19
ip pimsm max-rps 32-20
ip pimsm probe-time 32-21
ip pimsm register checksum 32-22
ip pimsm registersuppress-timeout 32-23
ip pimsm spt status 32-24
ip pimsm interface 32-25
ip pimsm interface hello-interval 32-27
ip pimsm interface joinprune-interval 32-28
ip pimsm interface cbsr-preference 32-30
ip pimsm interface dr-priority 32-32
ip pimsm interface prune-delay status 32-34
ip pimsm interface prune-delay 32-36
ip pimsm interface override-interval 32-38
ip pimsm interface triggered-hello 32-40
ip pimsm interface hello-holdtime 32-42
ip pimsm interface genid 32-44
ip pimsm interface joinprune-holdtime 32-46
ip pimsm debug-level 32-48
ip pimsm debug-type 32-49
show ip pimsm 32-51
show ip pimsm neighbor 32-55
show ip pimsm rp-candidate 32-57
show ip pimsm rp-set 32-59
show ip pimsm interface 32-61
show ip pimsm nexthop 32-65
show ip pimsm mroute 32-67
show ip pimsm static-rp 32-69
show ip pimsm debug 32-71

Chapter 33 DVMRP Commands 33-1
ip load dvmrp 33-2
ip dvmrp status 33-3
ip dvmrp flash-interval 33-5
ip dvmrp graft-timeout 33-6
ip dvmrp interface 33-7
ip dvmrp interface metric 33-8
ip dvmrp neighbor-interval 33-9
ip dvmrp neighbor-timeout 33-10
ip dvmrp prune-lifetime 33-11
ip dvmrp prune-timeout 33-12
ip dvmrp report-interval 33-13
ip dvmrp route-holddown 33-14
ip dvmrp route-timeout 33-15
ip dvmrp subord-default 33-16
ip dvmrp tunnel 33-18
ip dvmrp tunnel ttl 33-20
ip dvmrp debug-level 33-22
ip dvmrp debug-type 33-23
show ip dvmrp 33-25
show ip dvmrp interface 33-29

show ip dvmrp neighbor 33-32
show ip dvmrp nexthop 33-34
show ip dvmrp prune 33-36
show ip dvmrp route 33-38
show ip dvmrp tunnel 33-40
show ip dvmrp debug 33-42

Chapter 34 Multicast Routing Commands 34-1
ip mroute-boundary 34-2
ip mroute interface ttl 34-4
show ip mroute-boundary 34-5
show ip mroute 34-7
show ip mroute interface 34-9
show ip mroute-nexthop 34-11
ip mroute debug-level 34-13
ip mroute debug-type 34-14
show ip mroute debug 34-16

Chapter 35 Port Mirroring and Monitoring Commands 35-1
port mirroring source destination 35-2
port mirroring 35-4
port monitoring source 35-6
port monitoring 35-9
show port mirroring status 35-10
show port monitoring status 35-13
show port monitoring file 35-15

Chapter 36 RMON Commands 36-1
rmon probes 36-2
show rmon probes 36-4
show rmon events 36-7

Chapter 37 Health Monitoring Commands 37-1
health threshold 37-2
health interval 37-4
health statistics reset 37-5
show health threshold 37-6
show health interval 37-8
show health 37-9
show health all 37-11
show health slice 37-13

Chapter 38 QoS Commands 38-1
qos 38-5
qos trust ports 38-7
qos default queues 38-9
qos forward log 38-10
qos log console 38-11
qos log lines 38-12
qos log level 38-13
qos classifyl3 bridged 38-15
qos classify fragments 38-17

qos flow timeout 38-18
qos fragment timeout 38-19
qos reflexive timeout 38-20
qos nat timeout 38-22
qos default bridged disposition 38-24
qos default routed disposition 38-26
qos default multicast disposition 38-27
qos stats interval 38-28
debug qos 38-29
debug qos internal 38-31
qos clear log 38-33
qos apply 38-34
qos revert 38-35
qos flush 38-36
qos reset 38-38
qos stats reset 38-39
policy rule 38-40
policy network group 38-43
policy service group 38-45
policy mac group 38-47
policy port group 38-49
policy service 38-51
policy service protocol 38-54
policy service source tcp port 38-56
policy service destination tcp port 38-58
policy service source udp port 38-60
policy service destination udp port 38-62
policy map group 38-64
policy condition 38-66
policy condition source ip 38-70
policy condition destination ip 38-72
policy condition multicast ip 38-74
policy condition source network group 38-76
policy condition destination network group 38-78
policy condition multicast network group 38-80
policy condition source ip port 38-82
policy condition destination ip port 38-84
policy condition source tcp port 38-86
policy condition destination tcp port 38-88
policy condition source udp port 38-90
policy condition destination udp port 38-92
policy condition ethertype 38-94
policy condition service 38-96
policy condition service group 38-97
policy condition ip protocol 38-99
policy condition source mac 38-101
policy condition destination mac 38-103
policy condition source mac group 38-105
policy condition destination mac group 38-107
policy condition source vlan 38-109
policy condition destination vlan 38-110
policy condition source port 38-111

policy condition destination port 38-113
policy condition source port group 38-115
policy condition destination port group 38-117
policy condition source interface type 38-119
policy condition destination interface type 38-121
policy action 38-123
policy action disposition 38-126
policy action shared 38-128
policy action priority 38-130
policy action maximum bandwidth 38-132
policy action maximum buffers 38-134
policy action minimum depth 38-136
policy action maximum depth 38-138
policy action tos 38-140
policy action 802.1p 38-142
policy action dscp 38-144
policy action map 38-146
policy action source rewrite ip 38-148
policy action source rewrite network group 38-150
policy action destination rewrite ip 38-152
policy action destination rewrite network group 38-154
policy action load balance group 38-156
policy action alternate gateway ip 38-158
policy action permanent gateway ip 38-160
qos port reset 38-162
qos port 38-163
qos port default queues 38-165
qos port trusted 38-167
qos port maximum reserve bandwidth 38-169
qos port maximum signal bandwidth 38-171
qos port maximum default depth 38-173
qos port maximum default buffers 38-175
qos port default 802.1p 38-177
qos port default dscp 38-178
qos port default classification 38-179
qos port enqueuing thresholds 38-181
qos port protocol priority 38-184
qos slice 38-186
qos slice dscp 38-188
qos slice servicing mode 38-190
qos slice wred thresholds 38-192
show policy classify 38-195
show policy classify source port 38-198
show policy classify destination port 38-200
show policy classify source mac 38-202
show policy classify destination mac 38-204
show policy classify source vlan 38-206
show policy classify destination vlan 38-208
show policy classify source interface type 38-210
show policy classify destination interface type 38-212
show policy classify 802.1p 38-214
show policy classify source ip 38-215

show policy classify destination ip 38-217
show policy classify multicast ip 38-219
show policy classify tos 38-221
show policy classify dscp 38-223
show policy classify ip protocol 38-225
show policy classify source ip port 38-227
show policy classify destination ip port 38-229
show policy network group 38-231
show policy service 38-233
show policy service group 38-235
show policy mac group 38-237
show policy port group 38-239
show policy map group 38-241
show policy action 38-243
show policy condition 38-245
show active policy rule 38-248
show policy rule 38-250
show qos port 38-253
show qos port statistics 38-257
show qos port high-density-module 38-261
show qos port pdis 38-264
show qos queue 38-266
show qos slice 38-269
show qos slice high-density-module 38-271
show qos slice pcams 38-274
show qos log 38-276
show qos config 38-278
show qos statistics 38-281

Chapter 39 Policy Server Commands 39-1
policy server load 39-2
policy server flush 39-3
policy server 39-4
show policy server 39-6
show policy server long 39-8
show policy server statistics 39-10
show policy server rules 39-12
show policy server events 39-14

Chapter 40 IP Multicast Switching Commands 40-1
ip multicast switching 40-2
ip multicast igmp-proxy-version 40-3
ip multicast leave-timeout 40-4
ip multicast query-interval 40-5
ip multicast membership-timeout 40-6
ip multicast neighbor-timeout 40-7
ip multicast querier-timeout 40-8
ip multicast other-querier-timeout 40-9
ip multicast flow-timeout 40-10
ip multicast priority 40-11
ip multicast max-ingress-bandwidth 40-12
ip multicast static-neighbor 40-13

ip multicast static-querier 40-15
ip multicast static-member 40-17
ip multicast hardware-routing 40-19
show ip multicast switching 40-20
show ip multicast groups 40-23
show ip multicast neighbors 40-25
show ip multicast queriers 40-27
show ip multicast forwarding 40-29
show ip multicast policy-cache 40-31

Chapter 41 Server Load Balancing Commands 41-1
ip slb admin 41-3
ip slb cluster 41-4
ip slb cluster admin status 41-6
ip slb cluster ping period 41-7
ip slb cluster ping timeout 41-9
ip slb cluster ping retries 41-11
ip slb cluster distribution 41-12
ip slb cluster sticky time 41-14
ip slb cluster probe 41-16
ip slb server ip cluster 41-17
ip slb server ip cluster probe 41-19
ip slb probe 41-20
ip slb probe timeout 41-22
ip slb probe period 41-24
ip slb probe port 41-26
ip slb probe retries 41-28
ip slb probe username 41-30
ip slb probe password 41-31
ip slb probe url 41-32
ip slb probe status 41-33
ip slb probe send 41-34
ip slb probe expect 41-35
show ip slb 41-36
show ip slb clusters 41-38
show ip slb cluster 41-40
show ip slb cluster server 41-43
show ip slb servers 41-46
show ip slb probes 41-48

Chapter 42 High Availability VLAN Commands 42-1
vlan port-mac ingress-port 42-2
vlan port-mac egress-port 42-4
mac-address-table port-mac vlan mac 42-6
vlan port-mac bandwidth 42-8
show mac-address-table port-mac 42-9

Chapter 43 AAA Commands 43-1
aaa radius-server 43-3
aaa ldap-server 43-5
aaa ace-server clear 43-8
aaa authentication vlan single-mode 43-9
aaa authentication vlan multiple-mode 43-11
aaa vlan no 43-13
aaa avlan dns 43-14
aaa avlan default dhcp 43-15
aaa authentication 43-16
aaa authentication default 43-18
aaa authentication 802.1x 43-20
aaa authentication mac 43-22
aaa accounting 802.1x 43-24
aaa accounting vlan 43-26
aaa accounting session 43-28
avlan default-traffic 43-30
avlan port-bound 43-32
avlan auth-ip 43-34
aaa avlan http language 43-35
user 43-36
password 43-40
user password-size min 43-42
user password-expiration 43-43
end-user profile 43-45
end-user profile port-list 43-47
end-user profile vlan-range 43-49
show aaa server 43-51
show aaa authentication vlan 43-54
show aaa authentication 43-56
show aaa authentication 802.1x 43-58
show aaa authentication mac 43-60
show aaa accounting 802.1x 43-61
show aaa accounting vlan 43-62
show aaa accounting 43-64
show user 43-66
show user password-size 43-69
show user password-expiration 43-70
show avlan user 43-71
show aaa avlan config 43-73
show aaa avlan auth-ip 43-75
debug command-info 43-77
debug end-user profile 43-79
show end-user profile 43-81
show aaa priv hexa 43-83

Chapter 44 802.1X Commands 44-1
802.1x 44-2
802.1x initialize 44-5
802.1x re-authenticate 44-6
802.1x supp-polling retry 44-7
802.1x supplicant policy authentication 44-8
802.1x non-supplicant policy authentication 44-10
802.1x non-supplicant policy 44-12
802.1x policy default 44-14
show 802.1x 44-16
show 802.1x users 44-19
show 802.1x statistics 44-21
show 802.1x device classification policies 44-23
show 802.1x non-supp 44-25

Chapter 45 Memory Monitoring Commands 45-1
debug ktrace 45-2
debug ktrace appid level 45-4
debug ktrace show 45-6
debug ktrace show log 45-8
debug systrace 45-10
debug systrace watch 45-12
debug systrace appid level 45-13
debug systrace show 45-15
debug systrace show log 45-17
show log pmd 45-19
debug memory monitor 45-23
debug memory monitor show log 45-24
debug memory monitor show log global 45-27
debug memory monitor show log task 45-29
debug memory monitor show log size 45-31

Chapter 46 Switch Logging Commands 46-1
swlog 46-2
swlog appid level 46-3
swlog output 46-6
swlog output flash file-size 46-8
swlog clear 46-9
show log swlog 46-10
show swlog 46-13

Appendix A Software License and Copyright Statements A-1

Alcatel License Agreement A-1
ALCATEL INTERNETWORKING, INC. (“AII”)
SOFTWARE LICENSE AGREEMENT A-1

Third Party Licenses and Notices A-4
A. Booting and Debugging Non-Proprietary Software A-4
B. The OpenLDAP Public License: Version 2.4, 8 December 2000 ..... A-4
C. Linux A-5
D. GNU GENERAL PUBLIC LICENSE: Version 2, June 1991 ..... A-5
E. University of California A-10

F. Carnegie-Mellon University A-10
G. Random.c A-10
H. Apptitude, Inc. A-11
I. Agranat A-11
J. RSA Security Inc. A-11
K. Sun Microsystems, Inc. A-11
L. Wind River Systems, Inc. A-12
M. Network Time Protocol Version 4 ..... A-12

CLI Quick Reference

Index Index-1

About This Guide

This *OmniSwitch CLI Reference Guide* is a comprehensive resource to all Command Line Interface (CLI) commands available on the OmniSwitch 6600 Family, OmniSwitch 7700/7800, and the OmniSwitch 8800.

Supported Platforms

This information in this guide applies to the following products:

- OmniSwitch 6624
- OmniSwitch 6648
- OmniSwitch 6600-U24
- OmniSwitch 6600-P24
- OmniSwitch 6602-24
- OmniSwitch 6602-48
- OmniSwitch 7700
- OmniSwitch 7800
- OmniSwitch 8800

Note. All references to OmniSwitch 6624 and 6648 switches also apply to the OmniSwitch 6600-U24, 6600-P24, 6602-24, and 6602-48 unless specified otherwise.

Unsupported Platforms

The information in this guide does not apply to the following products:

- OmniSwitch (original version with no numeric model name)
- OmniSwitch 6800-24
- OmniSwitch 6800-48
- OmniSwitch 6800-U24
- OmniSwitch 6800-24L
- OmniSwitch 6800-48L
- OmniSwitch 6850
- OmniSwitch 9700
- Omni Switch/Router
- OmniStack
- OmniAccess

Who Should Read this Manual?

The audience for this user guide is network administrators and IT support personnel who need to configure, maintain, and monitor switches and routers in a live network. Anyone wishing to gain knowledge on the details of all CLI commands available on the OmniSwitch will benefit from the material in this reference guide. However, advanced users who have already familiarized themselves with the OmniSwitch CLI commands will benefit most from the detailed content in this guide.

When Should I Read this Manual?

Read this guide whenever you want detailed information on individual CLI commands. Although this guide provides helpful information during any stage of the configuration process, it is a good idea to first familiarize yourself with the software features available on the switch before investigating the detailed command information in this guide.

Overview information, procedures, and live network examples on switch software features may be found in the *OmniSwitch 6600 Family Switch Management Guide*, *OmniSwitch 7700/7800/8800 Switch Management Guide*, *OmniSwitch 6600 Family Network Configuration Guide*, *OmniSwitch 7700/7800/8800 Network Configuration Guide*, *OmniSwitch 6600 Family Advanced Routing Configuration Guide*, and the *OmniSwitch 7700/7800/8800 Advanced Routing Configuration Guide*. Once you are familiar with the procedures and base CLI commands in these configuration guides you can obtain more detailed information on the individual commands in this guide.

Note. The *OmniSwitch 6600 Family Switch Management Guide, the OmniSwitch 6600 Family Network Configuration Guide, and the OmniSwitch 6600 Family Advanced Routing Configuration Guide* were originally known as the "*OmniSwitch 6624/6648 Switch Management Guide*", the "*OmniSwitch 6624/6648 Network Configuration Guide*", and "*OmniSwitch 6624/6648 Advanced Routing Configuration Guide*", respectively.

What is in this Manual?

This reference guide includes information on every CLI command available in the switch. Command reference information is included for base software commands as well as commands associated with optional software packages, such as Advanced Routing (multicast routing protocols and OSPF). The information provided for each CLI command includes:

- Command description.
- Syntax.
- Description of all keywords and variables included in the syntax.
- Default values.
- Usage guidelines, which include tips on when and how to use the command.
- Examples of command lines using the command.
- Related commands with descriptions.
- Release history, which indicates the release when the command was introduced.
- SNMP information, such as the MIB files related to a set of CLI commands. In addition each CLI command includes the corresponding MIB variables that map to all parameters included in a command.

What is Not in this Manual?

Primarily a reference, this guide does not provide step-by-step instructions on how to set up particular features on the switch. It also does not provide overview or application examples on software features. For comprehensive information on how to configure particular software features in the switch, consult the appropriate configuration guide.

This guide also does not provide any information on the network management applications, WebView and OmniVista. Further information on WebView and OmniVista can be found in the context-sensitive on-line help available with those applications.

How is the Information Organized?

Each chapter in this guide includes reference material for all commands related to a single software feature, such as server load balancing or link aggregation. Typically commands in a single chapter will share a common prefix.

Text Conventions

The following table contains text conventions and usage guidelines for CLI commands as they are documented in this guide.

bold text	Indicates basic command and keyword syntax. Example: **show snmp station**
italicized text	Indicates user-specific information such as IP addresses, slot numbers, passwords, names, etc. Example: **no snmp station** *ip_address* Italicized text that is not enclosed with straight brackets (**[ ]**) indicates required information.
[ ] (Straight Brackets)	Indicates optional parameters for a given command. Example: **show aaa server [***server_name***]** Here, you can enter either of the following options: **show aaa server** **show aaa server** *server_name* (where *server_name* is the user-specified server name, e.g., **show aaa server myserver1**) Note that this example includes *italicized text*. The optional parameter in this case is a user-specified server name.
{ } (Curly Braces)	Indicates that the user must choose between one or more parameters. Example: **port mirroring {enable | disable}** Here, you must choose one of the following: **port mirroring enable** or **port mirroring disable**
| (Vertical Pipes)	Used to separate parameter choices within a command string. For example, the command string **show health threshold [rx | txrx | memory | cpu]** separates the choices **rx**, **txrx**, **memory,** and **cpu**. Examples: **show health threshold rx** **show health threshold txrx** **show health threshold memory** **show health threshold cpu**
“ ” (Quotation Marks)	Used to enclose text strings that contain spaces. The quotation marks are required input on the command line. Example: **vlan 2 “new test vlan”**

Documentation Roadmap

The OmniSwitch user documentation suite was designed to supply you with information at several critical junctures of the configuration process. The following section outlines a roadmap of the manuals that will help you at each stage of the configuration process. Under each stage, we point you to the manual or manuals that will be most helpful to you.

Stage 1: Using the Switch for the First Time

Pertinent Documentation: *Getting Started Guide*
Release Notes

A hard-copy *Getting Started Guide* is included with your switch; this guide provides all the information you need to get your switch up and running the first time. This guide provides information on unpacking the switch, rack mounting the switch, installing modules, unlocking access control, setting the switch's IP address, and setting up a password. It also includes succinct overview information on fundamental aspects of the switch, such as hardware LEDs, the software directory structure, CLI conventions, and web-based management.

At this time you should also familiarize yourself with the Release Notes that accompanied your switch. This document includes important information on feature limitations that are not included in other user guides.

Stage 2: Gaining Familiarity with Basic Switch Functions

Pertinent Documentation: *Hardware Users Guide*
Switch Management Guide

Once you have your switch up and running, you will want to begin investigating basic aspects of its hard ware and software. Information about switch hardware is provided in the platform-specific *Hardware Users Guide*. This guide provide specifications, illustrations, and descriptions of all hardware components—chassis, power supplies, Chassis Management Modules (CMMs), Network Interface (NI) modules, uplink modules, stacking modules, and cooling fans. It also includes steps for common procedures, such as removing and installing switch components.

The *Switch Management Guide* for your switch platform is the primary user guide for the basic software features on a single switch. This guide contains information on the switch directory structure, basic file and directory utilities, switch access security, SNMP, and web-based management. It is recommended that you read this guide before connecting your switch to the network.

Stage 3: Integrating the Switch Into a Network

Pertinent Documentation: *Network Configuration Guide*
Advanced Routing Configuration Guide

When you are ready to connect your switch to the network, you will need to learn how the OmniSwitch implements fundamental software features, such as 802.1Q, VLANs, Spanning Tree, and network routing protocols. The *Network Configuration Guide* for your switch platform contains overview information, procedures and examples on how standard networking technologies are configured in the OmniSwitch.

The *Advanced Routing Configuration Guide* includes configuration information for networks using advanced routing technologies, such as OSPF and multicast routing protocols (DVMRP and PIM-SM).

Anytime

The *OmniSwitch CLI Reference Guide* contains comprehensive information on all CLI commands supported by the switch. This guide includes syntax, default, usage, example, related CLI command, and CLI-to-MIB variable mapping information for all CLI commands supported by the switch. This guide can be consulted anytime during the configuration process to find detailed and specific information on each CLI command.

Related Documentation

The following are the titles and descriptions of all the next-generation OmniSwitch user manuals:

- *OmniSwitch 6600 Family Getting Started Guide*

  Describes the hardware and software procedures for getting an OmniSwitch 6600 Family switch up and running. Also provides information on fundamental aspects of OmniSwitch software and stacking architecture.

- *OmniSwitch 7700/7800 Getting Started Guide*

  Describes the hardware and software procedures for getting an OmniSwitch 7700 or 7800 up and running. Also provides information on fundamental aspects of OmniSwitch software architecture.

- *OmniSwitch 8800 Getting Started Guide*

  Describes the hardware and software procedures for getting an OmniSwitch 8800 up and running. Also provides information on fundamental aspects of OmniSwitch software architecture.

- *OmniSwitch 6600 Family Hardware Users Guide*

  Complete technical specifications and procedures for all OmniSwitch 6600 Family chassis, power supplies, fans, uplink modules, and stacking modules.

- *OmniSwitch 7700/7800 Hardware Users Guide*

  Complete technical specifications and procedures for all OmniSwitch 7700 and 7800 chassis, power supplies, fans, and Network Interface (NI) modules.

- *OmniSwitch 8800 Hardware Users Guide*

  Complete technical specifications and procedures for all OmniSwitch 8800 chassis, power supplies, fans, and Network Interface (NI) modules.

- *OmniSwitch CLI Reference Guide*

  Complete reference to all CLI commands supported on the OmniSwitch 6600, 7700/7800, and 8800. Includes syntax definitions, default values, examples, usage guidelines and CLI-to-MIB variable mappings.

- *OmniSwitch 6600 Family Switch Management Guide*

  Includes procedures for readying an individual switch for integration into a network. Topics include the software directory architecture, image rollback protections, authenticated switch access, managing switch files, system configuration, using SNMP, and using web management software (WebView).

Note. The *OmniSwitch 6600 Family Switch Management Guide* was originally known as the "*OmniSwitch 6624/6648 Switch Management Guide*."

- *OmniSwitch 7700/7800/8800 Switch Management Guide*

  Includes procedures for readying an individual switch for integration into a network. Topics include the software directory architecture, image rollback protections, authenticated switch access, managing switch files, system configuration, using SNMP, and using web management software (WebView).

- *OmniSwitch 6600 Family Network Configuration Guide*

  Includes network configuration procedures and descriptive information on all the major software features and protocols included in the base software package. Chapters cover Layer 2 information (Ethernet and VLAN configuration), Layer 3 information (RIP and static routes), security options (authenticated VLANs), Quality of Service (QoS), and link aggregation.

Note. The *OmniSwitch 6600 Family Network Configuration Guide* was originally known as the "*OmniSwitch 6624/6648 Network Configuration Guide*."

- *OmniSwitch 7700/7800/8800 Network Configuration Guide*

  Includes network configuration procedures and descriptive information on all the major software features and protocols included in the base software package. Chapters cover Layer 2 information (Ethernet and VLAN configuration), Layer 3 information (routing protocols, such as RIP and IPX), security options (authenticated VLANs), Quality of Service (QoS), link aggregation, and server load balancing.

- *OmniSwitch 6600 Family Advanced Routing Configuration Guide*

  Includes network configuration procedures and descriptive information on the software features and included in the advanced routing software package (OSPF).

Note. The *OmniSwitch 6600 Family Advanced Routing Configuration Guide* was originally known as the "*OmniSwitch 6624/6648 Advanced Routing Configuration Guide*"

- *OmniSwitch 7700/7800/8800 Advanced Routing Configuration Guide*

  Includes network configuration procedures and descriptive information on all the software features and protocols included in the advanced routing software package. Chapters cover multicast routing (DVMRP and PIM-SM) OSPF, and BGP.

- Technical Tips, Field Notices

  Includes information published by Alcatel's Customer Support group.

- *Release Notes*

  Includes critical Open Problem Reports, feature exceptions, and other important information on the features supported in the current release and any limitations to their support.

User Manuals Web Site

All related user guides for the OmniSwitch 6600 Family, OmniSwitch 7700/7800, and OmniSwitch 8800 can be found on our web site at
http://www.alcatel.com/enterprise/en/resource_library/user_manuals.html

All documentation on the User Manual web site is in PDF format and requires the Adobe Acrobat Reader program for viewing. Acrobat Reader freeware is available at www.adobe.com.

Note. When printing pages from the documentation PDFs, de-select Fit to Page if it is selected in your print dialog. Otherwise pages may print with slightly smaller margins.

Technical Support

An Alcatel service agreement brings your company the assurance of 7x24 no-excuses technical support. You'll also receive regular software updates to maintain and maximize your Alcatel product's features and functionality and on-site hardware replacement through our global network of highly qualified service delivery partners. Additionally, with 24-hour-a-day access to Alcatel's Service and Support web page, you'll be able to view and update any case (open or closed) that you have reported to Alcatel's technical support, open a new case or access helpful release notes, technical bulletins, and manuals. For more information on Alcatel's Service Programs, see our web page at eservice.ind.alcatel.com, call us at 1-800-995-2696, or email us at support@ind.alcatel.com.

1 CMM Commands

The Chassis Management Module (CMM) CLI commands allow you to manage switch software files in the working directory, the certified directory, and the running configuration.

MIB information for the CMM commands is as follows:

Filename: AlcatelIND1Chassis.mib
Module: ALCATEL-IND1-CHASSIS-MIB

A summary of available commands is listed here:

reload
reload working
copy running-config working
write memory
copy certified working
copy working certified
copy flash-synchro
takeover
debug chassis auto-reboot
show running-directory
show reload
show microcode
show microcode history

reload

Reboots the CMM to its startup software configuration.

reload [primary | secondary] [in [*hours***:] *minutes* | at *hour*:*minute* [*month day* | *day month*]]**

reload [primary | secondary] cancel

Syntax Definitions

primary | secondary	Reboot the primary or secondary CMM to its startup software configuration. If the primary CMM is already running the startup version, a primary reboot will result in a secondary takover.
in [*hours***:]** *minutes*	Optional syntax. Schedules a reload of the software to take effect in the specified minutes or hours and minutes within the next 24 hours.
at *hour*:*minute*	Optional syntax. Schedules a reload of the software to take place at the specified time using a 24-hour clock. If you do not specify the month and day, the reload takes place at the specified time on the current day provided the specified time is later than the time when the CLI command is issues. If the specified time is earlier than the current time, the reload will take place on the following day.
month day | *day month*	The name of the month and the number of the day for the scheduled reload. Specify a month name and the day number. It is unimportant if the month or day is first. See examples below for further explanation.
cancel	Cancels a pending time delayed reboot.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command causes the specified CMM to reboot. If no CMM is specified, the primary CMM reboots.
- If a reload command is issued, and another reload is currently scheduled, a message appears informing the user of the next reload time and asks for confirmation to change to the new reload time.
- If the switch has a redundant CMM and the primary CMM is rebooted, the switch will fail over to the secondary CMM. For more information on CMM failover, see “Managing CMM Directories” in the *OmniSwitch 6600 Family Switch Management Guide* or *OmniSwitch 7700/7800/8800 Switch Management Guide*.
- If the switch is part of an OmniSwitch 6600 Family stack with three or more switches, the next switch in “idle” mode becomes the secondary CMM, and the original primary CMM becomes “idle.” For more information on stacks, see “Managing Stacks” in the *OmniSwitch 6600 Family Hardware Users Guide*.

- The **cancel** keyword stops a pending reboot.
- This command can also be used on the secondary CMM.

Examples

```
-> reload
-> reload primary
-> reload primary in 15:25
-> reload primary at 15:25 february 10
-> reload primary at 15:25 10 february
```

Release History

Release 5.1; command was introduced.

Related Commands

reload working	Immediate primary CMM reboot to the working software configuration without secondary CMM takeover.

MIB Objects

```
chasEntPhysicalTable
   csEntPhysicalIndex
   chasEntPhysAdminStatus
chasControlRedundantTable
   chasControlDelayedRebootTimer
```

reload working

Immediately reboots the primary CMM from the working directory. There is no CMM fail over during this reboot, causing a loss of switch functionality during the reboot. All NIs reboot as well, including the secondary CMM.

reload working {rollback-timeout *minutes* | **no rollback-timeout} [in [***hours***:]** *minutes* **| at** *hour***:***minute***]**

Syntax Definitions

rollback-timeout *minutes*	Sets a timeout period, in minutes. At the end of this time, the switch automatically reboots from the certified directory. The range is 1–15.
no rollback-timeout	Specifies no timeout to rollback. If the command is issued with this keyword, then the switch will continue to run from the working directory until manually rebooted.
in [*hours***:]** *minutes*	Optional syntax. Schedules a reload of the working directory to take effect in the specified minutes or hours and minutes within the next 24 hours.
at *hour***:***minute*	Optional syntax. Schedules a reload of the working directory to take place at the specified time using a 24-hour clock. If you do not specify the month and day, the reload takes place at the specified time on the current day provided the specified time is later than the time when the CLI command is issues. If the specified time is earlier than the current time, the reload will take place on the following day.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command is used to reload the primary CMM from the working directory as opposed to the certified CMM. The working directory reload takes place immediately unless a time frame is set using the **in** or **at** keywords.
- The **in** or **at** keywords allow you to schedule a working reload sometime in the future. A schedule working reboot is called an **activate**.
- If a reload or an immediate working reload is initiated before a scheduled activate is enacted, a message appears displaying the number of seconds until the scheduled activate and if it should be overrided.
- If a timeout is set, the switch reboots again after the set number of minutes, from the certified directory. The reboot can be halted by issuing a cancel order as described in the **reload** command.

- If the switch is a part of an OmniSwitch 6600 Family stack, using this command synchronizes the working directories of all the switches in the stack to the working directory of the primary CMM switch.

Examples

```
-> reload working rollback-timeout 5
-> reload working no rollback-timeout
-> reload working no rollback-timeout in 50
-> reload working rollback-timeout 10 at 12:50
```

Release History

Release 5.1; command was introduced.

Related Commands

reload	Reboots the CMM to its startup software configuration.

MIB Objects

```
chasControlModuleTable
   csEntPhysicalIndex
   chasControlActivateTimeout
```

copy running-config working

Copies the running configuration (RAM) to the working directory.

[configure] copy running-config working

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command is used to copy the changes made using the CLI commands from the running configuration (RAM) to the working directory.
- This command is only valid if the switch is running from the working directory. Use the **show running-directory** command to check from where the switch is running.
- This command performs the same function as the **write memory** command.

Note. The saved **boot.cfg** file will be overwritten if the **takeover** command is executed after the **copy running-config working** or **write memory** commands, in an OmniSwitch set up with redundant CMMs.

Examples

```
-> configure copy running-config working
```

Release History

Release 5.1; command was introduced.

Related Commands

write memory	Copy the running primary RAM version of the CMM software to the working primary flash.
copy flash-synchro	Copy the startup primary flash version of the CMM software to the startup secondary flash version of the CMM software.

MIB Objects

```
chasControlModuleTable
   csEntPhysicalIndex
   chasControlVersionMngt
```

write memory

Copies the running configuration (RAM) to the working directory.

[configure] write memory

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command is used to copy the changes made using the CLI commands from the running configuration (RAM) to the working directory.
- This command is only valid if the switch is running from the working directory. Use the **show running-directory** command to check from where the switch is running.
- This command performs the same function as the **copy running-config working** command.

Note. The saved **boot.cfg** file will be overwritten if the **takeover** command is executed after the **copy running-config working** or **write memory** commands, in an OmniSwitch set up with redundant CMMs.

Examples

```
-> configure write memory
-> write memory
```

Release History

Release 5.1; command was introduced.

Related Commands

copy running-config working	Copy the running primary RAM version of the CMM software to the working primary flash. Or copy the startup primary flash version of the CMM software to the working primary flash.
copy flash-synchro	Copy the startup primary flash version of the CMM software to the startup secondary flash version of the CMM software.

MIB Objects

```
CONFIGMANAGER
   configWriteMemory
```

copy certified working

Copies the certified directory version of the CMM software to the working directory, on the primary CMM.

[configure] copy certified working

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command is used to overwrite the contents of the working directory with the contents of the certified directory.
- In order for this command to work, the amount of free space in flash must equal the size of the files being copied. If there isn't enough free space, the copy attempt will fail and an error message is generated. Only image files, the boot.cfg file, and the certs.pem file should be kept in the certified directory.

Examples

```
-> copy certified working
```

Release History

Release 5.1; command was introduced.

Related Commands

copy certified working	Copy the running primary RAM version of the CMM software to the working primary flash. Or copy the startup primary flash version of the CMM software to the working primary flash.
copy flash-synchro	Copy the startup primary flash version of the CMM software to the startup secondary flash version of the CMM software.

MIB Objects

```
chasControlModuleTable
   csEntPhysicalIndex
   chasControlVersionMngt
```

copy working certified

Copies the working directory version of the CMM software to the certified directory, on the primary CMM. This command also allows you to synchronize the primary and secondary CMMs.

[configure] copy working certified [flash-synchro]

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command is used to overwrite the contents of the certified directory with the contents of the working directory. This should only be done if the contents of the working directory have been verified as the best version of the CMM files.
- The **flash-synchro** keyword, when used with the **copy certified working** command, synchronizes the files between the primary and secondary CMMs by overwriting the contents of the secondary CMM certified directory with the contents of the primary CMM certified directory. If the switch is part of an OmniSwitch 6600 Family stack, all switches in the stack are updated with the primary CMM files.
- In order for this command to work, the amount of free space in flash must equal the size of the files being copied. If there isn't enough free space, the copy attempt will fail and an error message is generated. Only image files, the boot.cfg file, and the certs.pem file should be kept in the working directory.
- This command will not work if the switch is running from the certified directory. To view where the switch is running from, see the **show running-directory** command.

Examples

```
-> copy working certified
-> copy working certified flash-synchro
```

Release History

Release 5.1; command was introduced.

Related Commands

copy certified working	Copy the running primary RAM version of the CMM software to the working primary flash. Or copy the startup primary flash version of the CMM software to the working primary flash.
copy flash-synchro	Copy the startup primary flash version of the CMM software to the startup secondary flash version of the CMM software.

MIB Objects

```
chasControlModuleTable
   csEntPhysicalIndex
   chasControlVersionMngt
```

copy flash-synchro

Copies the certified directory version of the primary CMM software to the certified directory of the secondary CMM.

[configure] copy flash-synchro

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command is used to synchronize the certified directories of the primary and secondary CMMs. The two CMMs must be in synchronization if a fail over occurs, otherwise switch performance is lost.
- If the switch is part of an OmniSwitch 6600 Family stack, all switches in the stack are updated with the primary CMM files.

Examples

```
-> copy flash-synchro
-> configure copy flash-synchro
```

Release History

Release 5.1; command was introduced.

Related Commands

copy certified working	Copy the running primary RAM version of the CMM software to the working primary flash. Or copy the startup primary flash version of the CMM software to the working primary flash.
copy working certified	Copy the working primary flash version of the CMM software to certified primary flash. Or copy the working primary flash version of the CMM software to startup secondary flash.

MIB Objects

```
chasControlModuleTable
   csEntPhysicalIndex
   chasControlVersionMngt
```

takeover

The current secondary CMM assumes the role of primary CMM.

takeover

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command causes the secondary CMM to take over the functions of the primary CMM. After this command, the old primary CMM is the new secondary CMM.
- Before issuing the **takeover** command, be sure that the secondary CMM has all software (i.e., image and configuration files) required to continue CMM operations.
- For information on synchronizing the primary and secondary CMM software before issuing the **takeover** command, see the **copy flash-synchro** command.
- When the CMM modules switch primary and secondary roles, the console session to the new primary CMM will be disconnected. To continue managing the switch, be sure that you have physical connections to both CMMs *or* local access to the switch in order to move your Ethernet or serial cable from one CMM to the other.
- This command can also be used on the secondary CMM.
- If the switch is part of an OmniSwitch 6600 Family stack with three or more switches, the next switch in "idle" mode becomes the secondary CMM, and the original primary CMM becomes "idle." For more information on stacks, see "Managing Stacks" in the *OmniSwitch 6600 Family Hardware Users Guide*.

Note. The saved **boot.cfg** file will be overwritten if the **takeover** command is executed after the **copy running-config working** or **write memory** commands, in an OmniSwitch set up with redundant CMMs. Refer to the "NIs Reload On Takeover" description on page 1-19 for more information on the **takeover** command and redundant management modules.

Examples

```
-> takeover
```

Release History

Release 5.1; command was introduced.

Related Command

reload	Reboots the CMM to its startup software configuration.

MIB Objects

```
chasEntPhysicalTable
   csEntPhysicalIndex
   chasEntPhysAdminStatus
```

debug chassis auto-reboot

Enables or disables automatic reboot of the CMM if a task failure is detected.

debug chassis auto-reboot {enable | disable}

Syntax Definitions

enable | disable Enables or disables chassis reboot debugging.

Defaults

parameter	value
enable | disable	**enable**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Chassis Supervision constantly monitors CMM tasks and reboots if any one task fails. If debug chassis auto-reboot is set to **disable**, Chassis Supervision will not monitor tasks, so there will be no automatic reboots.
- This command can also be used on the secondary CMM.

Examples

```
-> debug chassis auto-reboot enable
```

Release History

Release 5.1; command was introduced.

Related Commands

N/A

MIB Objects

N/A

show running-directory

Shows the directory from where the switch was booted.

show running-directory

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Once a switch has booted and is running, it will run either from the working or certified directory. If running from the certified, changes made to the running configuration using CLI commands cannot be saved. A switch must be running from the working directory in order to save the current running configuration.
- This command can also be used on the secondary CMM.

Examples

The following is an example of the display on OmniSwitch 7700/7800/8800 switches:

```
-> show running-directory

CONFIGURATION STATUS
   Running CMM              : PRIMARY,
   CMM Mode                 : MONO CMM,
   Current CMM Slot         : A,
   Running configuration    : WORKING,
   Certify/Restore Status   : CERTIFY NEEDED
SYNCHRONIZATION STATUS
   Running Configuration    : SYNCHRONIZED,
   NIs Reload On Takeover   : NONE
```

The following is an example of the display on OmniSwitch 6600 Family switches:

```
-> show running-directory

CONFIGURATION STATUS
   Running CMM              : PRIMARY,
   CMM Mode                 : DUAL CMMs,
   Current CMM Slot         : 1,
   Running configuration    : WORKING,
   Certify/Restore Status   : CERTIFY NEEDED
SYNCHRONIZATION STATUS
   Flash Between CMMs       : SYNCHRONIZED,
   Running Configuration    : NOT AVAILABLE,
   Stacks Reload on Takeover: ALL STACKs (SW Activation)
```

output definitions

Running CMM	The CMM currently controlling the switch, either PRIMARY or SECONDARY.
CMM Mode	Displays whether the primary and secondary CMMs are synchronized. In the case that there is no secondary CMM, MONO-CMM-CHASSIS is shown.
Current CMM Slot	The slot number of the primary CMM.
Running Configuration	Where the switch is running from, either WORKING or CERTIFIED. A switch running from the certified directory will not be able to manipulate files in the directory structure.
Certify/Restore Status	Indicates if the CM has been certified (i.e., the Working directory matches the Certified directory).

output definitions (continued)

Flash Between CMMs	Displays whether the Working and Certified directories are the same.
NIs Reload On Takeover **Stacks Reload on Takeover**	Displays how many Network Interface (NI) modules or switches in a stack will be reloaded in the event of a management module takeover. Options include NONE, ALL, or a list of specific NIs. If there are *no* unsaved configuration changes *and* the flash directories on both the primary and secondary management modules have been synchronized via the **copy flash-synchro** command, no NIs will be reloaded if a management module takeover occurs. As a result, data flow is not interrupted on the NIs during the takeover. If a configuration change is made to one or more NI modules (e.g., a VLAN is configured on several different interfaces), and *the changes are not saved via the* **write memory** command, the corresponding NIs will automatically reload if a management module takeover occurs. Data flow on the affected NIs will be interrupted until the reload is complete. Note that the NIs will reload whether or not the flash synchronization status shows SYNCHRONIZED. This is because the unsaved changes have occurred in the running configuration (i.e., RAM), and have not been written to the flash directory's configuration file. In this case, a list of only the affected NIs displays in the table output (e.g., 1 6 9 12). If the flash directories on the primary and secondary management modules are *not synchronized* (e.g., a **copy flash-synchro** command has not been issued recently), all NIs will be reloaded automatically if a management module takeover occurs. Data flow will be interrupted on all NIs until the reload is complete.

Release History

Release 5.1; command was introduced.

Related Commands

reload	Reboots the CMM to its startup software configuration.
write memory	Copies the running configuration (RAM) to the working directory.
copy flash-synchro	Copies the certified directory version of the primary CMM software to the certified directory of the secondary CMM.

MIB Objects

```
chasControlModuleTable
   chasControlRunningVersion
   chasControlActivateTimeout
   chasControlVersionMngt
   chasControlDelayedActivateTimer
   chasControlCertifyStatus
   chasControlSynchronizationStatus
```

show reload

Shows the status of any time delayed reboot(s) that are pending on the switch.

show reload [status]

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- It is possible to preset a reboot on a CMM, using the **reload** command. If this is done, use the **show reload** command to see when the next scheduled reboot will occur.
- If the **reload working** command was used an a rollback timeout was set, the time the rollback will occur is shown using the **show reload** command.
- This command can also be used on the secondary CMM.

Examples

```
-> show reload status
Primary   Control Module Reload Status: No Reboot Scheduled,
Secondary Control Module Reload Status: No Reboot Scheduled
```

Release History

Release 5.1; command was introduced.

Related Commands

reload	Reboots the primary or secondary CMM to its startup software configuration.
reload working	Immediate primary CMM reboot to the working software configuration without secondary CMM takeover.

MIB Objects

N/A

show microcode

Displays microcode versions installed on the switch.

show microcode [working | certified | loaded]

Syntax Definitions

working	Specifies the switch's working directory; only microcode information from the working directory will be displayed.
certified	Specifies the switch's certified directory; only microcode information from the certified directory will be displayed.
loaded	Specifies that only loaded (i.e., currently-active) microcode versions will be displayed. Idle microcode versions will not be displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If no additional parameters are entered (i.e., **working**, **certified**, or **loaded**), microcode information for the running configuration will be displayed.
- This command can also be used on the secondary CMM.

Examples

```
-> show microcode
Package           Release       Size     Description
-----------------+--------------+--------+---------------------------------
Fadvrout.img      5.4.1.220.R01     987422 Alcatel Advanced Routing
Fbase.img         5.4.1.220.R01    4361627 Alcatel Base Software
Fdiag.img         5.4.1.220.R01     331512 Alcatel Diagnostics Archive
Feni.img          5.4.1.220.R01    1318201 Alcatel NI Software
Fl2eth.img        5.4.1.220.R01     990680 Alcatel Layer 2, Ethernet
Fos.img           5.4.1.220.R01    1498254 Alcatel Operating System
Fqos.img          5.4.1.220.R01     314202 Alcatel Quality of Service
Frout.img         5.4.1.220.R01     769341 Alcatel Routing
Fsecu.img         5.4.1.220.R01     129799 Alcatel Security
Fweb.img          5.4.1.220.R01    1472235 Alcatel Webview - Main
Fwebadvrout.img   5.4.1.220.R01     251953 Alcatel Webview - Advanced Routing
Fwebl2eth.img     5.4.1.220.R01     330897 Alcatel Webview - Layer 2 and Ethern
Fwebqos.img       5.4.1.220.R01     263716 Alcatel Webview - Quality of Service
Fwebrout.img      5.4.1.220.R01     350634 Alcatel Webview - Routing
Fwebsecu.img      5.4.1.220.R01     212658 Alcatel Webview - Security
```

output definitions

Package	File name.
Release	Version number.
Size	File size.
Description	File description.

Release History

Release 5.1; command was introduced.

Related Commands

show microcode history	Displays the archive history for microcode versions installed on the switch.

MIB Objects

N/A

show microcode history

Displays the archive history for microcode versions installed on the switch.

show microcode history [working | certified]

Syntax Definitions

working	The history for the working directory's microcode will be displayed.
certified	The history for the certified directory's microcode will be displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

If no additional parameters are entered (i.e., **working** or **certified**), the microcode history for the running directory will be displayed.

Examples

```
-> show microcode history
Archive Created 1/1/06 6:49:34
```

Release History

Release 5.1; command was introduced.

Related Commands

show microcode	Displays microcode versions installed on the switch.

MIB Objects

N/A

2 Chassis Management and Monitoring Commands

Chassis Management and Monitoring commands allow you to configure and view hardware-related operations on the switch. Topics include basic system information, as well as Network Interface (NI) module- and chassis management.

Additional Information. Refer to your separate *Hardware User Guide* for detailed information on chassis components, as well as managing and monitoring hardware-related functions.

MIB information for the Chassis Management and Monitoring commands is as follows:

Filename: AlcatelIND1Chassis.mib
Module: ALCATEL-IND1-CHASSIS-MIB

Filename: AlcatelIND1System.MIB
Module: ALCATEL-IND1-SYSTEM-MIB

Filename: AlcatelIND1StackManager.MIB
Module: ALCATEL-IND1-STACK-MANAGER-MIB

Note. The Stack Manager MIB is applicable only to OmniSwitch 6600 Family switches.

A summary of available commands is listed here:

Management Commands	**system contact** **system name** **system location** **system date** **system time** **system time-and-date synchro** **system timezone** **system daylight savings time** **reload ni** **reload all** **power ni** **temp-threshold** **fabric standby** **power fabric**
Monitoring Commands	**fabric standby** **show system** **show hardware info** **show chassis** **show cmm** **show ni** **show module** **show module long** **show module status** **show power** **show fan** **show temperature** **show stack topology** **show fabric**

system contact

Specifies the switch's administrative contact. An administrative contact is the person or department in charge of the switch. If a contact is specified, users can easily find the appropriate network administrator if they have questions or comments about the switch.

system contact *text_string*

Syntax Definitions

text_string	The administrative contact being specified for the switch. The system contact can range from 1 to 254 characters in length. Text strings that include spaces must be enclosed in quotation marks. For example, **"Jean Smith Ext. 477 jsmith@company.com"**.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> system contact "Jean Smith Ext. 477 jsmith@company.com"
-> system contact engineering-test@company.com
```

Release History

Release 5.1; command was introduced.

Related Commands

system name	Modifies the switch's current system name.
system location	Specifies the switch's current physical location.
fabric standby	Displays basic system information for the switch.

MIB Objects

```
system
   systemContact
```

system name

Modifies the switch's current system name. The system name can be any simple, user-defined text description for the switch.

system name *text_string*

Syntax Definitions

text_string	The new system name. The system name can range from 1 to 254 characters in length. Text strings that include spaces must be enclosed in quotation marks. For example, **"OmniSwitch 7700"**.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> system name "OmniSwitch 7700"
-> system name OS-7700
```

Release History

Release 5.1; command was introduced.

Related Commands

system contact	Specifies the switch's administrative contact (e.g., an individual or department).
system location	Specifies the switch's current physical location.
fabric standby	Displays basic system information for the switch.

MIB Objects

```
system
   systemName
```

system location

Specifies the switch's current physical location. If you will need to determine the switch's location from a remote site, entering a system location can be very useful.

system location *text_string*

Syntax Definitions

text_string	The switch's physical location. For example, **TestLab**. The system location can range from 1 to 254 characters in length. Text strings that include spaces must be enclosed in quotation marks. For example, **"NMS Test Lab"**.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> system location "NMS Test Lab"
-> system location TestLab
```

Release History

Release 5.1; command was introduced.

Related Commands

system contact	Specifies the switch's administrative contact (e.g., an individual or department).
system name	Modifies the switch's current system name.
fabric standby	Displays basic system information for the switch.

MIB Objects

```
system
   systemLocation
```

system date

Displays or modifies the switch's current system date.

system date [*mm/dd/yyyy***]**

Syntax Definitions

mm/dd/yyyy	The new date being specified for the system. Enter the date in the following format: *mm/dd/yyyy*, where *mm* is the month, *dd* is the day, and *yyyy* is the year. For example, **11/07/2002**.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If you do not specify a new system date in the command line, the current system date will be displayed.
- For more information on setting time zone parameters (e.g., Daylight Savings Time), refer to the **system timezone** command on page 2-9.

Examples

```
-> system date 11/07/2002
-> system date
11/07/2002
```

Release History

Release 5.1; command was introduced.

Related Commands

system time	Displays or modifies the switch's current system time.
system timezone	Displays or modifies the time zone for the switch.

MIB Objects

```
systemServices
   systemServicesDate
```

system time

Displays or modifies the switch's current system time.

system time [*hh:mm:ss***]**

Syntax Definitions

hh:mm:ss	The new time being specified for the system. To set this value, enter the current time in 24-hour format, where *hh* is the hour, *mm* is the minutes, and *ss* is the seconds. For example, **14:30:00**.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

If you do not specify a new system time in the command line, the current system time will be displayed.

Examples

```
-> system time 14:30:00
-> system time
15:48:08
```

Release History

Release 5.1; command was introduced.

Related Commands

system date	Displays or modifies the switch's current system date.
system timezone	Displays or modifies the time zone for the switch.

MIB Objects

```
systemServices
   systemServicesTime
```

system time-and-date synchro

Synchronizes the time and date settings between primary and secondary CMMs.

system time-and-date synchro

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The **system time-and-date synchro** command applies only to switches with redundant CMM configurations.
- Synchronizing date and time settings is an important step in providing effective CMM failover for switches in redundant configurations. Be sure to periodically synchronize the primary and secondary CMMs using this command.
- For detailed redundancy information on OS7700/7800 and OS8800 switches, refer to the "Chassis Management Module (CMM)" chapter in the *Hardware Users Guide*, and "Managing CMM Directory Content" in the *Switch Management Guide*. For OmniSwitch 6600 Family switches, refer to "Managing Stacks" in addition to "Managing CMM Directory Content."

Examples

```
-> system time-and-date synchro
```

Release History

Release 5.1; command was introduced.

Related Commands

copy flash-synchro	Copies the certified directory version of the primary CMM software to the certified directory of the secondary CMM.

MIB Objects

```
systemServices
```

system timezone

Displays or modifies the time zone for the switch.

system timezone [*timezone_abbrev* **|** *offset_value* **|** *time_notation***]**

Syntax Definitions

timezone_abbrev	Specifies a time zone for the switch and sets the system clock to run on UTC. Refer to the table below for a list of supported time zone abbreviations. If you specify a time zone abbreviation, the hours offset from UTC will be automatically calculated by the switch.
offset_value	Specifies the number of hours offset from UTC. Values may range from -13 through +12. The switch automatically enables UTC. However, if you do not want your system clock to run on UTC, simply enter the offset +0 for the system time zone. This sets UTC to run on local time.
time_notation	Specifies a non-integer time-notation offset for areas that are offset from UTC by increments of 15, 30, or 45 minutes (e.g., 05:30).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- To display the current time zone for the switch, enter the syntax **system timezone**.
- When Daylight Saving Time (DST)—also referred to as *summertime*—is enabled, the clock automatically sets up default DST parameters for the local time zone.
- Refer to the table below for a list of supported time zone abbreviations.

Abbreviation	Name	Hours from UTC	DST Start	DST End	DST Change
nzst	New Zealand	+12:00	1st Sunday in Oct. at 2:00 a.m.	3rd Sunday in Mar. at 3:00 a.m.	1:00
zp11	No standard name	+11:00	No default	No default	No default
aest	Australia East	+10:00	Last Sunday in Oct. at 2:00 a.m.	Last Sunday in Mar. at 3:00 a.m.	1:00
gst	Guam	+10:00	No default	No default	No default
acst	Australia Central Time	+09:30	Last Sunday in Oct. at 2:00 a.m.	Last Sunday in Mar. at 3:00 a.m.	1:00
jst	Japan	+09:00	No default	No default	No default
kst	Korea	+09:00	No default	No default	No default
awst	Australia West	+08:00	No default	No default	No default

Abbreviation	Name	Hours from UTC	DST Start	DST End	DST Change
zp8	China; Manila, Philippines	+08:00	No default	No default	No default
zp7	Bangkok	+07:00	No default	No default	No default
zp6	No standard name	+06:00	No default	No default	No default
zp5	No standard name	+05:00	No default	No default	No default
zp4	No standard name	+04:00	No default	No default	No default
msk	Moscow	+03:00	Last Sunday in Mar. at 2:00 a.m.	Last Sunday in Oct. at 3:00 a.m.	1:00
eet	Eastern Europe	+02:00	Last Sunday in Mar. at 2:00 a.m.	Last Sunday in Oct. at 3:00 a.m.	1:00
cet	Central Europe	+01:00	Last Sunday in Mar. at 2:00 a.m.	Last Sunday in Oct. at 3:00 a.m.	1:00
met	Middle Europe	+01:00	Last Sunday in Mar. at 2:00 a.m.	Last Sunday in Oct. at 3:00 a.m.	1:00
bst	British Standard Time	+00:00	Last Sunday in Mar. at 1:00 a.m.	Last Sunday in Oct. at 3:00 a.m.	1:00
wet	Western Europe	+00:00	Last Sunday in Mar. at 1:00 a.m.	Last Sunday in Oct. at 3:00 a.m.	1:00
gmt	Greenwich Mean Time	+00:00	No default	No default	No default
wat	West Africa	-01:00	No default	No default	No default
zm2	No standard name	-02:00	No default	No default	No default
zm3	No standard name	-03:00	No default	No default	No default
nst	Newfoundland	-03:30	1st Sunday in Apr. at 2:00 a.m.	Last Sunday in Oct. at 2:00 a.m.	1:00
ast	Atlantic Standard Time	-04:00	1st Sunday in Apr. at 2:00 a.m.	Last Sunday in Oct. at 2:00 a.m.	1:00
est	Eastern Standard Time	-05:00	1st Sunday in Apr. at 2:00 a.m.	Last Sunday in Oct. at 2:00 a.m.	1:00
cst	Central Standard Time	-06:00	1st Sunday in Apr. at 2:00 a.m.	Last Sunday in Oct. at 2:00 a.m.	1:00
mst	Mountain Standard Time	-07:00	1st Sunday in Apr. at 2:00 a.m.	Last Sunday in Oct. at 2:00 a.m.	1:00
pst	Pacific Standard Time	-08:00	1st Sunday in Apr. at 2:00 a.m.	Last Sunday in Oct. at 2:00 a.m.	1:00
akst	Alaska	-09:00	1st Sunday in Apr. at 2:00 a.m.	Last Sunday in Oct. at 2:00 a.m.	1:00
hst	Hawaii	-10:00	No default	No default	No default
zm11	No standard name	-11:00	No default	No default	No default

Examples

```
-> system timezone mst
-> system timezone -7
-> system timezone +0
-> system timezone +12
-> system timezone 12
-> system timezone 05:30
-> system timezone 00:00 hour from UTC
```

Release History

Release 5.1; command was introduced.

Related Commands

system date	Displays or modifies the switch's current system date.
system time	Displays or modifies the switch's current system time.

MIB Objects

```
systemServices
   systemServicesTimezone
   systemServicesTimezoneStartWeek
   systemServicesTimezoneStartDay
   systemServicesTimezoneStartMonth
   systemServicesTimezoneStartTime
   systemServicesTimezoneOffset
   systemServicesTimezoneEndWeek
   systemServicesTimezoneEndDay
   systemServicesTimezoneEndMonth
   systemServicesTimezoneEndTime
   systemServicesEnableDST
```

system daylight savings time

Enables or disabled Daylight Savings Time (DST) on the switch.

system daylight savings time [{enable | disable} | start {*week*} {*day*} in {*month*} at {*hh:mm*} end {*week*} {*day*} in {*month*} at {*hh:mm*} [by *min*]]

Syntax Definitions

enable	Enables DST. The switch clock will automatically adjust for DST as specified by one of the default time zone or by the specifications set with the system daylight savings time start command.
disable	Disables DST. The switch clock will not change for DST.
start	For non-default time zone, you can specify the *week*, *day*, *month*, and *hour* for DST to start. (You must also specify the *week*, *day*, *month*, and *hour* for DST to end.)
end	For non-default time zone, if you specify the week, day, month, and hour for DST to end, you must also specify the *week*, *day*, *month*, and *hour* for DST to end.
week	Indicate whether first, second, third, fourth, or last.
day	Indicate whether Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday.
month	Indicate whether January, February, March, April, May, June, July, August, September, October, November, or December.
hh:mm	Use two digits between 00 and 23 to indicate hour. Use two digits between 00 and 59 to indicate minutes. Use as for a 24 hour clock.
by *min*	Use two digits to indicate the number of minutes your switch clock will be offset for DST. The range is from 00 to 50.

Defaults

- By default, DST is disabled.
- Unless a different value is set with the **by** syntax, the system clock will offset one hour for DST.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If your timezone shows a default value in the DST Start and DST End columns in the "Abbreviation" on page 2-9, you do not need to set a start and end time. Your switch clock will automatically adjust for DST as shown in the table.
- You must enable DST whether you use a default DST timezone or if you specify your offset using the **daylight savings time start** syntax.

Examples

```
-> system daylight savings time enable
-> system daylight savings time disable
-> system daylight savings time start first Sunday in May at 23:00 end last Sunday
in November at 10:00
-> system daylight savings time start first Sunday in May at 23:00 end last Sunday
in November at 10:00 by 45
```

Release History

Release 5.1; command was introduced.

Related Commands

system time	Displays or modifies the switch's current system time.
system timezone	Displays or modifies the timezone for the switch.
fabric standby	Displays or modifies the switch's current system date.

MIB Objects

```
systemServices
   systemServicesTimezone
   systemServicesEnableDST
```

reload ni

Reloads (i.e., reboots) a specified Network Interface (NI) module.

reload ni [slot] *number*

Syntax Definitions

slot	Optional command syntax.
number	The slot number containing the NI module being reloaded.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- On OmniSwitch 7700, 7800, and 8800 the **reload ni** command reboots only the specified NI. Other modules installed in the chassis, including primary and secondary CMMs, are not affected.
- On OmniSwitch 6600 Family switches the **reload ni** command reboots only the specified switch. However, if you use this command on a switch that has a primary CMM role in a stack it will no longer be primary. Instead, it will be secondary in a two-switch stack and idle in stack consisting of three or more switches.

Examples

```
-> reload ni slot 2
-> reload ni 2
```

Release History

Release 5.1; command was introduced.

Related Commands

reload all	Reloads all NIs and CMMs in a chassis.
power ni	Turns the power on or off for a specified Network Interface (NI) module.
show ni	Shows hardware information and current status for Network Interface (NI) modules currently running in the chassis.

MIB Objects

```
chasEntPhysicalTable
   chasEntPhysAdminStatus
   reset
```

reload all

Reloads (i.e., reboots) all Network Interfaces (NIs) and Chassis Management Modules (CMMs) in an OmniSwitch 7700/7800/8800 chassis and all switches in an OmniSwitch 6600 Family stack.

reload all [in [*hours***:] *minutes* | **at** *hour***:***minute* **[***month day* | *day month***]]**

reload all cancel

Syntax Definitions

in [*hours***:] *minutes*	Optional syntax. Schedules a reload of all modules to take effect in the specified minutes or hours and minutes within the next 24 hours.
at *hour***:***minute*	Optional syntax. Schedules a reload of all modules to take place at the specified time using a 24-hour clock. If you do not specify the month and day, the reload takes place at the specified time on the current day provided the specified time is later than the time when the CLI command is issues. If the specified time is earlier than the current time, the reload will take place on the following day.
month day | *day month*	The name of the month and the number of the day for the scheduled reload. Specify a month name and the day number. It is unimportant if the month or day is first. See examples below for further explanation.
cancel	Cancels a pending time delayed reload.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> reload all
```

Release History

Release 5.1; command was introduced.

Related Commands

reload ni	Reloads a specific NI module.
power ni	Turns the power on or off for a specified Network Interface (NI) module.
show ni	Shows hardware information and current status for Network Interface (NI) modules currently running in the chassis.

MIB Objects

```
chasEntPhysicalTable
   chasEntPhysAdminStatus
   reset
```

power ni

Turns the power on or off for a specified Network Interface (NI) module.

power ni [slot] *slot-number*

no power ni [slot] *slot-number*

Syntax Definitions

slot	Optional command syntax.
slot-number	The chassis slot number containing the NI module being powered on or off. Valid slot numbers for OmniSwitch 7700 switches range from 1–8; valid slot numbers for OmniSwitch 7800 and 8800 switches range from 1–16. For information regarding OmniSwitch 6600 Family switches, refer to the "Usage Guidelines" section below.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- For OmniSwitch 7700, 7800, or 8800 switches, use the **no** form of the command to power off an NI module. When the **no** form of the command is used on OmniSwitch 6600 Family switches, the corresponding switch will be powered off. To power on the switch again, the user must manually toggle the power switch located on the back of the OmniSwitch 6600 Family switch chassis.
- OmniSwitch 6600 Family switches cannot be powered *on* via the **power ni** command. For OmniSwitch 6600 Family switches, only the **no** form of the command is supported.

Examples

```
-> power ni slot 1
-> power ni 7
```

Release History

Release 5.1; command was introduced.

Related Commands

reload ni	Reloads (i.e., reboots) a specified Network Interface (NI) module.
show ni	Shows hardware information and current status for Network Interface (NI) modules currently running in the chassis.

MIB Objects

```
chasEntPhysicalTable
   chasEntPhysAdminStatus
   powerOn
   powerOff
```

temp-threshold

Sets the CPU warning temperature threshold on OmniSwitch 6600, 7700, and 7800 switches and the Switch Fabric Module (SFM) warning temperature threshold on OmniSwitch 8800 switches.

temp-threshold *temp*

Syntax Definitions

temp	The new temperature threshold value, in Celsius (31–76 on OmniSwitch 6600 Family switches, 31–79 on OmniSwitch 7700/7800 switches, and 31–74 on OmniSwitch 8800 switches).

Defaults

parameter	default
temp (OmniSwitch 6600, 7700, 7800)	60
temp (OmniSwitch 8800)	50

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> temp-threshold 45
```

Release History

Release 5.1; command was introduced.

Related Commands

show temperature	Displays the current operating chassis ambient temperature, as well as current temperature threshold settings.

MIB Objects

```
chasChassisTable
   chasTempThreshold
```

fabric standby

Sets a Switch Fabric Module (SFM) from active to standby mode. When an SFM is in standby mode, it serves as a redundant module and will take over fabric-level processing in the event of an active SFM failure. For detailed information on SFMs, including SFM redundancy, refer to the "Switch Fabric Module (SFM)" chapter in the *OmniSwitch 8800 Hardware Users Guide*.

fabric standby *number*

Syntax Definitions

number	The slot position of the SFM to be set to standby mode (1–5). For slot locations, refer to the *Users Guide*.

Defaults

N/A

Platforms Supported

OmniSwitch 8800

Usage Guidelines

Because OS8800 switches require a minimum of four active SFMs *at all times*, a fifth (i.e., redundant) SFM must be installed in the chassis before the **fabric standby** command can be issued. If only four SFMs are installed, the switch will disregard the **fabric standby** command entry. For details on SFM redundancy and SFM slot locations, refer to the "Switch Fabric Module (SFM)" chapter in the *OmniSwitch 8800 Hardware Users Guide*.

Examples

```
-> fabric standby 4
```

Release History

Release 5.1; command was introduced.

Related Commands

power fabric	Turns the power on or off for a specified Switch Fabric Module (SFM).
show fabric	Displays the status and configuration of Switch Fabric Modules (SFMs).

MIB Objects

```
chasEntPhysicalTable
   chasEntPhysAdminStatus
```

power fabric

Turns the power on or off for a specified Switch Fabric Module (SFM). For detailed information on SFMs, refer to the "Switch Fabric Module (SFM)" chapter in the *OmniSwitch 8800 Hardware Users Guide*.

power fabric *number*

no power fabric *number*

Syntax Definitions

number	The slot position of the SFM to be turned on or off (1–5). For slot locations, refer to the *Users Guide*.

Defaults

N/A

Platforms Supported

OmniSwitch 8800

Usage Guidelines

- Because OmniSwitch 8800 switches require a minimum of four active SFMs *at all times*, a fifth (i.e., redundant) SFM must be installed in the chassis before the **power fabric** command can be issued. If only four SFMs are installed, the switch will disregard the **power fabric** command entry. For details on SFM redundancy and SFM slot locations, refer to the "Switch Fabric Module (SFM)" chapter in the *OmniSwitch 8800 Hardware Users Guide*.

Examples

```
-> power fabric 3
-> no power fabric 5
```

Release History

Release 5.1; command was introduced.

Related Commands

fabric standby	Sets a Switch Fabric Module (SFM) from active to standby mode.
show fabric	Displays the status and configuration of Switch Fabric Modules (SFMs).

MIB Objects

```
chasEntPhysicalTable
   chasEntPhysAdminStatus
```

show system

Displays basic system information for the switch. Information includes a user-defined system description, name, administrative contact, and location, as well as object ID, up time, and system services.

show system

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This command may be used when logged into either the primary or secondary CMM.

Examples

```
-> show system
System:
  Description:  5.4.1.231.R01 Development, April 13, 2006.,
  Object ID:    1.3.6.1.4.1.6486.800.1.1.2.1.2.1.1,
  Up Time:      0 days 0 hours 27 minutes and 23 seconds,
  Contact:      Alcatel Internetworking, www.Alcatel.com/enterprise/en,
  Name:         Eagle,
  Location:     Unknown,
  Services:     72,
  Date & Time:  WED APR 19 2006  18:25:51 (PST)

Flash Space:
    Primary CMM:
      Available (bytes):  1898496,
      Comments         :  None
    Secondary CMM:
      Available (bytes):  0,
      Comments         :  None
```

output definitions

System Description	The description for the current system. This description shows the current software version and the system date.
System Object ID	The SNMP object identifier for the switch.
System Up Time	The amount of time the switch has been running since the last system reboot.
System Contact	An user-defined administrative contact for the switch. This field is modified using the **system contact** command.
System Name	A user-defined text description for the switch. This field is modified using the **system name** command.
System Location	The user-defined physical location of the switch. This field is modified using the **system location** command.
System Services	The number of current system services.
System Date & Time	The current system date and time. This field is modified using the **system date** and **system time** commands.
Flash Space: Primary CMM: Available (bytes)	The available flash memory space available on the switch's *primary* management module.
Flash Space: Primary CMM: Comments	Comments regarding the available flash memory space available on the switch's primary management module, if applicable.
Flash Space: Secondary CMM: Available (bytes)	The available flash memory space available on the switch's *secondary* (i.e., redundant) management module, if applicable.
Flash Space: Secondary CMM: Comments	Comments regarding the available flash memory space available on the switch's primary management module, if applicable.

Release History

Release 5.1; command was introduced.

Related Commands

system contact	Specifies the switch's administrative contact (e.g., an individual or department).
system name	Modifies the switch's current system name.
system location	Specifies the switch's current physical location.

MIB Objects

```
system
   systemContact
   systemName
   systemLocation
```

show hardware info

Displays current system hardware information. Includes CPU, flash, RAM, NVRAM battery, jumper positions, BootROM, miniboot, and FPGA information.

show hardware info

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This command may be used when logged into either the primary or secondary CMM.

Examples

```
-> show hardware info
CPU Type                          : UltraSPARC IIe (SPARC-V9),
Flash Manufacturer                : AMD,
Flash size                        : 33554432 bytes (32 MB),
RAM Manufacturer                  : Micron,
RAM size                          : 134217728 bytes (128 MB),
NVRAM Battery OK                  : YES,
Interrupt Boot Jumper             : OFF,
Force UART Defaults Jumper        : OFF,
Run Extended Memory Diags Jumper  : OFF,
Spare Jumper                      : OFF,
BootROM Version                   : 5.1.5.340.R01,
Backup Miniboot Version           : 5.1.5.340.R01,
Default Miniboot Version          : 5.1.5.340.R01,
FPGA (1) Version                  : 42,
FPGA (2) Version                  : 42
FPGA (3) Version                  : 42
```

output definitions

CPU Type	The manufacturer and model number of the CPU used on the CMM.
Flash Manufacturer	The manufacturer of the flash memory used on the CMM.
Flash size	The total amount of flash memory (i.e., file space) on the CMM. This field specifies the total flash memory size only and does not indicate the amount of memory free or memory used.
RAM Manufacturer	The manufacturer of the RAM memory used on the CMM.
RAM size	The total amount of RAM memory on the CMM. This field specifies the total RAM memory only and does not indicate the amount of memory free or memory used.
NVRAM Battery OK	The current status of the NVRAM battery. If the battery is OK, YES is displayed in this field. If the battery charge becomes low, NO is displayed in this field.
Interrupt Boot Jumper	Displays whether the Interrupt Boot Jumper for the CMM has been set. The factory default setting is OFF, or unset.
Force UART Defaults Jumper	Displays whether the Force Uart Defaults Jumper for the CMM has been set. The factory default setting is OFF, or unset.
Run Extended Memory Diags Jumper	Displays whether the Run Extended Memory Diagnostics Jumper for the CMM has been set. The factory default setting is OFF, or unset.
Spare Jumper	Displays whether the Spare Jumper for the CMM has been set. The factory default setting is OFF, or unset.
BootROM Version	The current BootROM version. (This field is not displayed on OmniSwitch 6600 Family switches.)
Backup Miniboot Version	The current backup miniboot version. (This field is not displayed on OmniSwitch 6600 Family switches.)
Default Miniboot Version	The current default miniboot version. (This field is not displayed on OmniSwitch 6600 Family switches.)
FPGA (1) Version	The version number of the CMM's FPGA device 1. (This field is not displayed on OmniSwitch 6600 Family switches.)
FPGA (2) Version	The version number of the CMM's FPGA device 2 (applicable to OmniSwitch 7700/7800 switches only).
FPGA (3) Version	The version number of the CMM's FPGA device 2 (applicable to OmniSwitch 8800 switches only).

Release History

Release 5.1; command was introduced.

Related Commands

show chassis	Displays basic configuration and status information for the switch chassis.
show cmm	Displays basic hardware and status information for CMM modules running in the chassis.

MIB Objects

```
systemHardware
   systemHardwareBootCpuType
   systemHardwareFlashMfg
   systemHardwareFlashSize
   systemHardwareMemoryMfg
   systemHardwareMemorySize
   systemHardwareNVRAMBatteryLow
   systemHardwareJumperInterruptBoot
   systemHardwareJumperForceUartDefaults
   systemHardwareJumperRunExtendedMemoryDiagnostics
   systemHardwareJumperSpare
   systemHardwareBootRomVersion
   systemHardwareBackupMiniBootVersion
   systemHardwareDefaultMiniBootVersion
   systemHardwareFpgaVersionTable
   systemHardwareFpgaVersionEntry
   systemHardwareFpgaVersionIndex
```

show chassis

Displays basic configuration and status information for the switch chassis.

show chassis [*number***]**

Syntax Definitions

number	On OmniSwitch 6600 Family switches only you can specify the slot (i.e., switch) number within the stack, which can be 1–8.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This command may be used when logged into either the primary or secondary CMM.

Examples

```
-> show chassis
Model Name:                     OSR-F80,
Description:                    OSR-F80,
Part Number:                    901748-ÿÿÿ
Hardware Revision:              202,
Serial Number:                  1467014A,
Manufacture Date:               NOV 15 2001,
Admin Status:                   POWER ON,
Operational Status:             UP,
Free Slots:                     13,
Power Left:                     663,
Number Of Resets:               0
```

output definitions

Model Name	The factory-set model name for the switch. This field cannot be modified.
Description	The factory-set description for the switch. This field cannot be modified.
Part Number	The Alcatel part number for the chassis.
Hardware Revision	The hardware revision level for the chassis.
Serial Number	The Alcatel serial number for the chassis.
Manufacture Date	The date the chassis was manufactured.
Admin Status	The current power status of the chassis. Because chassis information is obtained from a running CMM, the value will always be POWER ON.
Operational Status	The current operational status of the chassis.

output definitions (continued)

Free Slots	The number of slots available for NI module installation. For example, a value of 13 on a 16-slot full chassis switch indicates that three NI modules are currently installed and 13 slots are available. However, this is subject to the current power available for NI modules in the chassis. Refer to the *Hardware User Manual* for important information on power supplies and maximum NI support. (This field is not displayed on OmniSwitch 6600 Family switches.)
Power Left	The amount of power available to additional chassis components, in watts. Refer to your *Hardware User Manual* for important information on power supplies and maximum NI support. (This field is not displayed on OmniSwitch 6600 Family switches.)
Number of Resets	The number of times the CMM has been reset (i.e., reloaded or rebooted) since the last cold boot of the switch.

Release History

Release 5.1; command was introduced.

Related Commands

show hardware info	Displays current system hardware information.
show power	Displays hardware information and current status for chassis power supplies.
show fan	Displays the current operating status of chassis fans.

MIB Objects

```
chasChassisTable
   chasFreeSlots
   chasPowerLeft
```

show cmm

Displays basic hardware and status information for CMM modules running in the chassis.

show cmm [*number***]**

Syntax Definitions

number	On OmniSwitch 6600 Family switches only you can specify the slot (i.e., switch) number within the stack, which can be 1–8.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- On OmniSwitch 7700/7800 switches a CMM installed in the left CMM slot position is defined as CMM-A. A CMM installed in the right position is CMM-B. CMM modules on these switches are made up of two subcomponents: the fabric board and the processor board. The fabric board is CMM subcomponent 1; the processor board is subcomponent 2.
- On OmniSwitch 8800 switches a CMM installed in the top CMM slot position is defined as CMM-A. A CMM installed in the bottom position is CMM-B.
- On OmniSwitch 7700/7800/8800 switches CMM information is displayed separately for each subcomponent. For example, on OmniSwitch 7700/7800 switches CMM-A-1 refers the fabric board of a CMM installed in the left position; on OmniSwitch 7700/7800/8800 switches CMM-A-2 refers to the processor board of the same CMM.
- If a secondary CMM is installed and running in the chassis, hardware and status information for both the primary and secondary CMM will be displayed.
- This command may be used when logged into either the primary or secondary CMM.

Examples

```
-> show cmm
Module in slot CMM-A-1
  Model Name:                     OS7700-CMM ,
  Description:                    BBUS Bridge,
  Part Number:                    901753-10,
  Hardware Revision:              212,
  Serial Number:                  1443025P,
  Manufacture Date:               DEC 10 2001,
  Firmware Version:               36,
  Admin Status:                   POWER ON,
  Operational Status:             UP,
  Power Control Checksum:         0x738,
  MAC Address:                    00:d0:95:6b:09:40,
  ASIC - Physical:                0x0701 0x0701 0x0701 0x0701 0x0701 0x0701 0x070
1 0x0701

    Module in slot CMM-A-2
      Model Name:                     CMM-PROC,
      Description:                    CMM-PROC,
      Part Number:                    901753-10,
      Hardware Revision:              202,
      Serial Number:                  1433086P,
      Manufacture Date:               NOV 01 2001,
      Firmware Version:               36
```

output definitions

Model Name	The model name of the CMM boards. Note that on OmniSwitch 7700/7800 switches CMM modules are made up of two major subcomponents: the fabric board and the processor board. Fabric boards are denoted as OS7*00-CMM and processor boards are denoted as CMM-PROC. Information for each board is displayed separately.
Description	A factory-defined description of the associated board (e.g., BBUS Bridge or PROCESSOR).
Part Number	The Alcatel part number for the board.
Hardware Revision	The hardware revision level for the board.
Serial Number	The Alcatel serial number for the board.
Manufacture Date	The date the board was manufactured.
Firmware Version	The firmware version for the board's ASICs.
Admin Status	The current power status of the CMM. Because information is obtained from a running CMM, the value will always be POWER ON.
Operational Status	The current operational status of the CMM.
Power Control Checksum	The current power control checksum for the corresponding CMM.

output definitions (continued)

MAC Address	The MAC address assigned to the chassis. This base chassis MAC address is a unique identifier for the switch and is stored on an EEPROM card in the chassis. It is not tied to the CMM. Therefore, it will not change if the CMM is replaced or becomes secondary. The MAC address is used by the Chassis MAC Server (CMS) for allocation to various applications. Refer to the "Managing MAC Addresses and Ranges" chapter of the *Switch Management Guide* for more information.
ASIC - Physical	General information regarding the fabric module's ASICs.

Release History

Release 5.1; command was introduced.

Related Commands

show chassis	Displays basic configuration and status information for the switch chassis.
show ni	Displays basic hardware and status information for Network Interface (NI) modules currently installed in the switch.
show module	Displays basic information for either a specified module or all modules installed in the chassis.
show module long	Displays detailed information for either a specified module or all modules installed in the chassis.
show module status	Displays basic status information for either a specified module or all modules installed in the chassis.
show fabric	Displays the status and configuration of Switch Fabric Modules (SFMs) on OmniSwitch 8800 switches.

show ni

Displays basic hardware and status information for Network Interface (NI) modules currently installed in the switch.

show ni [*number***]**

Syntax Definitions

number	The slot number for a specific NI module installed in the chassis. If no slot number is specified, information for all NI modules is displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command may be used when logged into either the primary or secondary CMM.
- On OmniSwitch 8800 switches only additional information is displayed on NI subcomponents.

Examples

```
-> show ni 2
Module in slot 2
  Model Name:                   OS8-GNI-U8 ,
  Description:                  8PT FIBER GIG MOD,
  Part Number:                  902162-10,
  Hardware Revision:            209,
  Serial Number:                2236006P,
  Manufacture Date:             JAN 01 1970,
  Firmware Version:             6,
  Admin Status:                 POWER ON,
  Operational Status:           UP,
  Power Control Checksum:       0x808,
  MAC Address:                  00:d0:95:77:50:ea,
  ASIC - Physical:              0x1a01 0x1a01 0x1a01 0x1a01

    Daughter Board in port 1
      Model Name:                   IBM,
      Description:                  IBM,
      Part Number:                  IBM42P12SNY,
      Hardware Revision:            AA106,
      Serial Number:                21P704214H2DIBM,
      Manufacture Date:             01041801,
      Firmware Version:             6,
      Admin Status:                 POWER ON,
      Operational Status:           UP
```

```
Daughter Board in port 2
  Model Name:                   IBM,
  Description:                  IBM,
  Part Number:                  IBM42P12SNY,
  Hardware Revision:            AA106,
  Serial Number:                21P704214H37IBM,
  Manufacture Date:             01041801,
  Firmware Version:             6,
  Admin Status:                 POWER ON,
  Operational Status:           UP
```

output definitions

Model Name	The NI's module name. For example, OS7-ENI-FM12 indicates a twelve-port 100BaseFX Ethernet module.
Description	A general description of the NI. For example, 12pt 100BaseF Mod indicates a twelve-port 100BaseFX Ethernet module.
Part Number	The Alcatel part number for the NI.
Hardware Revision	The hardware revision level for the NI.
Serial Number	The Alcatel serial number for the NI's printed circuit board (PCB).
Manufacture Date	The date the NI was manufactured.
Firmware Version	The firmware version for the NI's ASICs.
Admin Status	The current power status of the NI. Options include POWER ON or POWER OFF.
Operational Status	The operational status of the NI. Options include UP or DOWN. The operational status can be DOWN while the power status is on, indicating a possible software issue.
Power Control Checksum	The current power control checksum for the corresponding NI.
MAC Address	The MAC address assigned to the NI.
ASIC - Physical	General information regarding the NI module's ASICs.

Release History

Release 5.1; command was introduced.

Related Commands

reload ni	Reloads (i.e., reboots) a specified Network Interface (NI) module.
power ni	Turns the power on or off for a specified Network Interface (NI) module.
show module	Displays basic information for either a specified module or all modules installed in the chassis.
show module long	Displays detailed information for either a specified module or all modules installed in the chassis.
show module status	Displays basic status information for either a specified module or all modules installed in the chassis.

MIB Objects

`chasEntPhysOperStatus`

show module

Displays basic information for either a specified module or all modules installed in the chassis. Modules include primary and secondary CMMs and Network Interface (NI) modules.

show module [*number***]**

Syntax Definitions

number	The slot number for a specific module installed in the chassis. If no slot number is specified, information for all modules is displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This command may be used when logged into either the primary or secondary CMM.

Examples

```
-> show module
                                    HW    Mfg
Slot     Part-Number     Serial #   Rev   Date      Model Name
-------+--------------+------------+---+-----------+---------------------------
CMM-A-1 901753-10      1443032P     212 DEC 11 2001 OS7800-CMM

CMM-A-2 901753-10      1433056P     202 NOV 02 2001 CMM-PROC

NI-1    901759-10      1483117A     405 DEC 17 2001 OS7-GNI-U2

NI-3    901765-10      1453442A     405 DEC 17 2001 OS7-ENI-C24

NI-5    901766-10      1503078P     106 DEC 20 2001 OS7-ENI-FM12
```

output definitions

Slot	The chassis slot position of the module. For detailed slot numbering information, refer to the "Chassis and Power Supplies" chapter of the *Hardware User Manual*. Refer to page 2-30 for additional information on CMM location callouts.
Part-Number	The Alcatel part number for the module.
Serial #	The Alcatel serial number for the module.
Rev	The hardware revision level for the module.
Date	The date the module was manufactured.
Model Name	The descriptive name for the module. For example, OS7-GNI-U2 indicates a two-port Gigabit Ethernet module.

Release History

Release 5.1; command was introduced.

Related Commands

show module long	Displays detailed information for either a specified module or all modules installed in the chassis.
show module status	Displays basic status information for either a specified module or all modules installed in the chassis.

show module long

Displays detailed information for either a specified module or all modules installed in the chassis. Modules include primary and secondary CMMs and Network Interface (NI) modules.

show module long [*number***]**

Syntax Definitions

number	The slot number for a specific module installed in the chassis. If no slot number is specified, detailed information for all modules is displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- When a module with a daughter board is viewed using the **show module long** command (e.g., an OS7-GNI-U2 module with a GBIC installed), information for the daughter board is also displayed.
- When a particular NI module is specified in the command line, output is the same as that of the **show ni** command.
- This command may be used when logged into either the primary or secondary CMM.

Examples

```
-> show module long 5
Module in slot 5
  Model Name:                     OS7-ENI-FM12,
  Description:                    12pt 100BaseF Mod,
  Part Number:                    901766-10,
  Hardware Revision:              106,
  Serial Number:                  1503078P,
  Manufacture Date:               DEC 20 2001,
  Firmware Version:               5,
  Admin Status:                   POWER ON,
  Operational Status:             UP,
  Power Control Checksum:         0x732,
  MAC Address:                    00:d0:95:6b:3a:20,
  ASIC - Physical:                0x1901 0x0201 0x001e 0x001e
```

output definitions

Model Name	The NI's module name. For example, OS7-ENI-FM12 indicates a twelve-port 100BaseFX Ethernet module.
Description	A general description of the NI. For example, 12pt 100BaseF Mod indicates a twelve-port 100BaseFX Ethernet module.
Part Number	The Alcatel part number for the NI.
Hardware Revision	The hardware revision level for the NI.
Serial Number	The Alcatel serial number for the NI's printed circuit board (PCB).
Manufacture Date	The date the NI was manufactured.
Firmware Version	The firmware version for NI's ASICs.
Admin Status	The current power status of the NI. Options include POWER ON or POWER OFF.
Operational Status	The operational status of the NI. Options include UP or DOWN. The operational status can be DOWN while the power status is on, indicating a possible software issue.
Power Control Checksum	The current power control checksum for the corresponding NI.
MAC Address	The MAC address assigned to the NI.
ASIC - Physical	General information regarding the NI's ASICs.

Release History

Release 5.1; command was introduced.

Related Commands

show module	Displays basic information for either a specified module or all modules installed in the chassis.
show module status	Displays basic status information for either a specified module or all modules installed in the chassis.

show module status

Displays basic status information for either a specified module or all modules installed in the chassis. Modules include primary and secondary CMMs and Network Interface (NI) modules.

show module status [*number***]**

Syntax Definitions

number	The slot number for a specific module installed in the chassis. If no slot number is specified, status information for all modules is displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This command may be used when logged into either the primary or secondary CMM.

Examples

```
-> show module status
       Operational                Firmware
Slot     Status      Admin-Status   Rev           MAC
------+------------+------------+---------+-----------------
CMM-A    UP           POWER ON      36      00:d0:95:6b:09:40

NI-1     UP           POWER ON      5       00:d0:95:6b:22:5c

NI-3     UP           POWER ON      5       00:d0:95:6b:23:2e

NI-5     UP           POWER ON      5       00:d0:95:6b:3a:20
```

output definitions

Slot	The chassis slot position of the module. For detailed slot numbering information, refer to the “Chassis and Power Supplies” chapter of the *Hardware User Guide*. Refer to page 2-30 for additional information on CMM callouts.
Operational Status	The operational status of the module. Options include UP or DOWN. For NI and secondary CMM modules, the operational status can be DOWN while the power status is on, indicating a possible software issue.
Admin-Status	The current power status of the module. Options include POWER ON or POWER OFF.

output definitions (continued)

Firmware Rev	The firmware version for module's ASICs.
MAC	For the CMM, the base chassis MAC address is displayed. For detailed information on this base chassis MAC address, refer to the "Managing MAC Addresses and Ranges" chapter of the *Switch Management Guide*. For NI modules, the MAC address for the corresponding NI is displayed.

Release History

Release 5.1; command was introduced.

Related Commands

show module	Displays basic information for either a specified module or all modules installed in the chassis.
show module long	Displays detailed information for either a specified module or all modules installed in the chassis.

show power

Displays hardware information and current status for chassis power supplies.

show power [supply] [*number***]**

Syntax Definitions

supply	Optional command syntax.
number	The single-digit number for a specific power supply installed in the chassis. If no power supply number is specified, information for all power supplies is displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- When the **show power** command is entered on OmniSwitch 7700, 7800, and 8800 switches, information is displayed only for power supplies that are installed in the chassis *and powered on*. If a power supply is present in a power supply bay, but the power supply is unplugged or its on/off switch is in the off position, the power supply is not listed in the command output.
- On OmniSwitch 7700 and 7800 switches, power supplies are numbered from top to bottom. For example, a power supply installed in the top position in the chassis is Power Supply 1, or PS-1.
- On OmniSwitch 6600 Family switches the built-in power supply is PS-1 and the optional backup power supply is PS-2.
- On OmniSwitch 8800 switches, power supplies are numbered from left to right. For detailed slot numbering information, see the “Chassis and Power Supplies” chapter of your *Hardware Users Guide*.

Examples

The following is an example of the **show power** command on an OmniSwitch 7700, 7800, or 8800 switch:

```
-> show power supply 2
Module in slot PS-2
  Model Name:                   OSR-PS-06,
  Description:                  OSR-PS-06,
  Part Number:                  901750-10,
  Hardware Revision:            9C1,
  Serial Number:                B42N053P2,
  Manufacture Date:             OCT 18 2001º,
  Firmware Version:             9C1,
  Admin Status:                 POWER ON,
  Operational Status:           UP,
  Power Provision:              600
```

OmniSwitch 7700/7800/8800 output definitions

Model Name	The power supply's model number.
Description	A description of the associated power supply. This field will reflect the Model Name in most cases.
Part Number	The Alcatel part number for the power supply.
Hardware Revision	The hardware revision level for the power supply.
Serial Number	The Alcatel serial number for the power supply.
Manufacture Date	The date the power supply was manufactured.
Firmware Version	The firmware version for power supply's ASICs.
Admin Status	The current power status of the supply. Options include POWER ON or POWER OFF.
Operational Status	The operational status of the power supply. Options include UP or DOWN.
Power Provision	The number of Watts used by this power supply.

The following is an example of the **show power** command on an OmniSwitch 6600 Family switches.

```
-> show power
Power Supplies in chassis 1
PS    Operational Status
-----+------------------
PS-1   UP
PS-2          NOT PRESENT
```

OmniSwitch 6600 Family output definitions

Power PS	The power supply identification, which can be PS-1 for the built-in power supply or PS-2 for the optional backup power supply.
Operational Status	The operational status of the power supply. Options include UP, DOWN, or NOT PRESENT.

Release History

Release 5.1; command was introduced.

Related Commands

show chassis	Displays basic configuration and status information for the switch chassis.

show fan

Displays the current operating status of chassis fans.

show fan [*number***]**

Syntax Definitions

number	On OmniSwitch 7700, 7800, and 8800 switches the single-digit number for a specific chassis fan. On OmniSwitch 6600 Family switches this parameter specifies the switch (slot) number of the chassis.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- On OmniSwitch 7700 and 7800 switches the valid range for the chassis fan is 1–3. If no fan number is specified, the status of all fans is displayed.
- On OmniSwitch 8800 switches the valid range for the chassis fan 1–7. If no fan number is specified, the status of all fans is displayed.
- On OmniSwitch 6600 Family switches this parameter specifies the switch (slot) number of the chassis. In a stack if no switch number is specified then all switches in a stack will be displayed.

Examples

The following is an example of the **show fan** command on an OmniSwitch 7700, 7800, or 8800 switch:

```
-> show fan
Fan        Status
------+---------------
Fan-1     Running
Fan-2     Running
Fan-3     Running
```

OmniSwitch 7700/7800/8800 output definitions

Fan	The fan number describing the fan position.
Status	The current operational status of the corresponding fan.

The following is an example of the **show fan** command on an OmniSwitch 6600 switch:

```
-> show fan 1
Chassis Fan  Status
-------+---+-----------
   1     1   Running
   1     2   Running
   1     3   Running
```

OmniSwitch 6600 Family output definitions

Chassis	The switch (slot) number of the chassis.
Fan	The fan number describing the fan position.
Status	The current operational status of the corresponding fan.

Release History

Release 5.1; command was introduced.

Related Commands

show temperature	Displays the current operating chassis ambient temperature, as well as current temperature threshold settings.

show temperature

Displays the current operating chassis ambient temperature, as well as current temperature threshold settings.

show temperature [*number***]**

Syntax Definitions

number	On OmniSwitch 6600 Family switches only, you can specify the slot (i.e., switch) number within the stack, which can be 1–8. If no slot number is specified, temperature information for all switches operating in the stack displays.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

The following is an example of the **show temperature** command on an OmniSwitch 6600, 7700, or 7800 switch:

```
-> show temperature
Hardware Board Temperature (deg C)        = 34,
Hardware Cpu Temperature (deg C)          = 28,
Temperature Upper Threshold Range (deg C) = 30 to 80,
Temperature Upper Threshold (deg C)       = 60,
Temperature Range                         = UNDER THRESHOLD,
Temperature Danger Threshold (deg C)      = 80
```

OmniSwitch 6000 and 7700/7800 output definitions

Hardware Board Temperature	The current chassis temperature as determined by the built-in temperature sensor. The temperature is displayed in degrees Centigrade (i.e., Celsius). This temperature is checked against the upper threshold value. If the threshold is exceeded, a warning is sent to the user.
Hardware Cpu Temperature	The current CPU temperature. The temperature is displayed in degrees Centigrade (i.e., Celsius).
Temperature Upper Threshold Range	The supported threshold range. When you specify a threshold for the switch via the **temp-threshold** command, values may range from 31–79. In other words, *within* the 30 to 80 range displayed in this field on OmniSwitch 7700/7800 switches *within* the 30 to 70 range displayed in this field on OmniSwitch 6600 Family switches.

OmniSwitch 6000 and 7700/7800 output definitions (continued)

Temperature Upper Threshold	The warning temperature threshold, in degrees Celsius. If the switch reaches or exceeds this temperature, the primary switch or CMM's TEMP LED displays amber and a warning is sent to the user. Values may range from 31–79 on OmniSwitch 7700/7800 switches and 31–76 on OmniSwitch 6600 Family switches. The default value is 60. For information on changing the upper threshold value, refer to the **temp-threshold** command on page 2-20.
Temperature Range	The current threshold status of the switch. Displays whether the switch is UNDER THRESHOLD or OVER THRESHOLD. If the status is OVER THRESHOLD, the primary CMM's TEMP LED displays amber and a warning is sent to the user.
Temperature Danger Threshold	The factory-defined danger threshold. This field is not configurable. If the chassis temperature rises above 80 degrees Centigrade on OmniSwitch 7700/7800 switches, the switch will power off all Network Interface (NI) modules until the temperature conditions (e.g., chassis air flow obstruction or ambient room temperature) have been addressed and the switch is manually booted.

The following is an example of the **show temperature** command on an OmniSwitch 8800 switch:

```
-> show temperature
  Hardware Fabric Temperature (deg C)              = 34,
  Hardware Cpu Temperature (deg C)                 = 28,
  Temperature Fabric Upper Threshold Range (deg C) = 60 to 75,
  Temperature Cpu Upper Threshold Range (deg C)    = 50 to 62,
  Temperature Fabric Upper Threshold (deg C)       = 60,
  Temperature Cpu Upper Threshold (deg C)          = 50,
  Temperature Range                                = UNDER THRESHOLD,
  Temperature Fabric Danger Threshold (deg C)      = 75,
  Temperature CPU Danger Threshold (deg C)         = 62
```

OmniSwitch 8800 output definitions

Hardware Fabric Temperature	The current temperature of the Software Fabric Modules (SFMs). The temperature is displayed in degrees Centigrade (i.e., Celsius).
Hardware Cpu Temperature	The current CMM temperature. The temperature is displayed in degrees Centigrade (i.e., Celsius).
Temperature Fabric Upper Threshold Range	The supported threshold range for the Software Fabric Modules (SFMs). When you specify a threshold for the switch via the **temp-threshold** command, values may range from 31–74.
Temperature Cpu Upper Threshold Range	The supported threshold range of the CMMs.
Temperature Fabric Upper Threshold	The warning temperature threshold of the SFMs, in degrees Celsius. If the switch reaches or exceeds this temperature a warning is sent to the user. The default value is 50. For information on changing the upper threshold value, refer to the **temp-threshold** command on page 2-20.
Temperature Cpu Upper Threshold	The warning temperature threshold of the CMMs, in degrees Celsius. If the switch reaches or exceeds this temperature, the primary CMM's TEMP LED displays amber and a warning is sent to the user. The default value is 60.

OmniSwitch 8800 output definitions (continued)

Temperature Range	The current threshold status of the switch. Displays whether the switch is UNDER THRESHOLD or OVER THRESHOLD. If the status is OVER THRESHOLD, the primary CMM's TEMP LED displays amber and a warning is sent to the user.
Temperature Fabric Danger Threshold	The factory-defined danger threshold of the SFMs. This field is not configurable. If the temperature of the SFMs rises above 60 degrees Centigrade, the switch will send a warning message every 5 minutes. If the temperature of the SFMs rises above 75 degrees Centigrade, the switch will power down immediately.
Temperature Cpu Danger Threshold	The factory-defined danger threshold of the CMMs. This field is not configurable. If the temperature of the CMMs rises above 50 degrees Centigrade, the switch will send a warning message every 5 minutes. If the CPU temperature rises above 62 degrees Centigrade, the switch will power down immediately.

Release History

Release 5.1; command was introduced.

Related Commands

temp-threshold	Sets the chassis warning temperature threshold.
show fan	Shows hardware information and current status for the chassis fans.

MIB Objects

```
chasChassisTable
   chasHardwareBoardTemp
   chasHardwareCpuTemp
   chasTempRange
   chasTempThreshold
   chasDangerTempThreshold
```

show stack topology

Displays the current operating topology of switches within a stack.

show stack topology [*slot-number***]**

Syntax Definitions

slot-number	Optional syntax specifying a single slot number within the stack (1–8). When a slot number is specified, topology information for only the corresponding slot displays.

Defaults

N/A

Platforms Supported

OmniSwitch 6600

Usage Guidelines

N/A

Examples

The following example is for OmniSwitch 6600 Family switches:

```
-> show stack topology
                Link A    Link A    Link A      Link B    Link B    Link B
NI    Role      State     RemoteNI  RemoteLink  State     RemoteNI  RemoteLink
---+-----------+---------+---------+-----------+---------+---------+----------
 1  PRIMARY     ACTIVE       2          27      ACTIVE       2          28
 2  SECONDARY   ACTIVE       1          51      ACTIVE       1          52
```

output definitions

NI	The Network Interface (NI) number of the switch within the stack. This value can be 1–8 and cannot be changed through software. See the *OmniSwitch 6600 Family Hardware Users Guide* for information on changing this value.
Role	The current Chassis Management Module (CMM) role of this switch within the stack. This field can display PRIMARY (this switch acts as the primary CMM within the stack), SECONDARY (this switch acts as the secondary CMM), IDLE (the switch does not have a CMM role but is operating normally within the stack), STAND-ALONE (this switch is not part of the stack and is operating in standalone mode).
Link A State	The current status of the left-hand stacking port (port 27 on an OmniSwitch 6624 and Port 51 on an OmniSwitch 6648). Possible values are ACTIVE and INACTIVE. (If the port is inactive then the values displayed in the **Link A RemoteNI** and **Link A RemoteLink** fields are not significant.)

output definitions (continued)

Link A RemoteNI	The Network Interface (NI) number of the adjacent switch seen by this switch in the stack through the left-hand stacking port (Port 27 on an OmniSwitch 6624 and Port 51 on an OmniSwitch 6648). This value can be 1–8 or 0 if no neighboring switch is present.
Link A RemoteLink	The stacking port number of the adjacent switch seen by this switch in the stack through the left-hand stacking port (Port 27 on an OmniSwitch 6624 and Port 51 on an OmniSwitch 6648). This value can be 27 or 28 if an adjacent OmniSwitch 6624 is present, 51 or 52 if an adjacent OmniSwitch 6648 is present, or 0 if no neighboring switch is present.
Link B State	The current status of the right-hand stacking port (port 28 on an OmniSwitch 6624 and Port 52 on an OmniSwitch 6648). Possible values are ACTIVE and INACTIVE. (If the port is inactive then the values displayed in the **Link B RemoteNI** and **Link B RemoteLink** fields are not significant.)
Link B RemoteNI	The Network Interface (NI) number of the adjacent switch seen by this switch in the stack through right-hand stacking port (Port 28 on an OmniSwitch 6624 and Port 52 on an OmniSwitch 6648). This value can be 1–8 or 0 if no neighboring switch is present.
Link B RemoteLink	The stacking port number of the adjacent switch seen by this switch in the stack through right-hand stacking port (Port 28 on an OmniSwitch 6624 and Port 52 on an OmniSwitch 6648). This value can be 27 or 28 if an adjacent OmniSwitch 6624 is present, 51 or 52 if an adjacent OmniSwitch 6648 is present, or 0 if no neighboring switch is present.

Release History

Release 5.1; command was introduced.

Related Commands

N/A

MIB Objects

For OmniSwitch 6600 Family switches:

```
alaStackMgrChassisTable
   alaStackMgrSlotNINumber
   alaStackMgrSlotCMMNumber
   alaStackMgrChasRole
   alaStackMgrLocalLinkStateA
   alaStackMgrRemoteNISlotA
   alaStackMgrRemoteLinkA
   alaStackMgrLocalLinkStateB
   alaStackMgrRemoteNISlotB
   alaStackMgrRemoteLinkB
```

show fabric

Displays the status and configuration of Switch Fabric Modules (SFMs).

show fabric [*number***]**

Syntax Definitions

number	The slot position of the SFM for which status and configuration information is displayed (1–5). If no slot number is specified, information for all installed SFMs is displayed. For slot locations, refer to the *Users Guide*.

Defaults

N/A

Platforms Supported

OmniSwitch 8800

Usage Guidelines

N/A

Examples

```
-> show fabric
Fabric Number 1
  Model Name:                   OS8800-SFM ,
  Description:                  SWITCH FABRIC MOD,
  Part Number:                  901979-10,
  Hardware Revision:            102,
  Serial Number:                2366076P,
  Manufacture Date:             SEP 10 2002,
  Firmware Version:             ,
  Admin Status:                 POWER ON,
  Operational Status:           UP,
  Power Provision:              100

Fabric Number 2
  Model Name:                   OS8800-SFM ,
  Description:                  SWITCH FABRIC MOD,
  Part Number:                  901979-10,
  Hardware Revision:            102,
  Serial Number:                2366115P,
  Manufacture Date:             SEP 13 2002,
  Firmware Version:             ,
  Admin Status:                 POWER ON,
  Operational Status:           UP,
  Power Provision:              100
```

(Output continued on next page)

```
Fabric Number 3
  Model Name:                     OS8800-SFM ,
  Description:                    SWITCH FABRIC MOD,
  Part Number:                    901979-10,
  Hardware Revision:              102,
  Serial Number:                  2366078P,
  Manufacture Date:               SEP 10 2002,
  Firmware Version:               ,
  Admin Status:                   POWER ON,
  Operational Status:             UP,
  Power Provision:                100

Fabric Number 4
  Model Name:                     OS8800-SFM ,
  Description:                    SWITCH FABRIC MOD,
  Part Number:                    901979-10,
  Hardware Revision:              102,
  Serial Number:                  2366167P,
  Manufacture Date:               SEP 10 2002,
  Firmware Version:               ,
  Admin Status:                   POWER ON,
  Operational Status:             UP,
  Power Provision:                100

-> show fabric 3
Fabric Number 3
  Model Name:                     OS8800-SFM ,
  Description:                    SWITCH FABRIC MOD,
  Part Number:                    901979-10,
  Hardware Revision:              102,
  Serial Number:                  2366078P,
  Manufacture Date:               SEP 10 2002,
  Firmware Version:               ,
  Admin Status:                   POWER ON,
  Operational Status:             UP,
  Power Provision:                100
```

output definitions

Model Name	The factory-set model name for the SFM. This field cannot be modified.
Description	The factory-set description for the SFM. This field cannot be modified.
Part Number	The Alcatel part number for the SFM.
Hardware Revision	The hardware revision level for the SFM.
Serial Number	The Alcatel serial number for the SFM.
Manufacture Date	The date the SFM was manufactured.
Firmware Version	The firmware version for the SFM's ASICs.
Admin Status	The current power status of the SFM.
Operational Status	The current operational status of the SFM, which can be **UP** (the SFM is operational and being used by the switch) or **SECONDARY** (the SFM is operating in redundant mode).
Power Provision	The number of Watts used by this SFM.

Release History

Release 5.1; command was introduced.

Related Commands

fabric standby	Sets a Switch Fabric Module (SFM) from active to standby mode.
power fabric	Turns the power on or off for a specified Switch Fabric Module (SFM).
show cmm	Displays basic hardware and status information for CMM modules running in the chassis.
show chassis	Displays basic configuration and status information for the switch chassis.

1 Chassis MAC Server (CMS) Commands

The Chassis MAC Server (CMS) manages MAC addresses on the switch. The MAC addresses managed via the CMS are used as identifiers for the following functions:

- Base chassis MAC address
- Ethernet Management Port (EMP)
- VLAN router ports

Similar to IP addresses, MAC addresses are assigned by the Internet Assigned Numbers Authority (IANA) and distributed to users in sequential blocks. A sequential block of MAC addresses is referred to as a MAC address *range*.

The MAC address range is stored on the switch's EEPROM. The switch supports one MAC address range only. By default, this MAC address range contains thirty-two (32) factory-installed, contiguous MAC addresses. Users may add additional MAC addresses; the maximum capacity for the switch's default range is 256 MAC addresses.

MIB information for the Chassis MAC Server commands is as follows:

Filename: AlcatelIND1MacServer.MIB
Module: ALCATEL-IND1-MAC-SERVER-MIB

A summary of the available commands is listed here:

mac-range eeprom
show mac-range
show mac-range alloc

mac-range eeprom

Modifies the default MAC range on the switch's EEPROM.

Note. Use caution when modifying the default MAC range. Improper use of this command can disable your system and adversely affect your network. Contact Alcatel Customer Support for further assistance.

mac-range eeprom *start_mac_address count*

Syntax Definitions

start_mac_address	The first MAC address in the modified range. Enter the MAC address in the following format: **xx:xx:xx:xx:xx:xx**, where **x** is a hex value (0-f).
count	Specifies the number of MAC addresses in the range (1–256).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Because the factory-installed 32 MAC addresses are sufficient for most network configurations, this command should only be used by qualified network administrators for special network requirements.
- After modifying a MAC address range using the **mac-range eeprom** command, you must reboot the switch. Otherwise, MAC addresses for existing VLAN router ports will not be allocated properly.
- All MAC addresses in a range must be contiguous (i.e., there cannot be any gaps in the sequence of MAC addresses).

Examples

```
-> mac-range eeprom 00:20:da:23:45:35 32
```

Release History

Release 5.1; command was introduced.

Related Commands

show mac-range	Displays the MAC range table.

MIB Objects

```
chasMacAddressRangeTable
   chasMacRangeIndex
   chasGlobalLocal
   chasMacAddressStart
   chasMacAddressCount
```

show mac-range

Displays the MAC range table.

show mac-range [*index***]**

Syntax Definitions

index	Identifies the MAC range by referring to its position in the MAC range table.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Because the switch currently supports one MAC address range only, index position 1 displays.

Examples

```
-> show mac range

 Mac                    Local/
Range  Row Status       Global   Start Mac Addr     End Mac Addr
-----+----------------+--------+-----------------+-----------------

01     ACTIVE           GLOBAL   00:d0:95:6a:79:6e  00:d0:95:6a:79:8d
```

output definitions

Mac Range	The MAC range index number (1). Because the switch currently supports one MAC address range only, index position 1 displays.
Row Status	The current status of the MAC range. The status **ACTIVE** refers to MAC addresses that are available for allocation to VLAN router ports and other applications.
Local/Global	The Local/Global status for MAC addresses in the range. Local MAC addresses have the local bit set in the first byte of the address. Global MAC addresses (also referred to as *EEPROM* MAC addresses) have the global bit set in the first byte of the address and are stored on the switch's EEPROM. Because the switch's default MAC range is stored on EEPROM, the status GLOBAL displays.
Start Mac Addr	The first MAC address in the MAC address range.
End Mac Addr	The last MAC address in the MAC address range.

Release History

Release 5.1; command was introduced.

Related Commands

mac-range eeprom	Modifies the default MAC range on the switch's EEPROM.

MIB Objects

```
chasMacAddressRangeTable
   chasMacRangeIndex
   chasGlobalLocal
   chasMacAddressStart
   chasMacAddressCount
   chasMacRowStatus
```

show mac-range alloc

Displays all allocated addresses from the MAC range table.

show mac-range [*index***] alloc**

Syntax Definitions

index	Identifies the MAC range by referring to its position in the MAC range table. Currently, index position 1 only is supported.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If you are assigning VLAN router ports while the switch is in *single MAC router mode*, all VLAN router ports will use the base chassis MAC address (ID value 0).
- OmniSwitch 6600 switches support single MAC router mode *only*; OmniSwitch 7700, 7800, and 8800 switches support both single MAC router mode and *multiple MAC router mode*. Refer to your *Switch Management Guide* for additional information on MAC router modes.

Examples

```
-> show mac-range alloc
Range    Mac Address         Application     Id
-----+----------------+--------------------+---
01    00:d0:95:6b:09:40 CHASSIS              0
01    00:d0:95:6b:09:41 802.1X               0
01    00:d0:95:6b:09:5f CHASSIS              1
```

output definitions

Range	The MAC range's index number. The index number refers to the position of the range in the MAC range table. Values may range from 1–20. MAC ranges are divided by index number into four distinct categories. Refer to page 3-4 for more information.
Mac Address	Current MAC address allocated for a specific application.

output definitions (continued)

Application	The application for which the allocated MAC address is being used. Current options include **VLAN, 802.1X**, and **CHASSIS**. VLAN refers to MAC addresses allocated to VLAN router ports in multiple MAC router mode. CHASSIS refers to MAC addresses used for the base chassis MAC address and the Ethernet Management Port (EMP).
Id	An ID number used to identify an allocated MAC address. ID numbers are used for the base chassis MAC address and Ethernet Management Port (EMP), as well as VLAN router ports. The ID value 0 is reserved for the switch's base chassis MAC address. The ID value 1 is reserved for the EMP MAC address. Router ports assigned to VLANs 2 through 4094 are given corresponding MAC IDs. For example, a router port configured on VLAN 44 receives an allocated MAC ID of 44. Because default VLAN 1 router ports use the base chassis MAC address by default, any router port configured on VLAN 1 is assigned the ID value 0.

Release History

Release 5.1; command was introduced.

Related Commands

mac-range eeprom	Modifies the default MAC range on the switch’s EEPROM.

MIB Objects

```
ChasMacAddressAllocTable
   chasAppId
   chasObjectId
   chasAllocMacRangeIndex
   chasAllocMacAddress
```

4 Power over Ethernet (PoE) Commands

The Power over Ethernet (PoE) feature is supported on OmniSwitch 7700/7800 switches using OS7-ENI-P24 Ethernet modules and a peripheral power shelf (which holds up to four -48V hot-swappable power supplies) and the OmniSwitch 6600-P24. Refer to the *OmniSwitch 7700/7800 Hardware Users Guide* and the *OmniSwitch 6600 Family Hardware Users Guide* for details.

Note on Terminology. There are several general terms used to describe this feature. The terms *Power over Ethernet (PoE)*, *Power over LAN (PoL)*, *Power on LAN (PoL)*, and *Inline Power* are synonymous terms used to describe the powering of attached devices via Ethernet ports. For consistency, this chapter and the *OmniSwitch CLI Reference Guide* refer to the feature as *Power over Ethernet (PoE)*.

Additional terms, such as *Powered Device (PD)* and *Power Source Equipment (PSE)* are terms that are not synonymous, but are directly related to PoE.

- *PD* refers to any attached device that uses a PoE data cable as its only source of power. Examples include access points such as IP telephones, Ethernet hubs, wireless LAN stations, etc.
- *PSE* refers to the actual hardware source of the electrical current for PoE. In the case of OS7700 and OS7800 switches, the PSE is the peripheral power shelf unit, which contains up to four -48V hot-swappable power supplies. In the case of the OS6600-P24 the PSE is contained within the chassis and can be augmented by the backup inline power supply (OS6600-BPS-P).

PoE commands documented in this section comply with IEEE 802.3 and 802.af.

MIB information for the PoE commands is as follows:

Filename: AlcatelIND1InLinePowerEthernet_mib
Module: ALCATEL-IND1-INLINE-POWER-MIB

Filename: AaIETF_HUBMIB_POWER_ETHERNET_DRAFT_mib
Module: POWER-ETHERNET-MIB

A summary of the available commands is listed here:

lanpower start
lanpower stop
lanpower power
lanpower maxpower
lanpower priority
lanpower priority-disconnect
lanpower redundant-power
lanpower capacitor-detection
show lanpower
show lanpower capacitor-detection
show lanpower priority-disconnect
show lanpower slot-priority

lanpower start

Activates Power over Ethernet on a single specified PoE port *or* on all PoE ports in a specified slot.

lanpower start {*slot/port* **|** *slot***}**

Important. Inline power is *not activated* until the **lanpower start** *slot* syntax is issued for the applicable PoE slot(s).

Syntax Definitions

slot/port	Activates inline power on the specified PoE port only. This syntax is used to re-enable power to an *individual port* that has been manually turned off via the **lanpower stop** command.
slot	Activates inline power on all PoE ports in the corresponding slot.

Defaults

Power over Ethernet operational status is globally disabled by default.

Platforms Supported

OmniSwitch 6600-P24, 7700, 7800

Usage Guidelines

Use the *slot/port* syntax to activate power on a particular port. When *all* ports in a slot are manually turned off, use only the *slot* syntax in the command line. This activates power on all ports in the specified slot. As noted above, inline power is *not active* until the **lanpower start** *slot* syntax is issued for the applicable PoE slot(s).

Examples

```
-> lanpower start 5/11
-> lanpower start 5
```

Release History

Release 5.1; command was introduced.

Related Commands

lanpower stop	Manually disconnects power on a single specified PoE port or on all PoE ports in a specified slot.
show lanpower	Displays current inline power status and related statistics for all PoE ports in a specified slot.

MIB Objects

```
alaPethMainPseGroup
   alaPethMainPseAdminStatus
pethPsePortTable
   pethPsePortAdminEnable
```

lanpower stop

Manually disables power on a single specified PoE port *or* on all PoE ports in a specified slot.

lanpower stop {*slot/port* **|** *slot***}**

Syntax Definitions

slot/port	Disables inline power on the specified PoE port only.
slot	Disables inline power on all PoE ports in the corresponding slot.

Defaults

Power over Ethernet operational status is globally disabled by default.

Platforms Supported

OmniSwitch 6600-P24, 7700, 7800

Usage Guidelines

N/A

Examples

```
-> lanpower stop 5/22
-> lanpower stop 5
```

Release History

Release 5.1; command was introduced.

Related Commands

lanpower start	Activates inline power on a single specified PoE port *or* on all PoE ports in a specified slot.
show lanpower	Displays current inline power status and related statistics for all PoE ports in a specified slot.

MIB Objects

```
alaPethMainPseGroup
   alaPethMainPseAdminStatus
pethPsePortTable
   pethPsePortAdminEnable
```

lanpower power

Specifies the maximum amount of inline power, in milliwatts, allocated to *a specific PoE port*. The value specified is used to supply inline power to devices such as IP telephones and wireless LAN devices.

lanpower {*slot/port* **|** *slot***} power** *milliwatts*

Syntax Definitions

slot/port	A PoE port on which the maximum amount of inline power is being allocated.
milliwatts	The maximum amount of inline power, in milliwatts, being allocated to the corresponding port (3000–20000).

Defaults

parameter	default
milliwatts	15400

Platforms Supported

OmniSwitch 6600-P24, 7700, 7800

Usage Guidelines

- To globally specify the amount of inline power allocated to *all ports in a slot*, refer to the **lanpower maxpower** command on page 4-8.
- Be sure that the value specified complies with specific power requirements for all attached IP telephones and wireless LAN devices.
- Note that the power value for the **lanpower power** command is specified in milliwatts (mW); the related command, **lanpower maxpower**, is specified in watts (W).

Examples

```
-> lanpower 3/1 power 3025
```

Release History

Release 5.1; command was introduced.

Related Commands

lanpower maxpower	Specifies the maximum amount of inline power, in watts, allocated to all PoE ports in a specified slot.
show lanpower	Displays current inline power status and related statistics for all PoE ports in a specified slot.

MIB Objects

```
alaPethPsePortTable
   alaPethPsePortPowerMaximum
```

lanpower maxpower

Specifies the maximum amount of inline power, in watts, allocated to *all PoE ports in a specified slot*.

lanpower {*slot/port* | *slot***} maxpower** *watts*

Syntax Definitions

slot	The slot containing PoE ports on which the maximum amount of inline power allowed is being allocated.
watts	The maximum amount of inline power, in watts, allocated to all PoE ports in the corresponding slot (37–210).

Defaults

parameter	default
watts	210

Platforms Supported

OmniSwitch 6600-P24, 7700, 7800

Usage Guidelines

- Before changing the maximum slot-wide power allowance, you must disable PoE for the slot via the **lanpower stop** command. Once the new value is assigned, re-enable PoE for the slot via the **lanpower start** command.
- To specify the maximum amount of inline power allocated to a *single port*, refer to the **lanpower power** command on page 4-6.
- Note that the power value for the **lanpower maxpower** command is specified in watts (W); the related command, **lanpower power**, is specified in milliwatts (mW).

Examples

```
-> lanpower 3 maxpower 200
```

Release History

Release 5.1; command was introduced.

Related Commands

lanpower power	Specifies the maximum amount of inline power, in milli-watts, allocated to a specific PoE port.
show lanpower	Displays current inline power status and related statistics for all PoE ports in a specified slot.

MIB Objects

```
alaPethMainPseGroup
   alaPethMainPseMaxPower
```

lanpower priority

Specifies an inline power priority level to a port. Levels include critical, high, and low.

lanpower *slot/port* **priority {critical | high | low}**

Syntax Definitions

slot/port	The particular port on which a priority level is being configured.
critical	Intended for ports that have mission-critical devices attached, and therefore require top (i.e., critical) priority. In the event of a power management issue, inline power to critical ports is maintained as long as possible.
high	Intended for ports that have important, but *not* mission-critical, devices attached. If other ports in the chassis have been configured as critical, inline power to high-priority ports is given second priority.
low	Intended for ports that have low-priority devices attached. In the event of a power management issue, inline power to low-priority ports is interrupted first (i.e., before critical- and high-priority ports).

Defaults

parameter	default
low | high | critical	**low**

Platforms Supported

OmniSwitch 6600-P24, 7700, 7800

Usage Guidelines

N/A

Examples

```
-> lanpower 2/16 priority low
```

Release History

Release 5.1; command was introduced.

Related Commands

show lanpower	Displays current inline power status and related statistics for all PoE ports in a specified slot.

MIB Objects

```
pethPsePortGroup
   pethPsePortPowerPriority
```

lanpower priority-disconnect

Enables or disables the priority disconnect function on all ports in a specified slot. Priority disconnect is used by the system software in determining whether an incoming PD will be granted or denied power when there are too few watts remaining in the PoE power budget for an additional device. For detailed information on this function, refer to the "Managing Power over Ethernet (PoE)" chapter in the *OmniSwitch 7700/7800 Hardware Users Guide* and the "Managing Power over Ethernet (PoE)" chapter in the *OmniSwitch 6600 Family Hardware Users Guide.*

lanpower *slot* **priority-disconnect {enable | disable}**

Syntax Definitions

slot	The particular slot on which the priority disconnect function is being enabled or disabled.
enable	Enables priority disconnect on a specified port. When this function is enabled *and* a power budget deficit occurs in which there is inadequate power for an incoming device, the system software uses priority disconnect rules to determine whether an incoming device will be granted or denied power. For information on priority disconnect rules, refer to the "Managing Power over Ethernet (PoE)" chapter in the *OmniSwitch 7700/7800 Hardware Users Guide* and the "Managing Power over Ethernet (PoE)" chapter in the *OmniSwitch 6600 Family Hardware Users Guide*.
disable	Disables priority disconnect on a specified port. When priority disconnect is disabled and there is inadequate power in the budget for an additional device, power will be denied to *any* incoming PD, regardless of its priority status.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6600-P24, 7700, 7800

Usage Guidelines

N/A

Examples

```
-> lanpower 2 priority-disconnect disable
```

Release History

Release 5.1; command was introduced.

Related Commands

lanpower priority	Specifies an inline power priority level to a port. Levels include critical, high, and low.
show lanpower priority-disconnect	Displays the priority disconnect function status on all ports in a specified slot.

MIB Objects

```
alaPethMainPseTable
  alaPethMainPsePriorityDisconnect
```

lanpower redundant-power

Enables or disables power supply redundancy for Power over Ethernet on the switch.

lanpower redundant-power {enable | disable}

Syntax Definitions

enable	Enables redundant power on the switch.
disable	Disables redundant power on the switch.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 7700, 7800

Usage Guidelines

- In order to comply with 911 emergency requirements, PoE power redundancy status must be *enabled* at all times. For additional requirements, refer to the “Managing Power over Ethernet (PoE)” chapter in the *OmniSwitch 7700/7800 Users Guide*.
- This command is not supported on the OmniSwitch 6600-P24.

Examples

```
-> lanpower redundant-power enable
```

Release History

Release 5.1; command was introduced.

Related Commands

N/A

MIB Objects

```
alaPethMainTable
  alaPethMainPowerRedundancy
```

lanpower capacitor-detection

Enables or disables the capacitor detection method.

lanpower *slot* **capacitor-detection {enable | disable}**

Syntax Definitions

slot	The particular slot on which the capacitor detection method is being enabled or disabled.
enable	Enables the capacitor detection method.
disable	Disables redundant power on the switch.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6600-P24, 7700, 7800

Usage Guidelines

The capacitor detection method should only be enabled if there are legacy IP phones attached to the corresponding slot—this feature is *not* compatible with IEEE specification 802.3af. Please contact your Alcatel sales engineer or Customer Support representative to find out which Alcatel IP phones models need capacitive detection enabled.

Examples

```
-> lanpower 3 capacitor-detection enable
```

Release History

Release 5.1; command was introduced.

Related Commands

show lanpower capacitor-detection	Displays capacitor detection method status.

MIB Objects

```
alaPethMainTable
  alaPethMainPseCapacitorDetect
```

show lanpower

Displays current inline power status and related statistics for all PoE ports in a specified slot.

show lanpower *slot*

Syntax Definitions

slot	The slot for which current inline power status and related statistics are to be displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6600-P24, 7700, 7800

Usage Guidelines

N/A

Examples

```
-> show lanpower 8
Port Maximum(mW) Actual Used(mW)        Status       Priority  On/Off
----+-----------+---------------+--------------------+---------+------
  1      15400        3000          Powered Off         Low       ON
  2      15400        3000          Powered Off         Low       ON
  3      15400        3000          Powered Off         Low       ON
  4      15400        3000          Powered Off         Low       ON
  5      15400        3000          Powered On          High      ON
  6      15400        3000          Powered Off         Low       ON
  7      15400        3000          Powered Off         Low       ON
  8      15400        3000          Powered Off         Low       ON
  9      15400        3000          Powered Off         Low       ON
 10      15400        3000          Powered Off         Low       ON
 11      15400        3000          Powered On          Critical  ON
 12      15400        3000          Powered Off         Low       ON
 13      15400        3000          Powered Off         Low       ON
 14      15400        3000          Powered Off         Low       ON
 15      15400        3000          Powered Off         Low       ON
 16      15400        3000          Powered Off         Low       ON
 17      15400        3000          Powered Off         Low       ON
 18      15400        3000          Powered Off         Low       ON
 19      15400        3000          Powered Off         Low       ON
 20      15400        3000          Powered Off         Low       ON
 21      15400        3000          Powered Off         Low       ON
 22      15400        3000          Powered Off         Low       ON
 23      15400        3000          Powered Off         Low       ON
 24      15400        3000          Powered Off         Low       ON
```

(Output continued on next page)

```
Slot 8 Max Watts 150
364 Watts Total Power Budget Remaining
514 Watts Total Power Budget Available
1 Power Shelf Power Supplies Available
```

output definitions

Port	A PoE port for which current status and related statistics are being displayed.
Maximum (mW)	The current maximum amount of power allocated to the corresponding PoE port, in milliwatts. The default value is 15400. To change this setting, use the **lanpower power** command.
Actual Used (mW)	The actual amount of power being used by an attached device (if applicable), in milliwatts. If no device is attached to the corresponding port, this row displays a value of 0.
Status	Displays the current operational status. Options include **Powered On**, **Powered Off**, and **Undefined**.
Priority	The current priority level for the corresponding PoE port. Options include **Critical**, **High**, and **Low**. **Critical** should be reserved for ports that have mission-critical devices attached, and therefore require top (i.e., critical) priority. In the event of a power management issue, inline power to critical ports is maintained as long as possible. **High** indicates ports that have important, but not mission-critical, devices attached. If other ports in the chassis have been configured as critical, inline power to high-priority ports is given second priority. **Low** priority is for ports that have low-priority devices attached. In the event of a power management issue, inline power to low-priority ports is interrupted first (i.e., before critical and high-priority ports). The default value is Low. Priority levels can be changed using the **lanpower priority** command.
On/Off	Displays whether a port has been manually turned on or off by the user. **ON** indicates that the port has been turned on by the user via the **lanpower start** command. **OFF** indicates that the port has been turned off by the user via the **lanpower stop** command.
Measured Watts Consumption	The total amount of power, in watts, currently being used by all attached Powered Devices (PDs) in the corresponding slot.
Max Watts	The maximum watts allocated to the corresponding slot. The maximum watts value for a slot can be changed using the **lanpower maxpower** command.
Total Power Budget Remaining	The amount of power budget remaining that can be allocated for PoE modules (e.g., OS7-ENI-P24s). If the total power budget remaining is exceeded, a power error will occur and the switch's chassis management software will begin shutting down power to PoE ports according to their priority levels.
Total Power Budget Available	The total amount of power that can be allocated, based upon the number of power supplies installed and operating in the power shelf.
Power Shelf Power Supplies Available	The number of power supplies currently installed and operating in the switch's power shelf (1–4). The power shelf is also referred to as Power Source Equipment (PSE).

Release History

Release 5.1; command was introduced.

Related Commands

N/A

MIB Objects

```
alaPethMainPseGroup
   alaPethMainPseAdminStatus
pethPsePortTable
   pethPsePortAdminEnable
alaPethPsePortTable
   alaPethPsePortPowerMaximum
alaPethMainPseGroup
   alaPethMainPseMaxPower
   pethMainPsePower
pethPsePortGroup
   pethPsePortPowerPriority
```

show lanpower capacitor-detection

Displays the capacitor detection method status.

show lanpower capacitor-detection *slot*

Syntax Definitions

slot	The particular slot on which the capacitor detection method status is being displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6600-P24, 7700, 7800

Usage Guidelines

N/A

Examples

```
-> show lanpower capacitor-detection 2
Capacitor Detection enabled on Slot 2
```

Release History

Release 5.1; command was introduced.

Related Commands

lanpower capacitor-detection	Enables or disables the capacitor detection method.

MIB Objects

```
alaPethMainTable
  alaPethMainPseCapacitorDetect
```

show lanpower priority-disconnect

Displays the priority disconnect function status on all ports in a specified slot.

show lanpower priority-disconnect *slot*

Syntax Definitions

slot	The particular slot on which the priority disconnect function status you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 6600-P24, 7700, 7800

Usage Guidelines

N/A

Examples

```
-> show lanpower priority-disconnect 2
Slot 2 Priority Disconnect Enabled!
```

Release History

Release 5.1; command was introduced.

Related Commands

lanpower priority-disconnect	Enables or disables the priority disconnect function on all ports in a specified slot.

MIB Objects

```
alaPethMainPseTable
   alaPethMainPsePriorityDisconnect
```

show lanpower slot-priority

Displays the order in which a particular daughter module will be disabled if a power shelf power supply goes down, thus affecting the power budget available to the chassis.

show lanpower slot-priority *slot*

Syntax Definitions

slot	The particular slot on which the slot priority status you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800

Usage Guidelines

This command is not supported on the OmniSwitch 6600-P24.

Examples

```
-> show lanpower slot-priority 1
slot 1 priority High!
```

Release History

Release 5.1; command was introduced.

Related Commands

lanpower priority-disconnect	Enables or disables the priority disconnect function on all ports in a specified slot.

MIB Objects

```
alaPethMainPseTable
   alaPethMainPsePriority
```

5 Network Time Protocol Commands

The Network Time Protocol (NTP) is used to synchronize the time of a computer client or server to another server or reference time source, such as a radio or satellite receiver. It provides client time accuracies within a millisecond on LANs, and up to a few tens of millisecond on WANs. Typical NTP configurations utilize multiple redundant servers and diverse network paths in order to achieve high accuracy and reliability.

It is important for networks to maintain accurate time synchronization between network nodes. The standard timescale used by most nations of the world is based on a combination of Universal Coordinated Time (UTC) (representing the Earth's rotation about its axis), and the Gregorian Calendar (representing the Earth's rotation about the Sun). UTC time is disseminated by various means, including radio and satellite navigation systems, telephone modems, and portable clocks.

The MIB information for NTP is as follows:

Filename: AlcatelIND1Ntp.mib
Module: alcatelIND1NTPMIB

A summary of available commands is listed here:

ntp server
ntp client
ntp broadcast
ntp broadcast-delay
ntp key
ntp key load
show ntp client
show ntp server status
show ntp client server-list
show ntp keys

ntp server

Specifies an NTP server from which this switch will receive updates.

ntp server {*ip_address* **|** *domain_name***} [key** *key* **| version** *version* **| minpoll** *exponent* | **prefer]**

no ntp server {*ip_address* **|** *domain_name***}**

Syntax Definitions

ip_address	The IP address of the NTP server to be added or deleted to the client's server list.
domain_name	The domain name of the NTP server to be added or deleted to the client's server list. This is usually a text string.
key	The key identification number that corresponds to the specified NTP server.
version	The version of NTP being used. This will be 1, 2, 3, or 4.
exponent	The number of seconds between polls to this server. This number is determined by raising 2 to the power of the number entered. Therefore, if 4 were entered, the minimum poll time would be 16 seconds (2^4 = 16).
prefer	Marks this server as the preferred server. A preferred server's timestamp will be used before another server.

Defaults

Parameter	Default
version	4
exponent	6
prefer	not preferred

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- To configure NTP in client mode you must first define the NTP servers. Up to 3 NTP servers may be defined.
- Either an IP address or domain name for the specified server can be entered.
- The NTP key identification is an integer. It corresponds to an MD5 authentication key contained in an authentication file (.txt) located on the server. This file must be on both the server and the local switch, and match, for authentication to work. Enter the key identification using the **key** keyword if the server is set to MD5 authentication.

- Use the **version** keyword to set the correct version of NTP.
- Use the **minpoll** keyword to set the minimum poll time for the server. This number is determined by raising 2 to the power of the number entered. Therefore, if 4 were entered, the minimum poll time would be 16 seconds ($2^4 = 16$). The client will poll the server for a time update when the **minpoll** time is exceeded.
- The **no** form of this command deletes the specified server.

Examples

```
-> ntp server 1.1.1.1
-> ntp server spartacus
-> ntp server 1.1.1.1 key 1
-> ntp server 1.1.1.1 version 4
-> ntp server spartacus minpoll 5
-> no ntp server 1.1.1.1
```

Release History

Release 5.1; command was introduced.

Related Commands

ntp client	Enables or disables NTP operation on the switch.

MIB Objects

```
ALANTPCONFIG
   alaNtpPeerAddressType
   alaNtpPeerType
   alaNtpPeerAuth
   alaNtpPeerVersion
   alaNtpPeerMinpoll
   alaNtpPeerPrefer
   alaNtpPeerAddress
```

ntp client

Enables or disables NTP operation on the switch.

ntp client {enable | disable}

Syntax Definitions

enable	Enables NTP.
disable	Disables NTP.

Defaults

NTP protocol is disabled by default.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use this command to enable or disable NTP. Before NTP can be enabled, an NTP server must be specified using the **ntp server** command.

Examples

```
-> ntp client enable
-> ntp client disable
```

Release History

Release 5.1; command was introduced.

Related Commands

ntp server	Specifies an NTP server from which this switch will receive updates.

MIB Objects

```
alaNtpEnable
```

ntp broadcast

Enables or disables the client's broadcast mode.

ntp broadcast {enable | disable}

Syntax Definitions

enable	Enables the client broadcast mode.
disable	Disables the client broadcast mode.

Defaults

Broadcast mode is disabled by default.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Broadcast mode is intended for operation on networks with numerous workstations and where the highest accuracy is not required. In a typical scenario, one or more time servers on the network broadcast NTP messages that are received by NTP hosts. Correct time is determined from this NTP message based on a pre-configured latency or broadcast delay in the order of a few milliseconds.

Examples

```
-> ntp broadcast enable
-> ntp broadcast disable
```

Release History

Release 5.1; command was introduced.

Related Commands

ntp broadcast-delay	Sets the broadcast delay time in microseconds.

MIB Objects

```
alaNtpBroadcastEnable
```

ntp broadcast-delay

Sets the broadcast delay time in microseconds.

ntp broadcast delay *microseconds*

Syntax Definitions

microseconds	The number of microseconds for the broadcast delay.

Defaults

parameter	default
microseconds	4000

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

When running in the NTP client broadcast mode, a broadcast delay must be set. The broadcast delay is the number of microseconds added to the timestamp.

Examples

```
-> ntp broadcast delay 1000
-> ntp broadcast delay 10000
```

Release History

Release 5.1; command was introduced.

Related Commands

ntp broadcast	Enables or disables the client's broadcast mode.

MIB Objects

```
alaNtpBroadcastDelay
```

ntp key

Labels the specified authentication key identification as trusted or untrusted.

ntp key *key* **[trusted | untrusted]**

Syntax Definitions

key	The key number matching an NTP server.
trusted	Signifies the specified key is trusted and can be used for authentication.
untrusted	Signifies the specified key is not trusted and cannot be used for authentication. Synchronization will not occur with an untrusted authentication key.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Authentication keys are stored in a key file and loaded into memory when the switch boots. The keys loaded into memory are not trusted until this command is used.
- Once the keys are loaded into software (on boot up of the switch), they must be activated by being labeled as trusted. A trusted key will authenticate with a server that requires authentication as long as the key matches the server key.
- New keys must be added manually to the key file. A newly added key will not be loaded into the switch software until the **ntp key load** command is issued, or the switch is rebooted.

Examples

```
-> ntp key 5 trusted
-> ntp key 2 untrusted
```

Release History

Release 5.1; command was introduced.

Related Commands

ntp key	Sets the public key the switch uses when authenticating with the specified NTP server.
ntp client	Enables or disables authentication on the switch.

MIB Objects

```
alaNtpAccessKeyIdTable
   alaNtpAccessKeyIdKeyId
   alaNtpAccessKeyIdTrust
```

ntp key load

Loads the current key file into memory.

ntp key load

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command reloads the key file into the switch memory. This allows for new keys in the keyfile to be added to the list of keys the switch can use for authentication.
- Newly added keys must be labeled as **trusted** with the **ntp key** command before being used for authentication

Examples

```
-> ntp key load
```

Release History

Release 5.1; command was introduced.

Related Commands

ntp key	Labels the specified authentication key identification as trusted or untrusted.
ntp server	Specifies an NTP server from which this switch will receive updates.

MIB Objects

```
alaNtpAccessRereadkeyFile
```

show ntp client

Displays information about the current client NTP configuration.

show ntp client

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This command displays the current configuration parameters for the NTP client. The display is slightly different depending on what has been configured on the client. See the Examples section for more information.

Examples

```
-> show ntp client
Current time:                   SAT APR 12 2003  00:19:02 (UTC)
Last NTP update:                SAT APR 12 2003  00:06:45 (UTC)
Client mode:                    enabled
Broadcast client mode:          disabled
Broadcast delay (microseconds): 4000
```

output definitions

Current time	The current time for the NTP client.
Last NTP update	The time of the last synchronization with an NTP server.
Client mode	Whether the NTP client software is enabled or disabled.
Broadcast client mode	What NTP mode the client is running in, either client or broadcast.
Broadcast delay	The number of microseconds in the advertised broadcast delay time. This field is absent if the client broadcast mode is disabled.

Release History

Release 5.1; command was introduced.

Related Command

ntp client	Enables or disables NTP operation on the switch.

MIB Objects

```
alaNtpLocalInfo
```

show ntp client server-list

Displays a list of the servers with which the NTP client synchronizes.

show ntp client server-list

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show ntp client server-list
IP Address       Ver   Key    St     Delay        Offset         Disp
================+===+=======+====+==========+=================+==========
198.206.181.70    4       0    2      0.167             0.323      0.016
```

output definitions

IP Address	The server IP address.
Ver	The version of NTP the server is using. Versions 3 and 4 are valid.
Key	The NTP server's public key. This must be accurate and the same as the NTP server, or the client switch will not be able to synchronize with the NTP server. A zero (0) means there is no key entered.
St	The stratum of the server.
Delay	The delay received from the server in its timestamp.
Offset	The offset received from the server in its timestamp.
Disp	The dispersion value received from the server in its timestamp.

Release History

Release 5.1; command was introduced.

Related Command

ntp client	Enables or disables authentication on the switch.

MIB Objects

```
alaNtpPeerListTable
```

show ntp server status

Displays the basic server information for a specific NTP server or a list of NTP servers.

show ntp server status [*ip_address* **|** *domain_name***]**

Syntax Definitions

ip_address	The IP address of the NTP server to be displayed.
domain_name	The domain name of the server to be displayed. This is usually a text string.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command displays a selected server or a list of servers with witch the NTP client synchronizes.
- To display a specific server, enter the command with the server's IP address or domain name. To display all servers, enter the command with no server IP address.

Examples

```
-> show ntp server status
-> show ntp server status 1.1.1.1

IP address = 1.1.1.1
Prefer = yes
Version = 4
Key = 0
Stratum = 2
Minpoll = 4
Maxpoll = 10
Delay = 0.167 seconds
Offset = 0.323 seconds
Dispersion = 0.016 seconds
```

output definitions

IP address	The server IP address.
Prefer	Whether this server is a preferred server or not. A preferred server is used to synchronize the client before an non-preferred server.
Version	The version of NTP the server is using. Versions 3 and 4 are valid.
Key	The NTP server's public key. This must be accurate and the same as the NTP server, or the client switch will not be able to synchronize with the NTP server. A zero (0) means there is no key entered.

output definitions (continued)

Stratum	The stratum of the server. The stratum number is the number of hops from a UTC time source.
Minpoll	The minimum poll time. The client will poll the server for a time update every time this limit has been exceeded.
Maxpoll	The maximum poll time.
Delay	The delay received from the server in its timestamp.
Offset	The offset received from the server in its timestamp.
Dispersion	The dispersion value received from the server in its timestamp.

Release History

Release 5.1; command was introduced.

Related Command

ntp client	Enables or disables authentication on the switch.

MIB Objects

```
alaNtpPeerListTable
```

show ntp keys

Displays information about all authentication keys.

show ntp keys

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This command displays information on the authentication keys loaded into memory.

Examples

```
-> show ntp keys
Key      Status
=======+============
1        untrusted
2        untrusted
3        trusted
4        trusted
5        untrusted
6        untrusted
7        trusted
8        trusted
```

output definitions

Key	The key number corresponding to a key in the key file.
Status	Whether the key is trusted or untrusted.

Release History

Release 5.1; command was introduced.

Related Command

ntp key	Labels the specified authentication key identification as trusted or untrusted.
ntp key load	Loads the current key file into memory.

MIB Objects

```
alaNtpAccessKeyIdTable
```

6 Session Management Commands

Session Management commands are used to monitor and configure operator sessions including FTP, Telnet, HTTP (WebView), console, Secure Shell, and Secure Shell FTP on the switch. (See the SNMP Commands chapter for SNMP session commands.) The OmniSwitch 7700/7800 and OmniSwitch 8800 has the following limitations on the number of sessions allowed:

Telnet sessions allowed	4 concurrent sessions
FTP sessions allowed	4 concurrent sessions
HTTP (Web browser) sessions allowed	4 concurrent sessions
Secure Shell and Secure Shell FTP sessions allowed	8 concurrent sessions
Total sessions (Telnet, FTP, HTTP, Secure Shell and Secure Shell FTP, console)	21 concurrent sessions
SNMP sessions allowed	50 concurrent sessions

The OmniSwitch 6600 has the following limitations on the number of sessions allowed:

Telnet sessions allowed	4 concurrent sessions
FTP sessions allowed	4 concurrent sessions
HTTP (Web browser) sessions allowed	4 concurrent sessions
Total sessions (Telnet, FTP, HTTP, console)	13 concurrent sessions
SNMP sessions allowed	50 concurrent sessions

MIB information for commands in this chapter are as follows:

Filename: AlcatelInd1SessionMgr.mib
Module: AlcatelIND1SessionMgrMIB

Filename: AlcatelIND1AAA.mib
Module: Alcatel-IND1-AAA-MIB

Filename: AlcatelIND1System.mib
Module: Alcatel-IND1ConfigMgr.mib

A summary of the available commands is listed here.

session login-attempt
session login-timeout
session banner
session timeout
session prompt
session xon-xoff
prompt
show prefix
alias
show alias
user profile save
user profile reset
history size
show history
!
command-log
kill
exit
who
whoami
show session config
show session xon-xoff
more size
more
show more
telnet
ssh
show command-log
show command-log status

session login-attempt

Sets or resets the number of times a user can attempt unsuccessfully to log into the switch before the TCP connection is closed.

session login-attempt *integer*

Syntax Definitions

integer	The number of times the user can attempt to log in to the switch before the TCP connection is closed. Valid range is 1 to 10.

Defaults

Default is 3 login attempts.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> session login-attempt 5
```

Release History

Release 5.1; command was introduced.

Related Commands

show session config	Displays Session Manager information such as banner file name, session timeout value, and default prompt value.
session login-timeout	Sets or resets the amount of time the user can take to accomplish a successful login to the switch.
session timeout	Configures the inactivity timer for a CLI, HTTP (including Web-View), or FTP interface. When the switch detects no user activity for this period of time, the user is logged off the switch.

MIB Objects

```
sessionMgr
   sessionLoginAttempt
```

session login-timeout

Sets or resets the amount of time the user can take to accomplish a successful login to the switch. If the timeout period is exceeded, the TCP connection is closed by the switch.

session login-timeout *seconds*

Syntax Definitions

seconds	The number of seconds the switch allows for the user to accomplish a successful login. Valid range is from 5 to 600 seconds.

Defaults

- Login timeout default is 55 seconds.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> session login-timeout 30
```

Release History

Release 5.1; command was introduced.

Related Commands

show session config	Displays Session Manager information such as banner file name, session timeout value, default prompt value, login timer, and login attempt number.
session login-attempt	Sets or resets the number of times a user can attempt unsuccessfully to log into the switch before the TCP connection is closed.
session timeout	Configures the inactivity timer for a CLI, HTTP (including Web-View), or FTP interface. When the switch detects no user activity for this period of time, the user is logged off the switch.

MIB Objects

```
sessionMgr
   sessionLoginTimeout
```

session banner

Sets or resets the file name of the user–defined banner. The banner is a welcome banner that appears after the user sucessfully logs on to the switch.

session banner {cli | ftp} *file_name*

session banner no {cli | ftp}

Syntax Definitions

cli	Creates/modifies the CLI banner file name.
ftp	Creates/modifies the FTP banner file name.
file_name	Banner file name including the path from the switch's /flash directory. The maximum length of the filename and path is 255 characters.

Defaults

- A default banner is included in one of the switch's image files. It is automatically displayed at login so no configuration is needed.
- The user has the option of defining a custom supplementary banner or of using the default banner.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The **session banner** command is used to configure or modify the banner file *name*. You must use a text editor to edit the file containing the banner text.
- The **session banner no** command is used to disable a user defined session banner file from displaying when you log onto the switch. The text file containing the custom banner will remain on the switch until you remove it with the **rm** command.

Examples

```
-> session banner cli/switch/banner.txt
```

Release History

Release 5.1; command was introduced.

Related Commands

show session config	Displays Session Manager information such as banner file name, session timeout value, and default prompt value.

MIB Objects

```
SessionConfigTable
   SessionType
   SessionBannerFileName
```

session timeout

Configures the inactivity timer for a CLI, HTTP (including WebView), or FTP interface. When the switch detects no user activity for this period of time, the user is logged off the switch.

session timeout {cli | http | ftp} *minutes*

Syntax Definitions

cli	Sets the inactivity timeout for CLI sessions.
http	Sets the inactivity timeout for HTTP sessions.
ftp	Sets the inactivity timeout for FTP sessions.
minutes	Inactivity timeout value (in minutes). Valid range 1 to 596523.

Defaults

parameter	default
minutes	4

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The inactivity timer value may be different for each type of interface CLI (Console, Telnet), HTTP (including WebView), and FTP.
- If you change the timer, the new value does not affect current sessions; the new timer is applied to new sessions only.

Examples

```
-> session timeout cli 5
```

Release History

Release 5.1; command was introduced.

Related Commands

show session config	Displays Session Manager information such as banner file name, session timeout value, and default prompt value.

MIB Objects

```
SessionConfigTable
   SessionType
   SessionInactivityTimerValue
```

session prompt

Configures the default CLI prompt for console and Telnet sessions. The prompt is the symbol and/or text that appears on the screen in front of the cursor.

session prompt default [*string*]

Syntax Definitions

string	Prompt string.

Defaults

parameter	default
string	->

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The maximum prompt string length is 31 characters.
- The new prompt will take not take effect until you log off and back on to the switch.

Examples

```
-> session prompt default -->
```

Release History

Release 5.1; command was introduced.

Related Commands

show session config	Displays Session Manager information such as banner file name, session timeout value, and default prompt value.

MIB Objects

```
SessionConfigTable
   SessionType
   sessionDefaultPromptString
```

session xon-xoff

Enables/disables the XON-XOFF protocol on the console port.

session xon-xoff {enable | disable}

Syntax Definitions

enable	Enables XON-XOFF on the console port.
disable	Disables XON-XOFF on the console port.

Defaults

parameter	default
enable | **disable**	**disable**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

The switch may interpret noise from an RS232 line as Control-S (XOFF). If the **session console xon-xoff** command is enabled, traffic to the console port may be stopped.

Examples

```
-> session xon-xoff enable
-> session xon-xoff disable
```

Release History

Release 5.1; command was introduced.

Related Commands

show session xon-xoff	Displays whether the console port is enabled or disabled for XON-XOFF.

MIB Objects

```
sessionXonXoffEnable
```

prompt

This command defines the CLI prompt.

prompt [user] [time] [date] [string *string***] [prefix]**

no prompt

Syntax Definitions

user	The name of the current user is displayed as part of the CLI prompt.
time	The current system time is displayed as part of the CLI prompt.
date	The current system date is displayed as part of the CLI prompt.
string *string*	You can specify a text string as the prompt. Prompts specified with this parameter are limited to four characters.
prefix	The current prefix (if any) is displayed as part of the CLI prompt. Prefixes are stored for command families that support the prefix recognition feature. See Usage Guidelines.

Defaults

The default prompt is the arrow (->, or dash greater-than).

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Prefixes are stored for command families that support the prefix recognition feature. These command families include AAA, Interface, Link Aggregation, QoS, Spanning Tree, and VLAN Management. Other command families do not store a prefix.
- The “no” form of this command removes the CLI prompt.
- To set the CLI prompt back to the arrow (**->**) enter the **prompt string ->** (prompt string dash greater-than) syntax.

Examples

```
-> prompt user
-> prompt user time date
-> prompt prefix
-> prompt string 12->
-> prompt prefix ->
```

Release History

Release 5.1; command was introduced.

Related Commands

show prefix	Shows the command prefix (if any) currently stored by the CLI. Prefixes are stored for command families that support the prefix recognition feature.

MIB Objects

N/A

show prefix

Shows the command prefix (if any) currently stored by the CLI. Prefixes are stored for command families that support the prefix recognition feature.

show prefix

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Prefixes are stored for command families that support the prefix recognition feature. These command families include AAA, Interface, Link Aggregation, QoS, Spanning Tree, and VLAN Management. Other command families do not store a prefix.

Examples

```
-> show prefix
```

Release History

Release 5.1; command was introduced.

Related Commands

prompt	This command defines the format of the CLI prompt. The prompt can be defined to include the command prefix.

MIB Objects

N/A

alias

Defines substitute command text for the switch's CLI command keywords.

alias *alias command_name*

Syntax Definitions

alias	Text string that defines the new CLI command name (alias) that you will use to replace an old CLI command name.
command_name	The old CLI command name being replaced by your alias.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Alias commands are stored until the user session ends. To save alias settings, you must execute the **user profile save** command. Otherwise, once you log off the switch, substitute commands configured with the **alias** command are destroyed.
- You can eliminate excess typing by reducing the number of characters required for a command. For instance, the group syntax can be defined as gp.
- You can change unfamiliar command words into familiar words or patterns. For instance, if you prefer the term "privilege" to the term "attribute" with reference to a login account's read/write capabilities, you can change the CLI command from attrib to privileges.
- To reset commands set with alias back to their factory default, use the **user profile reset** command.

Examples

```
-> alias gp group
-> alias privilege attrib
```

Release History

Release 5.1; command was introduced.

Related Commands

show alias	Lists all current commands defined by the use of the **alias** CLI command.
user profile reset	Resets the alias, prompt and more values to their factory defaults.
user profile reset	Resets the alias, prompt and more values to their factory defaults.

MIB Objects

N/A

show alias

Lists all current commands defined by the use of the **alias** CLI command.

show alias

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

The following will display where the alias **gp** was defined to replace the **group** command, and the alias **privilege** was defined to replace the **attrib** command.

```
-> show alias
gp:        group
privilege: attrib
```

Release History

Release 5.1; command was introduced.

Related Commands

alias	Defines substitute command text for the switch's CLI command keywords.

MIB Objects

N/A

user profile save

Saves the user account settings for aliases, prompts, and the more mode screen setting. These settings will be automatically loaded when the user account logs on.

user profile save

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use this command to save alias definitions, prompt definitions, and more mode screen settings for use in future login sessions for the current user account.
- If you do not use the **user profile save** command, **alias**, **prompt**, and **more size** settings are lost when the user account logs off.
- Use the **user profile reset** command to set the alias, prompt and more size values to their factory defaults.

Examples

```
-> user profile save
```

Release History

Release 5.1; command was introduced.

Related Commands

alias	Defines substitute command text for the switch's CLI command keywords.
prompt	Defines substitute command text for the switch's CLI command keywords.
more size	Specifies the number of lines that your console screen will display.
user profile reset	Resets the alias, prompt and more values to their factory defaults.

MIB Objects

N/A

user profile reset

Resets the alias, prompt and more values to their factory defaults.

user profile reset

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> user profile reset
```

Release History

Release 5.1; command was introduced.

Related Commands

alias	Defines substitute command text for the switch's CLI command keywords.
prompt	Defines substitute command text for the switch's CLI command keywords.
more size	Specifies the number of lines that your console screen will display.
user profile save	Saves the user account settings for aliases, prompts and the more screen.

MIB Objects

N/A

history size

Sets the number of commands that will be stored in the CLI's history buffer.

history size *number*

Syntax Definitions

number	Enter an integer between 1 and 30. The history buffer can store up to 30 commands.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> history size 10
```

Release History

Release 5.1; command was introduced.

Related Commands

show history	Displays commands you have recently issued to the switch. The commands are displayed in a numbered list.
!	Recalls commands listed in the history buffer and displays them at the CLI prompt.

MIB Objects

N/A

show history

Displays commands you have recently issued to the switch. The commands are displayed in a numbered list.

show history [*parameters***]**

Syntax Definitions

parameters	When this syntax is used, the CLI displays the history buffer size, the current number of commands in the history buffer and the index range of the commands.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show history
1 show cmm
2 show fan
3 show sensor
4 show temp
5 show time
6 show arp
7 clear arp
8 show prefix

-> show history parameters
History size: 10
Current Size: 7
Index Range: 1-7
```

output definitions

History Size	The size of the history buffer.
Current Size	The number of commands currently stored in the history buffer for this session.
Index Range	The index range of the commands for this CLI session currently stored in the history buffer.

Release History

Release 5.1; command was introduced.

Related Commands

history size	Sets the number of commands that will be stored in the CLI's history buffer.
!	Recalls commands listed in the history buffer and displays them at the CLI prompt.

MIB Objects

N/A

!

Recalls commands listed in the history buffer and displays them at the CLI prompt.

!{! | *n***}**

Syntax Definitions

!	Recalls the last command listed in the history buffer and displays that command at the CLI prompt.
n	Identifies a single command in the history buffer by number and displays that command at the CLI prompt.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- You can use the **show history** command to list all commands in the history buffer, then use the **!*n*** syntax to issue a single command from the list.
- When you use **!*n*** or **!!** to recall a command in the history buffer list, you must press the Enter key to execute the command.

Examples

```
-> show history
1* show cmm
2 show fan
3 show sensor
4 show temp
5 show time
6 show arp
7 clear arp
```

Release History

Release 5.1; command was introduced.

Related Commands

history size	Sets the number of commands that will be stored in the CLI's history buffer.
show history	Displays commands you have recently issued to the switch. The commands are displayed in a numbered list.

MIB Objects

N/A

command-log

Enables or disables command logging on the switch. When command logging is enabled, a **command.log** is automatically created; this file stores a comprehensive CLI command history for all active sessions since the function was *first* enabled.

command-log {enable | disable}

Syntax Definitions

enable	Creates a file called **command.log** in the switch's **/flash** directory. Any configuration commands entered on the command line will be recorded to this file until command logging is disabled.
disable	Disables logging of current session commands to the **command.log** file.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The maximum log file size is 66,402 bytes; the file may hold up to 100 commands.

Examples

```
-> command-log enable
-> command-log disable
```

Release History

Release 5.1; command was introduced.

Related Commands

show command-log	Displays the contents of the **command.log** file.
show command-log status	Shows the current status of the command logging function (i.e., enabled or disabled).

MIB Objects

```
sessionCliCommandLogEnable
```

kill

Kills an active session. The command takes effect immediately.

kill *session_number*

Syntax Definitions

session_number	Number of the session you want to kill.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **who** command to obtain the session number variable.
- You cannot kill your own session.
- You cannot kill a connected session where the user has not yet completed the login process. These sessions appear with username “(at login)” when displayed with the **who** command.

Examples

```
-> kill 3
```

Release History

Release 5.1; command was introduced.

Related Commands

who	Displays all active login sessions (e.g., Console, Telnet, FTP, HTTP, Secure Shell, Secure Shell FTP).

MIB Objects

```
SessionMgr
   sessionIndex
   sessionRowStatus
```

exit

Ends the current CLI session. If the CLI session to the switch was via Telnet, the connection is closed.

exit

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

If changes were made using the CLI and have not been saved with the **copy running-config working** command, a warning message appears asking to confirm the user exit. To save changes, enter **N** at the warning prompt and use the **copy running-config working** command.

Examples

```
-> exit
```

Release History

Release 5.1; command was introduced.

Related Commands

kill	Kills an active session. The command takes effect immediately.

MIB Objects

```
SessionMgr
   sessionIndex
   sessionRowStatus
```

whoami

Displays the current user session.

whoami

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **who** command to display all sessions on the switch.

Examples

```
-> whoami
Session number = 5
  User name   = admin,
  Access type = telnet,
  Access port = NI,
  IP address  = 121.251.17.76,
  Read-only domains   = None,
  Read-only families  = ,
  Read-Write domains  = All ,
  Read-Write families = ,
  End-User profile    =
```

output definitions

Session Number	The session number assigned to the user.
User name	User name.
Access type	Type of access protocol used to connect to the switch.
Access port	Switch port used for access during this session.
Ip Address	User IP address.
Read-only domains	The command domains available with the user's read-only access. See the table beginning on page 6-28 for a listing of valid domains.
Read-only families	The command families available with the user's read-only access. See the table beginning on page 6-28 for a listing of valid families.
Read-Write domains	The command domains available with the user's read-write access. See the table beginning on page 6-28 for a listing of valid domains.
Read-Write families	The command families available with the user's read-write access. See the table beginning on page 6-28 for a listing of valid families.
End-User Profile	The name of an end-user profile associated with the user.

Possible values for command domains and families are listed here:

domain	families
domain-admin	file image bootrom telnet reset dshell debug
domain-system	system aip snmp rmon webmgt config
domain-physical	chassis module interface pmm flood health
domain-network	ip rip ospf bgp vrrp iprm ipx ipmr ipms
domain-layer2	vlan bridge stp 802.1q linkagg ip-helper
domain-service	ldap dhcp dns
domain-policy	qos policy slb
domain-security	session binding avlan aaa

Release History

Release 5.1; command was introduced.

Related Commands

who	Displays all active login sessions (e.g., Console, Telnet, FTP, HTTP, Secure Shell, Secure Shell FTP).
kill	Kills another user's session.

MIB Objects

```
SessionActive
   sessionIndex
   sessionAccessType
   sessionPhysicalPort
   sessionUserName
   sessionUserReadPrivileges
   sessionUserWritePrivileges
   sessionUserProfileNumber
   sessionUserIpAddress
   sessionRowStatus
```

who

Displays all active login sessions (e.g., Console, Telnet, FTP, HTTP, Secure Shell, Secure Shell FTP).

who

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

You can identify your current login session by IP address.

Examples

```
-> who
Session number = 0
  User name   = (at login),
  Access type = console,
  Access port = Local,
  IP address  = 0.0.0.0,
  Read-only domains   = None,
  Read-only families  = ,
  Read-Write domains  = None,
  Read-Write families = ,
  End-User profile    =
Session number = 5
  User name   = admin,
  Access type = telnet,
  Access port = NI,
  IP address  = 128.251.17.176,
  Read-only domains   = None,
  Read-only families  = ,
  Read-Write domains  = All ,
  Read-Write families = ,
  End-User profile    =
```

output definitions

Session Number	The session number assigned to the user.
User name	User name.
Access type	Type of access protocol used to connect to the switch.
Access port	Switch port used for access during this session.
Ip Address	User IP address.

output definitions (continued)

Read-only domains	The command domains available with the user's read-only access. See the table beginning on page 6-31 for a listing of valid domains.
Read-only families	The command families available with the user's read-only access. See the table beginning on page 6-31 for a listing of valid families.
Read-Write domains	The command domains available with the user's read-write access. See the table beginning on page 6-31 for a listing of valid domains.
Read-Write families	The command families available with the user's read-write access. See the table beginning on page 6-31 for a listing of valid families.
End-User Profile	The name of an end-user profile associated with the user.

Possible values for command domains and families are listed here:

domain	families
domain-admin	file image bootrom telnet reset dshell debug
domain-system	system aip snmp rmon webmgt config
domain-physical	chassis module interface pmm flood health
domain-network	ip rip ospf bgp vrrp iprm ipx ipmr ipms
domain-layer2	vlan bridge stp 802.1q linkagg ip-helper
domain-service	ldap dhcp dns
domain-policy	qos policy slb
domain-security	session binding avlan aaa

Release History

Release 5.1; command was introduced.

Related Commands

whoami	Displays current user session.
kill	Kills another user's session.

MIB Objects

```
SessionActive
   sessionIndex
   sessionAccessType
   sessionPhysicalPort
   sessionUserName
   sessionUserReadPrivileges
   sessionUserWritePrivileges
   sessionUserProfileNumber
   sessionUserIpAddress
   sessionRowStatus
```

show session config

Displays session manager configuration information (e.g., default prompt, banner file name, inactivity timer, login timer, login attempts).

show session config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the configuration commands detailed in this section to modify any of the values displayed.

Examples

```
-> show session config

Cli Default Prompt              = ->
Cli Banner File Name            = ,
Cli Inactivity Timer in minutes  = 60
Ftp Banner File Name            = ,
Ftp Inactivity Timer in minutes  = 60
Http Inactivity Timer in minutes = 60
Login Timer in seconds          = 60
Maximum number of Login Attempts = 2
```

output definitions

Cli Default Prompt	Default prompt displayed for CLI sessions.
Cli Banner File Name	Name of the file that contains the banner information that will appear during a CLI session.
Cli Inactivity Timer in minutes	Inactivity timer value (in minutes) for CLI sessions. The user is logged off when this value is exceeded.
Ftp Banner File Name	Name of the file that contains the banner information that will appear during an FTP session.
Ftp Inactivity Timer in minutes	Inactivity timer value (in minutes) for FTP sessions. The user is logged off when this value is exceeded.
Http Inactivity Timer in minutes	Inactivity timer value (in minutes) for HTTP (including WebView) sessions. The user is logged off when this value is exceeded.

output definitions

Login Timer in seconds	The amount of time the user can take to accomplish a successful login to the switch. If the timeout period is exceeded, the TCP connection is closed by the switch.
Maximum number of Login Attempts	The number of times a user can attempt unsuccessfully to log into the switch before the TCP connection is closed.

Release History

Release 5.1; command was introduced.

Related Commands

session prompt	Configures the default CLI prompt for console and Telnet sessions.
session banner	Sets the file name of the user–defined banner.
session timeout	Configures the inactivity timer for a CLI, HTTP (including Web-View), or FTP interface.
session login-attempt	Sets the number of times a user can attempt unsuccessfully to log into the switch before the TCP connection is closed.
session login-timeout	Sets the amount of time the user can take to accomplish a successful login to the switch.

MIB Objects

```
SessionConfigTable
   sessionType
   sessionBannerFileName
   sessionInactivityTimerValue
   sessionDefaultPromptString
```

show session xon-xoff

Displays whether the console port is enabled or disabled for XON-XOFF.

show session xon-xoff

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

The switch may interpret noise from an RS232 line as Control-S (XOFF). If the console port is enabled for XON-XOFF (through the **session xon-xoff** command), traffic to the console port may be stopped.

Examples

```
-> show session xon-xoff
XON-XOFF Enabled
```

Release History

Release 5.1; command was introduced.

Related Commands

session xon-xoff	Enables/disables the XON-XOFF protocol on the console port.

MIB Objects

```
sessionXonXoffEnable
```

more size

Specifies the number of lines that your console screen will display.

more size *lines*

Syntax Definitions

lines	Specify the number of lines for your console to display.

Defaults

parameter	default
table lines	128

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If the display from the switch contains more lines than specified with this command, the switch will display only the number of lines specified. The last line on your console will display as follows:

  ```
  More? [next screen <sp>, next line <cr>, filter pattern </>, quit </>]
  ```

- To display more lines, press the spacebar to show another full screen, press Enter to show the next line, or press q to quit the display and return to the system prompt.

Examples

```
-> more size 12
-> more size 30
```

Release History

Release 5.1; command was introduced.

Related Commands

more	Enables the more mode for your console screen display.
show more	Shows the enable status of the more mode along with the number of lines specified for the screen display.

MIB Objects

```
SystemServices
   systemServicesArg1
   systemServicesAction
```

more

Enables the more mode for your console screen display.

more

no more

Syntax Definitions

N/A

Defaults

Disabled

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This command enables the **more** mode where your console screen display is determined by the value set with the **more size** command.

Examples

```
-> more
-> no more
```

Release History

Release 5.1; command was introduced.

Related Commands

show more	Specifies the number of TTY lines and columns to be displayed.
more size	Specifies the number of lines that your console screen will display.

MIB Objects

```
SystemServices
   systemServicesArg1
   systemServicesAction
```

show more

Shows the enable status of the more mode along with the number of lines specified for the screen display.

show more

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command shows the enable status of the **more** mode.
- The number of lines displayed is the value set with the **more size** command.

Examples

```
-> show more
The more feature is enabled and the number of line is set to 12
```

Release History

Release 5.1; command was introduced.

Related Commands

more	Enables the more mode for your console screen display.
more size	Specifies the number of lines that your console screen will display.

MIB Objects

```
SystemServices
   systemServicesArg1
   systemServicesAction
```

telnet

Invokes a Telnet session. A Telnet session is used to connect to a remote system or device.

telnet {*host_name* **|** *ip_address***}**

Syntax Definitions

host_name	Specifies the host name for the Telnet session.
ip_address	Specifies the IP address for the Telnet session.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

To abort a Telnet session, enter **CTRL** + **]** and then **CTRL** + **D**. Refer to your switch's User Manual for more information on using Telnet.

Examples

```
-> telnet 172.17.6.228
Trying 172.17.6.228...
Connected to 172.17.6.228.
Escape character is '^]'.
```

Release History

Release 5.1; command was introduced.

Related Commands

ssh	Invokes a Secure Shell session. A Secure Shell session is used to make a secured connection to a remote system or device.

MIB Objects

```
SystemServices
   systemServicesArg1
   systemServicesAction
```

ssh

Invokes a Secure Shell session. A Secure Shell session is used to make a secured connection to a remote system or device.

ssh {*host_name* | *ip_address***}**

Syntax Definitions

host_name	Specifies the host name for the Secure Shell session.
ip_address	Specifies the IP address for the Secure Shell session.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

You must have a valid username and password for the specified host.

Examples

```
-> ssh 172.155.11.211
login as:
```

Release History

Release 5.1; command was introduced.

Related Commands

telnet	Invokes a Telnet session. A Telnet session is used to connect to a remote system or device.
sftp	Starts an SFTP session. An SFTP session provides a secure file transfer method.

MIB Objects

```
aaaAcctSATable
   aaacsInterface
```

show command-log

Displays the contents of the **command.log** file. This file contains a record of all CLI commands executed on the switch since the command logging function was enabled. For more information on enabling and disabling command logging, refer to page 6-24.

show command-log

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The **show command-log** command lists CLI commands in *descending order*. In other words, the most recent commands are listed first. In the example below, the **command-log enable** syntax is the *least recent* command logged; the **ip interface Marketing address 17.11.5.2 vlan 255** syntax is the *most recent*.
- By default, command logging is disabled. To enable command logging on the switch, use the **command-log** command.
- As mentioned above, command history is archived to the **command.log** file. If this file is removed, the command history will no longer be available. In addition, the **command.log** file has a 66,402 byte capacity. This capacity allows up to 100 commands; if the maximum capacity is reached, only the 100 most recent commands display.

Examples

```
-> show command-log
Command : ip interface Marketing address 17.11.5.2 vlan 255
  UserName : admin
  Date     : FRI JAN 09 00:20:01
  Ip Addr  : 128.251.19.240
  Result   : SUCCESS

Command : ip interface "Distribution" 11.255.14.102 vlan 500 local-proxy-arp
  UserName : admin
  Date     : FRI JAN 09 00:19:44
  Ip Addr  : 128.251.19.240
  Result   : ERROR: Ip Address must not belong to IP VLAN 44 subnet

Command : command-log enable
  UserName : admin
  Date     : FRI JAN 09 00:18:49
  Ip Addr  : 128.251.19.240
  Result   : SUCCESS
```

output definitions

Command	The exact syntax of the command, as entered by the user.
UserName	The name of the user session that entered the command. For more information on different user session names, refer to the **user** command on page 43-36, or the "Managing Switch User Accounts" chapter in the *Switch Management Guide*.
Date	The date and time, down to the second, when the command was entered.
IpAddr	The IP address of the terminal from which the command was entered.
Result	The outcome of the command entry. Options include **SUCCESS** and **ERROR**. For erroneous command entries, the same error details presented by the switch at the time the command was entered are also displayed in the log file.

Release History

Release 5.1; command was introduced.

Related Commands

command-log	Enables or disables command logging on the switch.
show command-log status	Shows the current status of the command logging function (i.e., enabled or disabled).

MIB Objects

```
sessionCliCommandLogEnable
```

show command-log status

Shows the current status of the command logging function (i.e., enabled or disabled). For more information on enabling and disabling command logging, refer to the **command-log** command on page 6-24.

show command-log status

Syntax Definitions

N/A

Defaults

Command logging is disabled by default.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show command-log status
CLI command logging : Enable
```

output definitions

CLI command logging	The current status of command logging on the switch. Options include **Disable** and **Enable**. Disable indicates that the command logging function is currently disabled (default). Enable indicates that the command logging function has been enabled via the **command-log** command. For more information, refer to page 6-24.

Release History

Release 5.1; command was introduced.

Related Commands

command-log	Enables or disables command logging on the switch.
show command-log	Displays the contents of the **command.log** file.

MIB Objects

```
sessionCliCommandLogStatus
```

7 File Management Commands

This chapter includes descriptions for CLI commands used to manage files on the switch. Several of these commands are used to create, move, and delete both files and directories in the OmniSwitch flash directory. Other commands allow you to change command privileges and to monitor the switch's memory.

MIB information for the system commands is as follows:

Filename: AlcatelIND1System.MIB
Module: ALCATEL-IND1-SYSTEM-MIB

Filename: AlcatelIND1Chassis.mib
Module: ALCATEL-IND1-CHASSIS-MIB

A summary of the available commands is listed here:

File System	**cd** **pwd** **mkdir** **rmdir** **ls** **dir** **rename** **rm** **delete** **cp** **mv** **move** **chmod** **attrib** **freespace** **fsck** **newfs** **rcp** **rrm** **rls** **rdf**
System Services	**vi** **view** **tty** **show tty** **more** **ftp** **sftp** **rz** **install**

cd

Changes the switch's current working directory.

cd [*path***]**

Syntax Definitions

path	Specifies a particular working directory. If no path is specified, the switch's working directory is changed to the top level.

Defaults

The switch's default working directory is **/flash**.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Up to 255 characters may be used for a fully qualified path.
- A path can contain up to a maximum of seven (7) directories including /flash.
- As with files names, up to thirty-two (32) characters may be used for a directory name.
- File and directory names can include only the following character types: a-z, A-Z, 0-9, dashes (-), dots (.), and underscores (_).
- This command can also be used on the secondary CMM.

Examples

```
-> cd
-> cd test_path
```

Release History

Release 5.1; command was introduced.

Related Commands

pwd	Displays the switch's current working directory.
mkdir	Creates a new directory.
rmdir	Deletes an existing directory.
ls	Displays the contents of a specified directory or the current working directory.
dir	Displays the contents of a specified directory or the current working directory.

MIB Objects

```
systemServices
   systemServicesWorkingDirectory
```

pwd

Displays the switch's current working directory.

pwd

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This command can also be used on the secondary CMM.

Examples

```
-> pwd
/flash
```

Release History

Release 5.1; command was introduced.

Related Commands

cd	Changes the switch's current working directory.
mkdir	Creates a new directory.
rmdir	Deletes an existing directory.
ls	Displays the contents of a specified directory or the current working directory.
dir	Displays the contents of a specified directory or the current working directory.

MIB Objects

```
systemServices
   systemServicesWorkingDirectory
```

mkdir

Creates a new directory.

mkdir [*path/***]***dir*

Syntax Definitions

path	The path in which the new directory is being created. If no path is specified, the new directory is created in the current path.
dir	A user-defied name for the new directory. Up to thirty-two (32) characters may be used (e.g., **test_directory**).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Be sure to separate path directories with a slash (/). Refer to the examples below.
- Up to 255 characters may be used for a fully qualified path.
- A path can contain up to a maximum of seven (7) directories including /flash.
- As with files names, up to thirty-two (32) characters may be used for a directory name.
- File and directory names can include only the following character types: a-z, A-Z, 0-9, dashes (-), dots (.), and underscores (_).
- This command can also be used on the secondary CMM.

Examples

```
-> mkdir test_directory
-> mkdir flash/test_directory
```

Release History

Release 5.1; command was introduced.

Related Commands

cd	Changes the switch's current working directory.
pwd	Displays the switch's current working directory.
rmdir	Deletes an existing directory.
ls	Displays the contents of a specified directory or the current working directory.
dir	Displays the contents of a specified directory or the current working directory.

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesAction
```

rmdir

Deletes an existing directory.

rmdir [*path/***]***dir*

Syntax Definitions

path	The path containing the directory to be removed. If no path is specified, the command assumes the current path.
dir	The name of the existing directory being removed. Up to thirty-two (32) characters may be used (e.g., **test_directory**).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Be sure to separate path directories with a slash (/). Refer to the examples below.
- Up to 255 characters may be used for the specified path.
- This command can also be used on the secondary CMM.

Examples

```
-> rmdir ../working
-> rmdir flash/working
```

Release History

Release 5.1; command was introduced.

Related Commands

cd	Changes the switch's current working directory.
pwd	Displays the switch's current working directory.
mkdir	Creates a new directory.
ls	Displays the contents of a specified directory or the current working directory.
dir	Displays the contents of a specified directory or the current working directory.

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesAction
```

ls

Displays the contents of a specified directory or the current working directory.

ls [-r] [[*path/***]***dir***]**

Syntax Definitions

-r	Optional syntax that displays the contents of the current directory in addition to *recursively* displaying all subdirectories. Be sure to include a space between the syntax **ls** and **-r** (i.e., **ls -r**).
path/	Specifies the path (i.e., location) of a particular directory to be displayed. If no path is specified, the command assumes the current location.
dir	Specifies a particular directory to be displayed. If no directory name is specified, the contents of the current working directory are displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Be sure to separate multiple path directories with a slash (/).
- Up to 255 characters may be used for a fully qualified path.
- A path can contain up to a maximum of seven (7) directories including /flash.
- As with files names, up to thirty-two (32) characters may be used for a directory name.
- File and directory names can include only the following character types: a-z, A-Z, 0-9, dashes (-), dots (.), and underscores (_).
- This command can also be used on the secondary CMM.

Examples

```
-> ls

Listing Directory /flash:

-rw       268 Oct  2 09:54 boot.params
drw      2048 Sep 29 15:36 certified/
drw      2048 Oct  2 05:32 working/
drw      2048 Sep 27 12:26 switch/
-rw    115837 Sep 27 15:30 debug.lnk
-rw       185 Sep 29 14:19 phwi
-rw       706 Sep 29 14:52 incrsrc2
-rw    127640 Sep 29 14:52 pktgen.o
-rw       354 Sep 29 15:48 incrsrc

        3143680 bytes free
```

Release History

Release 5.1; command was introduced.

Related Commands

cd	Changes the switch's current working directory.
pwd	Displays the switch's current working directory.
mkdir	Creates a new directory.
rmdir	Deletes an existing directory.
dir	Displays the contents of a specified directory or the current working directory.

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesAction
```

dir

Displays the contents of a specified directory or the current working directory.

dir [[*path/***]***dir***]**

Syntax Definitions

path/	Specifies the path (i.e., location) of a particular directory to be displayed. If no path is specified, the command assumes the current location.
dir	Specifies a particular directory to be displayed. If no directory name is specified, the contents of the current working directory are displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Be sure to separate multiple path directories with a slash (/).
- Up to 255 characters may be used for a fully qualified path.
- A path can contain up to a maximum of seven (7) directories including /flash.
- As with files names, up to thirty-two (32) characters may be used for a directory name.
- File and directory names can include only the following character types: a-z, A-Z, 0-9, dashes (-), dots (.), and underscores (_).
- This command can also be used on the secondary CMM.

Examples

```
-> dir /certified

Listing Directory /certified:

drw      2048 Sep 29 15:36 ./
drw      2048 Oct  2 09:54 ../
-rw    552068 Sep 27 12:24 FNS7V54.img
-rw    599477 Sep 29 14:23 Fadvrout.img
-rw    556331 Sep 29 15:36 Feni.img
-rw     76801 Sep 29 14:24 Fdiag.img
-rw    149701 Sep 29 15:36 Fenisym
-rw    469351 Sep 29 14:25 Fl2eth.img
-rw    840593 Sep 29 14:24 Fos.img
-rw    182073 Sep 29 14:24 Fqos.img
-rw    358882 Sep 29 14:24 Frout.img
-rw     91579 Sep 29 14:24 Fsecu.img
-rw      5520 Sep 29 14:24 release.img
-rw   2609508 Sep 29 14:23 Fbase.img

        3143680 bytes free
```

Release History

Release 5.1; command was introduced.

Related Commands

cd	Changes the switch's current working directory.
pwd	Displays the switch's current working directory.
mkdir	Creates a new directory.
rmdir	Deletes an existing directory.
ls	Displays the contents of a specified directory or the current working directory.

MIB Objects

```
systemServices
   systemServicesArg22
   systemServicesAction
```

rename

Renames an existing file or directory.

rename [*path/***]***old_name* **[***path/***]***new_name*

Syntax Definitions

path/	Specifies the particular path (i.e., location) containing the file or directory to be renamed. If no path is specified, the command assumes the current directory.
old_name	The name of the existing file or directory to be renamed.
new_name	The new user-defined file or directory name. Up to thirty-two (32) characters may be used.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Be sure to separate path directories and file names with a slash (/). Refer to the examples below.
- Up to 255 characters may be used for a fully qualified path.
- A path can contain up to a maximum of seven (7) directories including /flash.
- As with files names, up to thirty-two (32) characters may be used for a directory name.
- File and directory names can include only the following character types: a-z, A-Z, 0-9, dashes (-), dots (.), and underscores (_).
- This command can also be used on the secondary CMM.

Examples

```
-> rename flash/working/asc.1.snap new_file
```

Release History

Release 5.1; command was introduced.

Related Commands

cp	Copies an existing file or directory.
mv	Moves an existing file or directory to a new location.
move	Moves an existing file or directory to a new location.

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesArg2
   systemServicesAction
```

rm

Permanently deletes an existing file. This command can also delete a directory if the -r keyword is used.

rm [-r] [*path/***]***filename*

Syntax Definitions

-r	Syntax that *recursively* removes directories, as well as any associated subdirectories and files. Be sure to include a space between the syntax **rm** and **-r** (i.e., **rm -r**).
path	The path (i.e., location) containing the file being removed. If no path is specified, the command assumes the current directory.
filename	The name of the existing file being deleted. Up to thirty-two (32) characters may be used (e.g., **test_config_file**).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Be sure to separate path directories and file names with a slash (/). Refer to the examples below.
- Use care when deleting files. Depending on your switch and network configurations, specific configuration and image files must be present for your system to work properly.
- This command can also be used on the secondary CMM.

Examples

```
-> rm test_config_file
-> rm flash/test_config_file
```

Release History

Release 5.1; command was introduced.

Related Commands

delete	Deletes an existing file.

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesAction
```

delete

Deletes an existing file.

delete [*path/***]***filename*

Syntax Definitions

path/	The path (i.e., location) containing the file being removed. If no path is specified, the command assumes the current directory.
filename	The name of the existing file being removed. Up to thirty-two (32) characters may be used (e.g., **test_config_file**).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Be sure to separate path directories and file names with a slash (/). Refer to the examples below.
- Use care when deleting files. Depending on your switch and network configurations, specific configuration and image files must be present for your system to work properly.
- This command can also be used on the secondary CMM.

Examples

```
-> delete test_config_file
-> delete flash/test_config_file
```

Release History

Release 5.1; command was introduced.

Related Commands

rm	Deletes an existing file or directory.

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesAction
```

cp

Copies an existing file. This command can also copy a directory if the -r keyword is used.

cp [-r] [*path/***]***orig_filename* **[***dest_path/***]***dupl_filename*

Syntax Definitions

-r	Syntax that *recursively* copies directories, as well as any associated subdirectories and files. Be sure to include a space between the syntax **cp** and **-r** (i.e., **cp -r**).
path/	Specifies the path containing the original file to be copied. If no path name is specified, the command assumes the current path.
dest_path/	Specifies the destination path for the resulting file copy. If no destination path is specified, the file copy will be placed in the current path.
orig_filename	The name of the existing file to be copied.
dupl_filename	The new user-defined file name for the resulting file copy. If you are copying a file to the same directory as the original, the file name for the copy must be different from the original. Up to thirty-two (32) characters may be used.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- You should verify that your switch's /flash directory has enough available memory to hold the new files and directories that will result from using the **cp -r** command.
- A file may be copied to a new location; you are not required to copy a file to the same directory that contains the original.
- Be sure to separate path directories and file names with a slash (/). Refer to the examples below.
- Up to 255 characters may be used for a fully qualified path.
- A path can contain up to a maximum of seven (7) directories including /flash.
- As with files names, up to thirty-two (32) characters may be used for a directory name.
- File and directory names can include only the following character types: a-z, A-Z, 0-9, dashes (-), dots (.), and underscores (_).
- This command can also be used on the secondary CMM.

Examples

```
-> cp flash/snapshots/asc.1.snap flash/snapshot/snapshot_copy
-> cp flash/snapshots/asc.1.snap snapshot_copy
-> cp asc.1.snap flash/snapshot/snapshot_copy
-> cp asc.1.snap snapshot_copy
```

Release History

Release 5.1; command was introduced.

Related Commands

mv	Moves an existing file or directory to a new location.

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesArg2
   systemServicesAction
```

mv

Moves an existing file or directory to a new location.

mv {[*path/***]***filename dest_path***[***/new_filename***] | [***path/***]***dir dest_path***[***/new_dir***]}**

Syntax Definitions

path/	Specifies the path (i.e., location) containing the file or directory being moved. If no path name is specified, the command assumes the current path.
filename	Specifies the name of the existing file to be moved.
dest_path/	Specifies the destination path (i.e., new location) for the file or directory that is being moved.
new_filename	Specifies a new file name for the file being moved. If a new name is not specified, the existing name will be used.
dir	Specifies the name of the existing directory to be moved.
new_dir	Specifies a new directory name for the directory being moved. If a new name is not specified, the existing name will be used.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The **mv** command does not make a copy of the file or directory being moved. To copy a file or directory to the current path or to a new location, use the **cp** command on page 7-18.
- Be sure to separate path directories and file names with a slash (/). Refer to the examples below.
- Up to 255 characters may be used for a fully qualified path.
- A path can contain up to a maximum of seven (7) directories including /flash.
- As with files names, up to thirty-two (32) characters may be used for a directory name.
- File and directory names can include only the following character types: a-z, A-Z, 0-9, dashes (-), dots (.), and underscores (_).
- This command can also be used on the secondary CMM.

Examples

```
-> mv flash/asc.1.snap flash/backup_files/asc.1.snap
```

Release History

Release 5.1; command was introduced.

Related Commands

rename	Renames an existing file or directory.
cp	Copies an existing file or directory.

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesArg2
   systemServicesAction
```

move

Moves an existing file or directory to a new location.

move {[*path/***]***filename dest_path***[***/new_filename***] | [***path/***]***dir dest_path***[***/new_dir***]}**

Syntax Definitions

path/	Specifies the path (i.e., location) containing the file or directory being moved. If no path name is specified, the command assumes the current path.
filename	Specifies the name of the existing file to be moved.
dest_path/	Specifies the destination path (i.e., new location) for the file or directory that is being moved.
new_filename	Specifies a new file name for the file being moved. If a new name is not specified, the existing name will be used.
dir	Specifies the name of the existing directory to be moved.
new_dir	Specifies a new directory name for the directory being moved. If a new name is not specified, the existing name will be used.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The **move** command does not make a copy of the file or directory being moved. To copy a file or directory to the current path or to a new location, use the **cp** command.
- Be sure to separate path directories and file names with a slash (/). Refer to the examples below.
- Up to 255 characters may be used for a fully qualified path.
- A path can contain up to a maximum of seven (7) directories including /flash.
- As with files names, up to thirty-two (32) characters may be used for a directory name.
- File and directory names can include only the following character types: a-z, A-Z, 0-9, dashes (-), dots (.), and underscores (_).
- This command can also be used on the secondary CMM.

Examples

```
-> move flash/asc.1.snap flash/backup_files/asc.1.snap
```

Release History

Release 5.1; command was introduced.

Related Commands

rename	Renames an existing file or directory.
cp	Copies an existing file or directory.

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesArg2
   systemServicesAction
```

chmod

Changes the write privileges for a specified file.

chmod { +w | -w } [*path/***]***file***

Syntax Definitions

+w	Enables read-write privileges for the file.
-w	Disables write privileges for the file—i.e., the file becomes read-only.
path/	The path containing the file for which privileges are being changed. Be sure to separate path directories and file names with a slash (/). Up to 255 characters may be used for the specified path. Also, a path may contain a maximum of thirty-two (32) directories.
file	The name of the file for which read-write privileges are being changed.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This command can also be used on the secondary CMM.

Examples

```
-> chmod +w vlan.config
-> chmod -w flash/backup_configs/vlan.config
```

Release History

Release 5.1; command was introduced.

Related Commands

attrib	Changes the write privileges for a specified file.

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesAction
```

attrib

Changes the write privileges for a specified file.

attrib { +w | -w } [*path/***]***file***

Syntax Definitions

+w	Enables read-write privileges for the file.
-w	Disables write privileges for the file—i.e., the file becomes read-only.
path/	The path containing the file for which write privileges are being changed. Be sure to separate path directories and file names with a slash (/). Up to 255 characters may be used for the specified path. Also, a path may contain a maximum of thirty-two (32) directories.
file	The name of the file for which write privileges are being changed.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This command can also be used on the secondary CMM.

Examples

```
-> attrib +w vlan.config
-> attrib -w flash/backup_configs/vlan.config
```

Release History

Release 5.1; command was introduced.

Related Commands

chmod	Changes the write privileges for a specified file.

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesAction
```

freespace

Displays the amount of free space available in the /flash directory.

freespace [*/flash***]**

Syntax Definitions

/flash	Optional syntax. The amount of free space is shown for the /flash directory.

Defaults

N/A

Usage Guidelines

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Examples

```
-> freespace /flash
/flash 3143680 bytes free

-> freespace
/flash 3143680 bytes free
```

Release History

Release 5.1; command was introduced.

Related Commands

fsck	Performs a file system check.

MIB Objects

```
SystemFileSystemTable
   systemFileSystemFreespace
```

fsck

Performs a file system check, including diagnostic information in the event of file corruption. If the **fsck** command detects a problem with the /flash file system, a message is displayed indicating the problem, along with any steps needed to resolve it.

fsck */flash*

Syntax Definitions

/flash	Indicates that the file system check will be performed on the /flash directory.

Defaults

This command gives you the option of having the errors repaired automatically. The default is to *not* repair errors.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- When you execute this command, a message appears asking if you want the file system check command to automatically repair any errors found. If you accept the default by pressing Enter, errors found will be displayed but they will *not* be repaired automatically.
- If you elect to have the file system check command repair any errors found, enter **y** for yes. The switch will display the errors found and specify those errors that have been repaired.
- This command can also be used on the secondary CMM.

Examples

```
-> fsck /flash
Do you want fsck to automatically repair any errors found? (<CR> = No)
/flash/  - disk check in progress ...
/flash/  - Volume is OK

          total # of clusters:  14,773
           # of free clusters:  4,132
            # of bad clusters:  0
              total free space:  8,264 Kb
    max contiguous free space:  5,163,008 bytes
                   # of files:  46
                 # of folders:  3
          total bytes in files:  21,229 Kb
              # of lost chains:  0
   total bytes in lost chains:  0

(Example Continued on Next Page)
```

```
-> fsck /flash
/flash/  - disk check in progress ...air any errors found? (<CR> = No) y
/flash/  - Volume is OK

          total # of clusters:  14,773
           # of free clusters:  4,132
            # of bad clusters:  0
             total free space:  8,264 Kb
    max contiguous free space:  5,163,008 bytes
                   # of files:  46
                 # of folders:  3
          total bytes in files:  21,229 Kb
              # of lost chains:  0
   total bytes in lost chains:  0
```

Release History

Release 5.1; command was introduced.

Related Commands

freespace	Displays the amount of free space remaining in the /flash directory.

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesAction
```

newfs

Deletes a complete flash file system and all files within it, replacing it with a new, empty flash file system. Use this command when you want to reload all files in the file system or in the unlikely event that the flash file system becomes corrupted.

newfs */flash*

Syntax Definitions

/flash	Required syntax. This indicates that the complete flash file system will be replaced.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- It is recommended that you preserve all required image and configuration files by saving them to a remote host before executing the **newfs** command.
- Do not power-down the switch after running the **newfs** command until you reload all required image and configuration files.
- This command can also be used on the secondary CMM.

Examples

```
-> newfs /flash
```

Release History

Release 5.1; command was introduced.

Related Commands

N/A

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesAction
```

rcp

Copies a file from a secondary CMM to a primary CMM or from a non primary switch to a primary switch in a stack.

rcp *slot source_filepath destination_file*

Syntax Definitions

slot	The slot number of the non primary switch in a stack. This parameter is only variable on OmniSwitch 6600 Family switches and is not available on OmniSwitch 7700/7800/8800 switches.
source_filepath	The name and path of the source file.
destination_file	The name of the destination file.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- On OmniSwitch 7700/7800/8800 switches this command copies any file from the secondary CMM to the primary CMM.
- On OmniSwitch 6600 Family switches this command copies any file from any non primary switch to the primary switch in a stack. You must specify the slot number on these switches.

Examples

On OmniSwitch 7700, 7800, and 8800 switches:

```
-> rcp /flash/boot.params boot.params
```

On OmniSwitch 6600 Family switches:

```
-> rcp 5 /flash/boot.params boot.params
```

Release History

Release 5.1; command was introduced.

Related Commands

rrm	Removes a file from a from a secondary CMM or from a non primary switch in a stack.
rls	Displays the content of a non primary CMM in a switch or a non primary switch in a stack.

MIB Objects

```
chasSupervisionRfsLsTable
   alcatelIND1ChassisSupervisionRfsCommands
   chasSupervisionRfsCommandsSlot
   chasSupervisionRfsCommandsCommand
   chasSupervisionRfsCommandsSrcFileName
   chasSupervisionRfsCommandsDestFileName
```

rrm

Removes a file from a from a secondary CMM or from a non primary switch in a stack.

rrm *slot filepath*

Syntax Definitions

slot	The slot number of the non primary switch in a stack. This parameter is only variable on OmniSwitch 6600 Family switches and is not available on OmniSwitch 7700/7800/8800 switches.
filepath	The name and path of the file to be deleted.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- On OmniSwitch 7700/7800/8800 switches this command deletes any file from the secondary CMM.
- On OmniSwitch 6600 Family switches this command deletes any file from any non primary switch. You must specify the slot number on these switches.

Examples

On OmniSwitch 7700, 7800, and 8800 switches:

```
-> rrm /flash/boot.params
```

On OmniSwitch 6600 Family switches:

```
-> rrm 5 /flash/boot.params
```

Release History

Release 5.1; command was introduced.

Related Commands

rcp	Copies a file from a secondary CMM to a primary CMM or from a non primary switch to a primary switch in a stack.
rls	Displays the content of a non primary CMM in a switch or a non primary switch in a stack.

MIB Objects

```
chasSupervisionRfsLsTable
   alcatelIND1ChassisSupervisionRfsCommands
   chasSupervisionRfsCommandsSlot
   chasSupervisionRfsCommandsCommand
   chasSupervisionRfsCommandsSrcFileName
```

rls

Displays the content of a non primary CMM in a switch or a non primary switch in a stack.

rls *slot directory* **[***file_name***]**

Syntax Definitions

slot	The slot number of the non primary switch in a stack. This parameter is only valid on OmniSwitch 6600 Family switches and is not available on OmniSwitch 7700/7800/8800 switches.
directory	The name of the directory on the non primary CMM or switch.
destination_file	The file to be displayed on the non primary CMM or switch.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- On OmniSwitch 7700/7800/8800 switches this command displays directory content on the secondary CMM.
- On OmniSwitch 6600 Family switches this command displays directory content on any non primary switch in a stack. You must specify the slot number on these switches.

Examples

On OmniSwitch 7700, 7800, and 8800 switches:

```
-> rls /flash
-rw          324  Mar  3 11:32   boot.params
drw         2048  Mar  3 11:32   certified/
drw         2048  Mar  3 11:32   working/
-rw        64000  Mar  7 09:54   swlog1.log
-rw        64000  Mar  4 12:51   swlog2.log
-rw           29  Feb  5  2023   policy.cfg
-rw      3369019  Mar  3 11:20   cs_system.pmd
-rw       394632  Jan  1  1980   bootrom.bin
-rw       511096  Jan  1  1980   miniboot.backup
-rw       511096  Jan  1  1980   miniboot.default
drw         2048  Feb 25 06:34   network/
-rw          266  Feb 24 13:21   boot.cfg.1.err
drw         2048  Mar  3 11:29   switch/
-rw          256  Mar  3 11:29   random-seed
```

On OmniSwitch 6600 Family switches:

```
-> rls 5 /flash
-rw          324  Mar  3 11:32   boot.params
drw         2048  Mar  3 11:32   certified/
drw         2048  Mar  3 11:32   working/
-rw        64000  Mar  7 09:54   swlog1.log
-rw           29  Feb  5  2023   policy.cfg
-rw      3369019  Mar  3 11:20   cs_system.pmd
-rw       394632  Jan  1  1980   bootrom.bin
-rw       511096  Jan  1  1980   miniboot.backup
-rw       511096  Jan  1  1980   miniboot.default
drw         2048  Feb 25 06:34   network/
drw         2048  Mar  3 11:29   switch/
-rw          256  Mar  3 11:29   random-seed
```

Release History

Release 5.1; command was introduced.

Related Commands

rcp	Copies a file from a secondary CMM to a primary CMM or from a non primary switch to a primary switch in a stack.
rrm	Removes a file from a from a secondary CMM or from a non primary switch in a stack.

MIB Objects

```
chasSupervisionRfsLsTable
   chasSupervisionRfsLsFileIndex
   chasSupervisionRfsLsSlot
   chasSupervisionRfsLsDirName
   chasSupervisionRfsLsFileName
   chasSupervisionRfsLsFileType
   chasSupervisionRfsLsFileSize
   chasSupervisionRfsLsFileAttr
   chasSupervisionRfsLsFileDateTime
```

rdf

Displays the amount of free space on a non primary CMM in a switch or a non primary switch in a stack.

rdf {*slot***}**

Syntax Definitions

slot	The slot number of the non primary switch in a stack.

Defaults

N/A

Platforms Supported

OmniSwitch 6600

Usage Guidelines

On OmniSwitch 6600 Family switches this command displays the amount of free space on any non primary switch in a stack. If you specify the slot number then all switches in a stack will be displayed.

Examples

On OmniSwitch 6600 Family switches:

```
-> rdf
Slot  Filesystem     Size          Used         Available    Use
----+-----------+-------------+-------------+-------------+--------+
* 1    /flash       29949952      24134656       5815296      81
  2    /flash       29949952      24135168       5814784      81
  3    /flash       29949952      28024320       1925632      94
-> rdf 3
Slot  Filesystem     Size          Used         Available    Use
----+-----------+-------------+-------------+-------------+--------+
  3    /flash       29949952      28024320       1925632      94
```

output definitions

Slot	The slot number of the CMM (OmniSwitch 7700, 7800, and 8800 switches) or switch in a stack (OmniSwitch 6600 Family switches). On OmniSwitch 6600 Family switches only an asterisk (*****) indicates that the switch is the primary unit in the stack.
Filesystem	The name of the flash directory.
Size	The total amount of memory (in bytes) of flash memory.
Used	The amount of flash memory used (in bytes).
Available	The amount of available flash memory (in bytes).
Use	The percentage of flash memory in use.

Release History

Release 5.1.6; command was introduced.

Related Commands

rls	Displays the content of a non primary CMM in a switch or a non primary switch in a stack.
rrm	Removes a file from a from a secondary CMM or from a non primary switch in a stack.

MIB Objects

```
chasSupervisionRfsDfTable
   chasSupervisionRfsDfSlot
   chasSupervisionRfsDfFlashFree
   chasSupervisionRfsDfFlashSize
```

vi

Launches the switch's UNIX-like Vi text editor. The Vi file editor allows you to view or edit the contents of a specified text file.

vi [*path/***]***filename*

Syntax Definitions

path	The path (i.e., location) containing the file being viewed or edited. If no path is specified, the command assumes the current directory.
filename	The name of the existing file being viewed or edited. Up to thirty-two (32) characters may be used (e.g., **test_config_file**).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Until you exit the switch's file editor, all keystrokes will be passed to the text editor rather than the switch's command line.
- This command can also be used on the secondary CMM.

Examples

```
-> vi test_config_file
```

Release History

Release 5.1; command was introduced.

Related Commands

vi	Launches the switch's file editor.
view	Allows you to view the contents of a specified file by invoking the Vi text editor in read-only mode.

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesAction
```

view

Allows you to view the contents of a specified file by invoking the vi text editor in read-only mode.

view [*path/***]***filename*

Syntax Definitions

path	The path directory leading to the file being viewed. If no path is specified, the command assumes the current directory.
filename	The name of the existing file being viewed. Up to thirty-two (32) characters may be used (e.g., **test_config_file**).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This command can also be used on the secondary CMM.

Examples

```
-> view flash/text_file.txt
```

Release History

Release 5.1; command was introduced.

Related Commands

vi	Launches the switch's Vi text editor.

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesAction
```

tty

Specifies the number of lines and columns to be displayed on the terminal screen while the switch is in the edit file mode.

tty *lines columns*

Syntax Definitions

lines	The number of lines to be displayed on the terminal emulation screen for the current session. Values may range from 10 to 150.
columns	The number of columns to be displayed for each line. One column is the same width as a single text character. Values may range from 20 to 150.

Defaults

parameter	default
lines	24
columns	80

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The number of lines and columns set with this command control the screen size when the switch is editing or viewing a text file with the **vi** or **more** commands.
- The values set with this command do not control the CLI screen when the switch is operating in normal mode.
- This command can also be used on the secondary CMM.

Examples

```
-> tty 10 60
```

Release History

Release 5.1; command was introduced.

Related Commands

show tty	Displays current TTY settings.
more	Displays a switch text file onto the console screen.

MIB Objects

```
systemServices
   systemServicesTtyLines
   systemServicesTtyColumns
```

show tty

Displays current TTY settings.

show tty

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Shows the settings made with the **tty** command.
- This command can also be used on the secondary CMM.

Examples

```
-> show tty
lines = 24, columns = 80
```

Release History

Release 5.1; command was introduced.

Related Commands

tty	Specifies the number of TTY lines and columns to be displayed.

MIB Objects

```
systemServices
   systemServicesTtyLines
   systemServicesTtyColumns
```

more

Displays a switch text file onto the console screen.

more [*path/***]***file*

Syntax Definitions

path	The directory path leading to the file to be displayed. If no path is specified, the command assumes the current path.
file	The name of the text file to be displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command displays the specified text file within the line and column parameters set with the **tty** command.
- If the specified text file contains more columns than set with the **tty** command, the text will wrap to the next line displayed.
- If the text file contains more lines than set with the **tty** command, the switch will display only the number of lines specified. To display more lines, press the spacebar to show another full screen, press Enter to show the next line, or press q to quit the display and return to the system prompt.
- This command can also be used on the secondary CMM.

Examples

```
-> more config_file1
-> more flash/config_file1
-> more flash/working/config_file1
```

Release History

Release 5.1; command was introduced.

Related Commands

tty	Specifies the number of TTY lines and columns to be displayed.

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesAction
```

ftp

Starts an FTP session.

ftp {*host_name* **|** *ip_address***}**

Syntax Definitions

host_name	Specifies the host name for the FTP session.
ip_address	Specifies the IP address for the FTP session.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- You must have a valid username and a password for the specified host.
- After logging in, FTP commands are supported. They are defined in the following table.

ascii	Set transfer type to ASCII (7-bit).
binary	Set transfer type to binary (8-bit).
bye	Close session gracefully.
cd	Change to a new directory on the remote machine.
delete	Delete a file on the remote machine.
dir	Obtain a long listing on the remote machine.
get	Retrieve a file from the remote machine.
hash	Print the hash symbol (#) for every block of data transferred. (This command toggles hash enabling and disabling.)
ls	Display summary listing of the current directory on the remote host.
put	Send a file to the remote machine.
pwd	Display the current working directory on the remote host.
quit	Close session gracefully.
remotehelp	List the commands that the remote FTP server supports.
user	Send new user information.
lpwd	Display the current working directory on the local host.
?	Display list of available FTP commands.

Examples

```
-> ftp 172.17.6.228
Connecting to 172.17.6.228 [172.17.6.228]...connected.
220 Annex FTP server (Version RA4000 R14.1.15) ready.
Name :
```

Release History

Release 5.1; command was introduced.

Related Commands

sftp	Starts an SFTP session.

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesAction
```

sftp

Starts an SFTP session. An SFTP session provides a secure file transfer method.

Syntax Definitions

host_name	Specifies the host name for the SFTP session.
ip_address	Specifies the IP address for the SFTP session.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- You must have a valid username and a password for the specified host.
- After logging in, SFTP commands are supported. They are defined in the following table.

cd path	Change remote path to ‘path’.
lcd path	Change local directory to ‘path’.
chmod mode path	Change permissions of file ‘path’ to ‘mode’.
help	Display command help information.
get remote-path [local path]	Download a file from the remote path to the local path.
lls [path]	Display local directory listing.
ln oldpath newpath	Creates a symbolic link (symlink) to the remote file.
symlink oldpath newpath	Creates a symbolic link (symlink) to the remote file.
lmkdir path	Create local directory.
lpwd	Print local working directory.
ls [path]	Display remote directory listing.
mkdir path	Create remote directory.
put local-path [remote-path]	Upload file.
pwd	Display remote working directory.
exit	Quit the sftp mode.
quit	Exit the sftp mode.
rename oldpath newpath	Rename a remote file.
rmdir path	Remove remote directory.
rm path	Delete remote file.
version	Show the current SFTP version.
?	Synonym for help. Displays command help information.

Examples

```
-> sftp 12.251.11.122
login as:
```

Release History

Release 5.1; command was introduced.

Related Commands

ftp	Starts an FTP session.
ssh	Invokes a Secure Shell session. A Secure Shell session is used to make a secured connection to a remote system or device.

MIB Objects

```
SystemServices
   systemServicesArg1
   systemServicesAction
```

rz

Starts a Zmodem session.

rz

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- To use Zmodem, you must have a terminal emulator that supports the Zmodem protocol.
- Activate the Zmodem transfer according to the instructions that came with your terminal emulation software.
- When the transfer is complete, you can use the **ls** command to verify that the files were loaded successfully.
- To abort a Zmodem session, enter **CTRL** + **X** five times in succession. Refer to your switch's User Manual for more information on uploading files via Zmodem.
- This command can also be used on the secondary CMM.

Examples

```
-> rz
Upload directory: /flash
rz ready to receive file, please start upload (or send 5 CTRL-X's to abort).
```

Release History

Release 5.1; command was introduced.

Related Commands

install	Installs an image file from the switch's working directory.

MIB Objects

```
systemServices
   systemServicesAction
```

install

Installs an image file from the switch's working directory. (Software transferred to the switch must go through an installation process before it can be used by the switch's loader function.)

install *file* **[***argument***]**

Syntax Definitions

file	The name of the image file to be installed. Before a file can be installed, it must be present in the switch's working directory.
argument	Optional arguments specific to the package. For details on an optional argument, refer to the installation notes for the associated package.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> install Feni.img
```

Release History

Release 5.1; command was introduced.

Related Commands

ftp	Starts an FTP session.
rz	Starts a Zmodem session.

MIB Objects

```
SystemServices
   systemServicesArg1
   systemServicesArg2
   systemServicesArg3
   systemServicesArg4
   systemServicesArg5
   systemServicesArg6
   systemServicesArg7
   systemServicesArg8
   systemServicesArg9
   systemServicesAction
```

8 Web Management Commands

The switch can be configured and monitored using WebView, which is a web-based device management tool. Web Management CLI commands allow you to enable/disable web-based management and configure certain WebView parameters, such as Secure Socket Layer (SSL).

MIB information for the Web Management commands is as follows:

Filename: AlcatelInd1WebMgt.mib
Module: alcatelIND1WebMgtMIB

A summary of the available commands is listed here:

http server
http ssl
debug http sessiondb
show http

http server

Enables/disables web management on the switch. When enabled, a user is able to configure the switch using the WebView application.

{[ip] http | https} server

no {[ip] http | https} server

Syntax Definitions

ip	Optional syntax. Using this optional syntax is the same as using the **http server** command.

Defaults

Web management is enabled by default.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **no** form of the command to disable web management. If web management is disabled, you will not be able to access the switch using WebView.

Examples

```
-> http server
-> no http server
-> https server
-> no https server
```

Release History

Release 5.1; command was introduced.
Release 5.3.1; **https** keyword was added.

Related Commands

http ssl	Enables/disables SSL on the switch.
debug http sessiondb	Displays web management session information.
show http	Displays web management configuration information.

MIB Objects

```
alaIND1WebMgtConfigMIBGroup
   alaInd1WebMgtAdminStatus
```

http ssl

Enables/disables Force SSL on the switch. SSL is a protocol that establishes and maintains secure communication between SSL-enabled servers and clients across the Internet.

{[ip] http | https} ssl

no {[ip] http | https} ssl

Syntax Definitions

ip	Optional syntax. Using this optional syntax is the same as using the **http ssl** command.

Defaults

SSL is enabled by default.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **no** form of the command to disable SSL.

Examples

```
-> http ssl
-> no http ssl
-> https ssl
-> no https ssl
```

Release History

Release 5.1; command was introduced.
Release 5.3.1; **https** keyword was added.

Related Commands

http server	Enables/disables web management on the switch.
show http	Displays web management configuration information.

MIB Objects

```
alaIND1WebMgtConfigMIBGroup
   alaInd1WebMgtSsl
```

debug http sessiondb

Displays web management session information.

debug http sessiondb

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> debug http sessiondb

Sess    SessName   Name  TimeOut     Status             URL Name--&--StatMsg
-----+-----------+------+-------+--------------+---------------------------------
0  6  sess_21606  admin  5848035  AUTHENTICATED  /web/content/index.html
1 -2  sess_28257         5999940  IN_PROGRESS    /ip/content/index.html
Current Active WebView Session: 1
```

output definitions

Sess	The first number is the session number.
SessName	Unique ID assigned by the browser.
Name	User name.
TimeOut	User-configured inactivity timer, in minutes.
Status	Session status. If the user has successfully logged in, the status is “Authenticated.”
URL Name&StatMsg	Current page being viewed by the user.

Release History

Release 5.1; command was introduced.

Related Commands

http server	Enables/disables web management on the switch.
http ssl	Enables/disables SSL on the switch.
show http	Displays web management configuration information.

MIB Objects

N/A

show http

Displays web management configuration information.

show [ip] http

Syntax Definitions

ip	Optional syntax. Using this optional syntax is the same as using the **show http** command.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show http

Web Management = on
Force SSL = on
Web Management Http Port = 80
Web Management Https Port = 443
```

output definitions

Web Management	Indicates whether web management is enabled (on) or disabled (off) on the switch.
Force SSL	Indicates whether Force SSL is enabled (on) or disabled (off) on the switch. If this is set to **on** this means that SSL is forced on an HTTP session and hence HTTPS protocol is negotiated between the client and server. For example, an “http://switchname.com” URL will be redirected to an “https://switchname.com” URL.
Web Management Http Port	The port configured for the HTTP connection.
Web Management Https Port	The port configured for a secure HTTP connection (SSL enabled).

Release History

Release 5.1; command was introduced.

Related Commands

http server	Enables/disables web management on the switch.
http ssl	Enables/disables SSL on the switch.

MIB Objects

```
alaIND1WebMgtConfigMIBGroup
   alaInd1WebMgtAdminStatus
   alaInd1WebMgtSsl
   alaInd1WebMgtHttpPort
   alaInd1WebMgtHttpsPort
```

9 Configuration File Manager Commands

The Configuration Manager feature allows you to configure your switch using an ASCII-based text file. CLI commands may be typed into a text document—referred to as a *configuration file*—and then uploaded and applied to the switch.

MIB information for the Configuration Manager commands is as follows:

Filename: AlcatelIND1System.mib
Module: Alcatel-IND1ConfigMgr.mib

A summary of the available commands is listed here:

configuration apply
configuration error-file limit
show configuration status
configuration cancel
configuration syntax check
configuration snapshot
show configuration snapshot
write terminal

configuration apply

Applies a configuration file to the switch. Files may be applied immediately or after a designated timer session. With the timer session option, files are applied either at a scheduled date and time or after a specified period of time (i.e., a countdown) has passed.

configuration apply *filename* **[at** *hh:mm month dd* **[***year***]] | [in** *hh***[***:mm***]] [verbose]**

Syntax Definitions

filename	The name of the configuration text file to be applied to the switch (e.g., **newfile1**).
at *hh:mm* **{***dd month* | *month dd***} [***year***]**	Designates a timer session in which a configuration file is applied at a specified date and time in the future. Values for *hh* range from 00 through 23. Values for *mm* range from 00 through 59. Values for *dd* range from 01 through 31. Values for month range from january through december. The switch assumes either the current year or the next calendar year for month and day pairs that precede the current date.
in *hh***[***:mm***]**	Designates a timer session in which the configuration file is applied after a specific amount of time (i.e., a countdown) has passed. Values for *hh* range from 00 through 23. Values for *mm* range from 00 through 59.
verbose	When verbose is entered, information is displayed on your workstation's console as each command in the configuration file is applied.

Defaults

By default, **verbose** error checking is not performed.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The **configuration apply** command only applies settings to the running configuration. The **boot.cfg** file does not get overwritten.
- It is recommended that you check all configuration files for syntax errors before applying them to your switch.
- To schedule a timer session in which a file is applied at a specific date and time, enter **at** followed by the hour, minute, month, day and year. The switch assumes either the current calendar year or the next calendar year for dates beginning January 1.
- To schedule a timer session in which a file is applied after a specific amount of time (i.e., a countdown) has passed, enter **in** followed by the number of hours and minutes.
- Verbose mode is not supported for timer sessions.

- The keyword, **authkey**, along with a related alpha-numeric text string, are automatically included in many snapshot files (e.g., **configuration snapshot all**). The text string following the **authkey** keyword represents a login password that has been encrypted *twice*. (The first encryption occurs when a password is first created by a user; the second encryption occurs when a configuration snapshot is taken.) This dual encryption further enhances switch security. However, it is important to note that any configuration file (including a generated snapshot) that includes this dual-encrypted password information will result in an error whenever it is applied to the switch via the **configuration apply** command. This is a valid switch function and does not represent a significant problem. If an **authkey**-related error is the *only* error detected, simply remove all **authkey**-related syntax using a text editor. If a new password is required for the switch, include valid password syntax in the configuration file or immediately issue a new password using the **password** command at the command prompt. For more information on passwords, refer to page 43-40.

Examples

```
-> configuration apply new_configuration at 12:00 15 november
-> configuration apply new_configuration at 12:00 november 15
-> configuration apply newfile1 in 01:30
-> configuration apply my_switch_config in 00:05
-> configuration apply asc.1.snap in 23:00
-> configuration apply aaa_config in 12
-> configuration apply vlan_config verbose
-> configuration apply vlan_config
...
```

Note. When the **configuration apply** command is entered *without* **at** or **in** syntax information, one or more dots "**.**" is displayed in the next line, immediately following the command line. This indicates command progress; each dot represents 256 text lines in the configuration file processed by the configuration apply mechanism.

Release History

Release 5.1; command was introduced.

Related Commands

configuration syntax check	Performs a syntax and authorization check of all CLI commands contained in a configuration file.

MIB Objects

```
alcatelIND1ConfigMgrMIBObjects
   configFileName
   configFileMode
   configFileAction
   configTimerFileName
   configTimerFileTime
```

configuration error-file limit

Specifies the maximum number of configuration error files allowed in the switch's **/flash** directory. Error files are normally generated when a configuration file is applied to the switch. Error files are identified by their **.err** extension.When the maximum number of **.err** files is exceeded, any new error file will over-write the **.err** file with the oldest timestamp.

configuration error-file limit *number*

Syntax Definitions

number	Indicate the number of error files allowed in the **/flash** directory. The valid range is from 1 to 25 files.

Defaults

parameter	default
number	1

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- When the error file limit is set to 1 (the default value), the next error file generated by the switch will replace the existing one.
- When the error file limit is set to a value greater than 1, when a new error file that exceeds the maximum limit is created, the switch will automatically remove the error file with the smallest timestamp.
- The error files generated by the switch have the **.err** extension.
- If you want to save an error file, you may change the file name so that it does not have the .err extension or you can move it from the /flash directory.

Examples

```
-> configuration error-file limit 2
-> configuration error-file limit 1
```

Release History

Release 5.1; command was introduced.

Related Commands

configuration apply	Applies a configuration file to the switch. Also used for scheduling a timer session for a configuration file.
configuration cancel	Cancels a pending timer session for a configuration file.

MIB Objects

```
alcatelIND1ConfigMgrMIBObjects
   configErrorFileMaximum
```

show configuration status

Displays whether there is a pending timer session scheduled for a configuration file and indicates whether the running configuration and the saved configuration files are *identical* or *different*. This command also displays the number of error files that will be held in the flash directory.

show configuration status

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- A timer session can be scheduled using the **configuration apply** command. For more information, refer to page 9-2.
- The screen output **File configuration** *</path/filename>***: scheduled at** *dd/mm hh:mm* indicates that a timer session has been scheduled for a later time.
- The output **No file configuration has been scheduled** indicates an idle timer session (i.e., no timer session has been scheduled for a configuration file).
- The output **File configuration is in progress** indicates that a file is currently being applied to the switch.
- The output **File configuration** *</path/filename>***: completed with 2 errors** indicates that the named file was applied to the switch with two recorded errors.
- When the running and saved configurations are the same, the output **Running configuration and saved configuration are identical** will be displayed.
- When the running and saved configurations are the different, the output **Running configuration and saved configuration are different** will be displayed.
- To synchronize the running and saved configuration, use the **write memory** command.

Examples

```
-> show configuration status
```

Release History

Release 5.1; command was introduced.

Release History

configuration apply	Applies a configuration file to the switch. Also used for scheduling a timer session for a configuration file.
configuration cancel	Cancels a pending timer session for a configuration file.
configuration error-file limit	Specifies the maximum number of configuration error files allowed in the switch's **/flash** directory.
write memory	Copies the running configuration (RAM) to the working directory.

MIB Objects

```
configTimerFileGroup
   configTimerFileStatus
```

configuration cancel

Cancels a pending timer session for a configuration file.

configuration cancel

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> configuration cancel
```

Release History

Release 5.1; command was introduced.

Related Commands

configuration apply	Applies a configuration file to the switch. Also used for scheduling a timer session for a configuration file.
show configuration status	Displays whether there is a pending timer session scheduled for a configuration file.

MIB Objects

```
configTimerFileGroup
   configTimerClear
```

configuration syntax check

Performs a syntax and authorization check of all CLI commands contained in a configuration file.

configuration syntax check *path/filename* **[verbose]**

Syntax Definitions

path/filename	The configuration file being checked for syntax and authorization errors. If a configuration file is located in another directory, be sure to specify the full path. For example, **/flash/working/asc.1.snap**.
verbose	When **verbose** is specified in the command line, all syntax contained in the configuration file is printed to the console, even if no error is detected. When **verbose** is *not* specified in the command line, cursory information (number of errors and error log file name) will be printed to the console *only if a syntax or configuration error is detected.*

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- When an error is detected, an error file (**.err**) is automatically generated by the switch. By default, this file is placed in the root **/flash** directory. To view the contents of a generated error file, use the **view** command. For example, **view asc.1.snap.1.err**.
- The syntax, **mac alloc**, is automatically included in many snapshot files (e.g., **configuration snapshot all**). All **mac alloc**-related syntax is valid *during switch boot up only* (i.e., it cannot be applied while the switch is in run-time operation). Because snapshot files are commonly used as configuration files, syntax checks may detect **mac alloc** syntax and issue an error (along with a generated **.err** file). This is a valid switch function and does not represent a significant problem. If a **mac alloc**-related error is the *only* error detected, simply remove the syntax using a text editor, then re-check the file using the **configuration syntax check** command.
- It is recommended that you check all configuration files for syntax errors before applying them to your switch.

Examples

```
-> configuration syntax check vlan_file1
..
```

Note. When the **configuration syntax check** command is entered, one or more dots "**.**" is displayed in the command output. This indicates command progress; each dot represents 256 text lines in the configuration file processed by the syntax check mechanism.

Release History

Release 5.1; command was introduced.

Related Commands

configuration apply	Applies a configuration file to the switch. Also used for scheduling a timer session for a configuration file.
show configuration status	Displays whether there is a pending timer session scheduled for a configuration file.

MIB Objects

```
configFileGroup
   configErrorFileName
   configErrorFileMaximum
   configFileMode
   configFileStatus
```

configuration snapshot

Generates a snapshot file of the switch's non-default current running configuration. A snapshot can be generated for all current network features or for one or more specific network features. A snapshot is a single text file that can be viewed, edited, and reused as a configuration file.

configuration snapshot *feature_list* **[***path/filename***]**

Syntax Definitions

feature_list	The description for the network feature(s) to be included in the snapshot. You may enter more than one network feature in the command line. Current snapshot-supported network features are listed below.

snapshot-supported features		
802.1q	**ip-routing**	**rdp**
aaa	**ipmr**	**rip**
aip	**ipms**	**ripng**
all	**ipx**	**session**
bgp	**ipv6**	**slb**
bridge	**linkagg**	**snmp**
chassis	**module**	**stp**
health	**ospf**	**system**
interface	**pmm**	**vlan**
ip	**policy**	**vrrp**
ip-helper	**qos**	**webmgt**

path/filename	A user-defined name for the resulting snapshot file. For example, **test_snmp_snap**. You may also enter a specific path for the resulting file. For example, the syntax **/flash/working/test_snmp_snap** places the **test_snmp_snap** file in the switch's **/flash/working** directory.

Defaults

If a file name is not specified, the default file name **asc.#.snap** is used. Here, # indicates the order in which the default file is generated. For example, the first default file name to be generated is **asc.1.snap**, the second default file name to be generated is named **asc.2.snap**, etc. By default, all snapshot files are placed in the root **/flash** directory.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Only current, non-default configuration settings are written to the snapshot file.
- You may enter more than one network feature in the command line. Separate each network feature with a space and no comma. Network features may be entered in any order.
- The snapshot file is automatically placed in the root **/flash** directory unless otherwise specified.

Examples

```
-> configuration snapshot all
-> configuration snapshot new_file1 qos health aggregation
-> configuration snapshot snmp_snapshot snmp
-> configuration snapshot 802.1q
```

Release History

Release 5.1; command was introduced.

Related Commands

N/A

MIB Objects

```
configManager
   configSnapshotFileName
   configSnapshotAction
   configSnapshotAllSelect
   configSnapshotVlanSelect
   configSnapshotSpanningTreeSelect
   configSnapshotQOSSelect
   configSnapshotIPSelect
   configSnapshotIPXSelect
   configSnapshotIPMSSelect
   configSnapshotAAASelect
   configSnapshotSNMPSelect
   configSnapshot802.1QSelect
   configSnapshotLinkAggregateSelect
   configSnapshotPortMirrorSelect
   configSnapshotXIPSelect
   configSnapshotHealthMonitorSelect
   configSnapshotBootPSelect
   configSnapshotBridgeSelect
   configSnapshotChassisSelect
   configSnapshotInterfaceSelect
   configSnapshotPolicySelect
   configSnapshotSessionSelect
   configSnapshotServerLoadBalanceSelect
   configSnapshotSystemServiceSelect
   configSnapshotVRRPSelect
   configSnapshotWebSelect
   configSnapshotRIPSelect
   configSnapshotRIPngSelect
   configSnapshotOSPFSelect
   configSnapshotBGPSelect
   configSnapshotIPRMSelect
```

```
configSnapshotIPMRSelect
configSnapshotModuleSelect
configSnapshotRDPSelect
configSnapshotIPv6Select
```

show configuration snapshot

Displays the switch's current running configuration for all features or for the specified feature(s).

show configuration snapshot [*feature_list***]**

Syntax Definitions

feature_list	Specify the feature(s) for which you want to display the running configuration. List the features separated by a space with no comma.

Snapshot Keywords		
802.1q	**ip-routing**	**rdp**
aaa	**ipmr**	**rip**
aip	**ipms**	**ripng**
all	**ipx**	**session**
bgp	**ipv6**	**slb**
bridge	**linkagg**	**snmp**
chassis	**module**	**stp**
health	**ospf**	**system**
interface	**pmm**	**vlan**
ip	**policy**	**vrrp**
ip-helper	**qos**	**webmgt**

Defaults

By default, this command shows configuration information for *all* features.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use this command to view the current configuration for any feature shown in the table.
- To show a list of features on the switch, use the **show configuration snapshot ?** syntax.
- Configurations are listed below the name of each feature.
- Features with no current configuration show only the name of the feature.

Examples

```
-> show configuration snapshot
-> show configuration snapshot aaa bridge
! Bridging :

! AAA :
aaa authentication default "local"
aaa authentication console "local"
user "public" read All write All no auth authkey 391b0e74dbd13973d703cceaa4a8e30
```

Release History

Release 5.1; command was introduced.

Related Commands

write terminal	Displays the switch's current running configuration for all features.

MIB Objects

```
configManager
   configSnapshotFileName
   configSnapshotAction
   configSnapshotAllSelect
   configSnapshotVlanSelect
   configSnapshotSpanningTreeSelect
   configSnapshotQOSSelect
   configSnapshotIPSelect
   configSnapshotIPXSelect
   configSnapshotIPMSSelect
   configSnapshotAAASelect
   configSnapshotSNMPSelect
   configSnapshot802.1QSelect
   configSnapshotLinkAggregateSelect
   configSnapshotPortMirrorSelect
   configSnapshotXIPSelect
   configSnapshotHealthMonitorSelect
   configSnapshotBootPSelect
   configSnapshotBridgeSelect
   configSnapshotChassisSelect
   configSnapshotInterfaceSelect
   configSnapshotPolicySelect
   configSnapshotSessionSelect
   configSnapshotServerLoadBalanceSelect
   configSnapshotSystemServiceSelect
   configSnapshotVRRPSelect
   configSnapshotWebSelect
   configSnapshotRIPSelect
   configSnapshotRIPngSelect
   configSnapshotOSPFSelect
   configSnapshotBGPSelect
   configSnapshotIPRMSelect
   configSnapshotIPMRSelect
   configSnapshotModuleSelect
   configSnapshotRDPSelect
   configSnapshotIPv6Select
```

write terminal

Displays the switch's current running configuration for all features.

write terminal

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Configurations are listed below the name of each feature.
- Features with no current configuration show only the name of the feature.

Examples

```
-> write terminal
```

Release History

Release 5.1; command was introduced.

Related Commands

show configuration snapshot	Displays the switch's current running configuration for all features or for the specified feature(s).

MIB Objects

```
configManager
   mib_configSnapshotAllSelect
```

10 SNMP Commands

This chapter includes descriptions for Trap Manager and SNMP Agent commands. The commands are used for configuring SNMP settings on the switch.

- SNMP station commands can create, modify, or delete an SNMP station. Also included is a show command for monitoring current SNMP station status.
- SNMP traps commands configure SNMP trap settings. Traps can be replayed and filtered. Also, test traps can be generated to verify that individual traps are being correctly handled by the Network Management Station (NMS). The SNMP traps commands set includes a show commands for monitoring SNMP trap information.
- SNMP agent commands configure SNMP security levels on the switch. Also includes show commands for monitoring current SNMP security status.

MIB information for SNMP Community commands is a follows:

Filename: IETFsnmpCommunity.MIB
Module: IETF SNMP-COMMUNITY.MIB

MIB information for Trap Manager commands is a follows:

Filename AlcatelIND1TrapMgr.MIB
Module: ALCATEL-IND1-TRAP-MGR.MIB

MIB information for SNMP Agent commands is a follows:

Filename: AlcatelIND1SNMPAgent.MIB
Module: ALCATEL-IND1-SNMP-AGENT.MIB

A summary of the available commands is listed here:

SNMP station commands	**snmp station** **show snmp station**
SNMP community map commands	**snmp community map** **snmp community map mode** **show snmp community map**
SNMP security commands	**snmp security** **show snmp security** **show snmp statistics** **show snmp mib family**
SNMP trap commands	**snmp trap absorption** **snmp trap to webview** **snmp trap replay** **snmp trap filter** **snmp authentication trap** **show snmp trap replay** **show snmp trap filter** **snmp authentication trap** **show snmp trap config**

snmp station

Adds a new SNMP station; modifies or deletes an existing SNMP station.

snmp station *ip_address* **{[***udp_port***] [***username***] [v1 | v2 | v3] [enable | disable]}**

no snmp station *ip_address*

Syntax Definitions

ip_address	The IP address to which SNMP unicast traps will be sent.
udp_port	A UDP destination port.
username	The user name on the switch or external server used to send traps to the SNMP station(s). The username specified here must match an existing user account name.
v1	Specifies that traps are sent using SNMP version 1.
v2	Specifies that traps are sent using SNMP version 2.
v3	Specifies that traps are sent using SNMP version 3.
enable	Enables the specified SNMP station.
disable	Disables the specified SNMP station.

Defaults

parameter	default
udp_port	162
v1 | v2 | v3	v3
enable | disable	enable

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- When adding an SNMP station, you must specify an IP address *plus username parameters*. For example, the syntax **snmp station 1.2.3.4** is not a valid command entry; however, **snmp station 1.2.3.4 username1** is a valid command entry.
- When modifying an SNMP station, you must specify an IP address *plus at least one additional parameter*. For example, the syntax **snmp station 1.2.3.4** is not a valid command entry; however, **snmp station 1.2.3.4 v2** is a valid command entry.
- The default UDP port 162 is commonly used for traps; however, the destination port can be redefined to accommodate an SNMP station using a nonstandard port. The destination port specified in the command line must correspond with the UDP destination port configured at the receiving SNMP station(s).
- When the SNMP station is enabled, the switch transmits traps to the specified IP address.

Examples

```
-> snmp station 168.22.2.2 111 username2 v1 disable
-> snmp station 168.151.2.101 "test lab"
-> snmp station 170.1.2.3 username1 enable
-> snmp station 1.1.2.2 v2
-> no snmp station 2.2.2.2
```

Release History

Release 5.1; command was introduced.

Related Commands

show snmp station	Displays current SNMP station information.

MIB Objects

```
trapStationTable
   trapStationIP
   trapStationPort
   trapStationUser
   trapStationProtocol
   trapStationRowStatus
```

show snmp station

Displays the current SNMP station status.

show snmp station

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show snmp station
ipAddress/udpPort           status    protocol user
-------------------------------------------------------------------------------
199.199.100.200/8010        enable    v3       NMSuserV3MD5DES
199.199.101.201/111         disable   v2       NMSuserV3MD5
199.199.102.202/8002        enable    v1       NMSuserV3SHADES
199.199.103.203/8003        enable    v3       NMSuserV3SHADES
199.199.104.204/8004        enable    v3       NMSuserV3SHA
```

output definitions

IPAddress	IP Address of the SNMP management station that replayed the trap.
UDP Port	UDP port number.
Status	The Enabled/Disabled status of the SNMP management station.
Protocol	The version of SNMP set for this management station.
User	The user account name.

Release History

Release 5.1; command was introduced.

Related Commands

snmp station	Adds a new SNMP station; modifies or deletes an existing SNMP station.

snmp community map

Configures and enables a community string on the switch and maps it to an existing user account name.

snmp community map *community_string* **{[user** *useraccount_name***] | {enable | disable}}**

no snmp community map *community_string*

Syntax Definitions

community_string	Specify a community string in the form of a text string. This string must be between 1 and 32 characters.
useraccount_name	Specify a user name in the form of a text string. This name must match a user login account name already configured on the switch or configured remotely on an external AAA server. This user name must be between 1 and 32 characters.
enable	Enables SNMP community string mapping.
disable	Disables SNMP community string mapping.

Defaults

By default, SNMP community map authentication is enabled.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Community strings configured on the switch are used for v1 and v2c SNMP managers only.
- The user account name must be a current user account recognized by the switch. For a list of current user names use the **show user** command. To create a new user account, use the **user** command.
- There is one to one mapping between each community string and a user account name.
- Privileges attached to the community string are the ones inherited from the user account name that created it.

Examples

```
-> snmp community map community1 user testname1
-> snmp community map community1 enable
```

Release History

Release 5.1; command was introduced.

Related Commands

snmp community map mode Enables the local community strings database.

MIB Objects

```
SNMPCommunityTable
   snmpCommunityIndex
   snmpCommunitySecurityName
   snmpCommunityStatus
```

snmp community map mode

Enables the local community strings database.

snmp community map mode {enable | disable}

Syntax Definitions

enable	Enables SNMP community map database.
disable	Disables SNMP community map database.

Defaults

By default, SNMP community strings database is enabled.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- When enabled, the community string carried over each incoming v1 or v2c SNMP request must be mapped to a user account name in order to be processed by the SNMP agent.
- When enabled, mapping is contained in the local community strings database populated by using the **snmp community map** command.
- When disabled, the community strings carried over each incoming v1 or v2c request must be *equal to* a user account name in order to be processed by the SNMP agent.

Examples

```
-> snmp community map mode enable
-> snmp community map mode disable
```

Release History

Release 5.1; command was introduced.

Related Commands

snmp community map	Configures and enables a community string on the switch and maps it to an existing user account name.

MIB Objects

```
SNMPCommunityTable
   snmpCommunityIndex
   snmpCommunitySecurityName
   snmpCommunityStatus
```

show snmp community map

Shows the local community strings database.

show snmp community map

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guideline

N/A

Examples

```
-> show snmp community map
Community mode : enabled

status   community string                user name
--------+--------------------------------+--------------------------------
enabled   test_string1                   bb_usename
enabled   test_string2                   rr_usename
disabled  test_string3                   cc_usename
disabled  test_string4                   jj_usename
```

output definitions

Status	The Enabled/Disabled status of the community string.
Community String	The text that defines the community string.
User Name	The user account name.

Release History

Release 5.1; command was introduced.

Related Commands

snmp community map	Configures and enables a community string on the switch and maps it to an existing user account name.

snmp security

Configures SNMP security settings.

snmp security {no security | authentication set | authentication all | privacy set | privacy all | trap only}

Syntax Definitions

no security	The switch will accept all SNMP v1, v2, and v3 requests.
authentication set	The switch will accept all requests *except* v1, v2, and non-authenticated v3 set requests. SNMP v1, v2, and non-authenticated v3 set requests will be rejected.
authentication all	The switch will accept all requests *except* v1, v2, and non-authenticated v3 get, get-next, and set requests. SNMP v1, v2, and non-authenticated v3 get, get-next, and set requests will be rejected.
privacy set	The switch will accept *only* authenticated SNMP v3 get, get-next and encrypted v3 set requests. All other requests will be rejected.
privacy all	The switch will accept only encrypted v3 get, get-next, and set requests. All other requests will be rejected.
trap only	All SNMP get, get-next, and set requests will be rejected.

Defaults

By default, the SNMP security default is set to **privacy all**, which is the highest level of security.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Refer to the table below for a quick-reference list of security parameter and the SNMP request allowances for each parameter.

	v1 set v2 set v3 non-auth set	**v1 get v2 get v3 non-auth get/ get-next**	**v3 auth set**	**v3 auth get/ get-next**	**v3 encryp set**	**v3 encryp get/ get-next**
no security	accepted	accepted	accepted	accepted	accepted	accepted
authentication set	rejected	accepted	accepted	accepted	accepted	accepted
authentication all	rejected	rejected	accepted	accepted	accepted	accepted
privacy set	rejected	rejected	rejected	accepted	accepted	accepted
privacy all	rejected	rejected	rejected	rejected	accepted	accepted
trap only	rejected	rejected	rejected	rejected	rejected	rejected

Examples

```
-> snmp security no security
-> snmp security authentication set
-> snmp security authentication all
-> snmp security privacy set
-> snmp security trap only
```

Release History

Release 5.1; command was introduced.

Related Commands

show snmp security	Displays current SNMP security status.

MIB Objects

```
SNMPAgtConfig
   SnmpAgtSecurityLevel
```

show snmp security

Displays current SNMP security status.

show snmp security

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Refer to the command on page 10-11 for descriptions of the five SNMP security states: no security, authentication set, authentication all, privacy set, privacy all, and trap only.

Examples

```
-> show snmp security
snmp security = no security

-> show snmp security
snmp security = authentication set

-> show snmp security
snmp security = authentication all

-> show snmp security
snmp security = privacy set

-> show snmp security
snmp security = privacy all

-> show snmp security
snmp security = trap only
```

Release History

Release 5.1; command was introduced.

Related Commands

snmp security	Configures SNMP security settings.

show snmp statistics

Displays current SNMP statistics.

show snmp statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show snmp statistics
From RFC1907
  snmpInPkts                  = 801
  snmpOutPkts                 = 800
  snmpInBadVersions           = 0
  snmpInBadCommunityNames     = 0
  snmpInBadCommunityUses      = 0
  snmpInASNParseErrs          = 0
  snmpEnableAuthenTraps       = disabled(2)
  snmpSilentDrops             = 0
  snmpProxyDrops              = 0
  snmpInTooBigs               = 0
  snmpOutTooBigs              = 0
  snmpInNoSuchNames           = 0
  snmpOutNoSuchNames          = 0
  snmpInBadValues             = 0
  snmpOutBadValues            = 0
  snmpInReadOnlys             = 0
  snmpOutReadOnlys            = 0
  snmpInGenErrs               = 0
  snmpOutGenErrs              = 0
  snmpInTotalReqVars          = 839
  snmpInTotalSetVars          = 7
  snmpInGetRequests           = 3
  snmpOutGetRequests          = 0
  snmpInGetNexts              = 787
  snmpOutGetNexts             = 0
  snmpInSetRequests           = 7
  snmpOutSetRequests          = 0
  snmpInGetResponses          = 0
  snmpOutGetResponses         = 798
```

```
  snmpInTraps                  = 0
  snmpOutTraps                 = 0
From RFC2572
  snmpUnknownSecurityModels    = 0
  snmpInvalidMsgs              = 0
  snmpUnknownPDUHandlers       = 0
From RFC2573
  snmpUnavailableContexts      = 0
  snmpUnknownContexts          = 1
From RFC2574
  usmStatsUnsupportedSecLevels = 0
  usmStatsNotInTimeWindows     = 1
  usmStatsUnknownUserNames     = 1
  usmStatsUnknownEngineIDs     = 0
  usmStatsWrongDigests         = 0
  usmStatsDecryptionErrors     = 0
```

output definitions

From RFCxxxx	Displays the RFC number that defines the SNMP MIB objects listed.
MIB Objects	Name of the MIB object listed as an SNMP statistic.
= (integer)	The number of times the MIB object has been reported to the SNMP management station since the last reset.

Release History

Release 5.1; command was introduced.

Related Commands

N/A

show snmp mib family

Displays SNMP MIB information. Information includes MIP ID number, MIB table name, and command family.

show snmp mib family [*table_name***]**

Syntax Definitions

table_name	The name of the MIB table to be displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If a table name is not specified in the command syntax, all MIB table names will be displayed.
- If the command family is not valid for the entire MIB table, the command family will be displayed on a per-object basis.

Examples

```
-> show snmp mib family trapstationtable
MIP             MIB TABLE                    FAMILY
ID                 NAME
----+-----------------------------------+--------------------
001   aaaAcctSATable                      aaa
002   aaaAcctVlanTable                    avlan
003   aaaAuthSATable                      aaa
005   aaaAuthenticatedUserTable           avlan
…
093   chasMacAddressAllocTable            Chassis
094   chasMacAddressRangeTable            Chassis
096   configManager                       Config
097   directoryServerTable                policy
098   distObjectPseudo                    DEPENDENT ON THE NOMINATOR
                                          snmp :  1 3 5 7 9 11
                                          Chassis :  2 4 6 8 10
099   distObjectTable                     DEPENDENT ON THE NOMINATOR
                                          Chassis :  1 3 5 7 9 11
                                          snmp :  2 4 6 8 10
…
144   icmp                                ip
145   ifMIBObjects                        DEPENDENT ON THE IFINDEX
146   ifStackTable                        interface
147   ifTable                             DEPENDENT ON THE IFINDEX
148   ifXTable                            DEPENDENT ON THE IFINDEX
149   igmpCacheTable                      ipms
150   igmpInterfaceTable                  ipms
```

output definitions

MIP ID	Identification number for the MIP associated with this MIB Table.
MIB Table Name	Name of the MIB table.
Family	Command family to which this MIB table belongs.

Release History

Release 5.1; command was introduced.

Related Commands

show snmp trap filter	Displays SNMP trap filter information.

snmp trap absorption

Enables or disables the trap absorption function.

snmp trap absorption {enable | disable}

Syntax Definitions

enable	Enables SNMP trap absorption. When trap absorption is enabled, identical, repetitive traps sent by applications during a pre-configured time period will be absorbed, and therefore not sent to SNMP Manager stations configured on the switch.
disable	Disables SNMP trap absorption.

Defaults

By default, trap absorption is enabled.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

To view the current trap absorption status, use the **show snmp trap config** command.

Examples

```
-> snmp trap absorption enable
-> snmp trap absorption disable
```

Release History

Release 5.1; command was introduced.

Related Commands

show snmp trap config	Displays SNMP trap information. Information includes trap ID numbers and corresponding trap names and families.

MIB Objects

```
trapFilterTable
   trapAbsorption
```

snmp trap to webview

Enables the forwarding of traps to WebView.

snmp trap to webview {enable | disable}

Syntax Definitions

enable	Enables WebView forwarding. When WebView forwarding is enabled, all traps sent by switch applications are also forwarded to WebView. This allows a WebView session to retrieve the trap history log.
disable	Disables WebView forwarding.

Defaults

By default, WebView forwarding is enabled.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

To view the current WebView forwarding status, use the **show snmp trap config** command.

Examples

```
-> snmp trap to webview enable
-> snmp trap to webview disable
```

Release History

Release 5.1; command was introduced.

Related Commands

show snmp trap config	Displays SNMP trap information, including the current status for trap absorption and WebView forwarding.

MIB Objects

```
trapFilterTable
   trapToWebView
```

snmp trap replay

Replays stored traps from the switch to a specified SNMP station. This command is used to replay (to resend) traps on demand. This is useful in the event that any traps are lost in the network.

snmp trap replay *ip_address* **{***seq_id***}**

Syntax Definitions

ip_address	The IP address for the SNMP station to which traps will be replayed from the switch.
seq_id	The sequence number from which trap replay will begin. Each trap sent by the switch to an SNMP station has a sequence number. The sequence number reflects the order in which the trap was sent to the SNMP station. For example, the first trap sent to an SNMP station has a sequence number of 1; the second trap has a sequence number of 2, etc. If no sequence number is entered, all stored traps are replayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **show snmp station** command on page 10-5 to display the latest stored sequence number for each SNMP station.
- The switch replays traps in the same order that they were previously sent, beginning from the specified sequence number.
- When traps are replayed, the original dates on which the trap was issued, rather than the current dates are used.
- If the specified sequence number is lower than the oldest trap sequence number stored in the switch, the switch replays *all* stored traps.
- If the specified sequence number is equal to or greater than the oldest trap sequence number stored, the switch replays all stored traps from the specified sequence number up to the latest sequence number.
- If the specified sequence number is greater than the latest sequence number, no traps are replayed.

Examples

```
-> snmp trap replay 172.12.2.100
-> snmp trap replay 168.22.2.2
```

Release History

Release 5.1; command was introduced.

Related Commands

show snmp station	Displays the current SNMP station status.
show snmp trap replay	Displays SNMP trap replay information.

MIB Objects

```
trapStationTable
   trapStation Replay
```

snmp trap filter

Enables or disables SNMP trap filtering. Trap filtering is used to determine whether a trap or group of traps will be sent from the switch to a specified SNMP station.

snmp trap filter *ip_address trap_id_list*

no snmp trap filter *ip_address trap_id_list*

Syntax Definitions

ip_address	The IP address for the SNMP station for which trap filtering is being enabled or disabled.
trap_id_list	Specifies the trap(s) for which filtering is being enabled or disabled. Traps must be specified using the numeric trap ID. You can specify more than one trap in the command line; separate each trap ID with a space and no comma.

Defaults

By default, SNMP trap filtering is disabled.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- To *enable* trap filtering, use the syntax **snmp trap filter** *ip_address trap_id_list.*
- To *disable* trap filtering, use the syntax **no snmp trap filter** *ip_address trap_id_list*.
- When filtering is enabled, the specified trap(s) *will not* be sent to the SNMP station. When filtering is disabled, the specified traps *will* be sent to the SNMP station.
- To display a list of traps and their ID numbers, use the **show snmp trap config** command.

Examples

```
-> snmp trap filter 172.1.2.3 1
-> snmp trap filter 172.1.2.3 0 1 3 5
-> no snmp trap filter 172.1.2.3 1
-> no snmp trap filter 172.1.2.3 0 1 3 5
```

Release History

Release 5.1; command was introduced.

Related Commands

show snmp trap filter	Displays the current SNMP trap filter status.
show snmp trap config	Displays SNMP trap information including trap ID numbers, trap names, command families and absorption rate.

MIB Objects

```
trapFilterTable
   trapFilterStatus
```

snmp authentication trap

Enables or disables SNMP authentication failure trap forwarding.

snmp authentication trap {enable | disable}

Syntax Definitions

enable	Enables authentication failure trap forwarding. When enabled, the standard authentication failure trap is sent each time an SNMP authentication failure is detected.
disable	Disables authentication failure trap forwarding.

Defaults

By default, authentication failure trap forwarding is disabled.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> snmp authentication trap enable
-> snmp authentication trap disable
```

Release History

Release 5.1; command was introduced.

Related Commands

show snmp authentication trap	Displays the current authentication failure trap forwarding status.

MIB Objects

```
snmpGroup
   snmpEnableAuthenTraps
```

show snmp trap replay

Displays SNMP trap replay information.

show snmp trap replay

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

A maximum of 60 traps will be replayed.

Examples

```
-> show snmp trap replay
ipAddress       : oldest replay number
---------------------------------------
199.199.101.200 :       1234
199.199.105.202 :        578
199.199.101.203 :       1638
199.199.101.204 :       2560
```

output definitions

IPAddress	IP address of the SNMP station manager that replayed the trap.
Oldest Replay Number	Number of the oldest replayed trap.

Release History

Release 5.1; command was introduced.

Related Commands

show snmp trap replay	Replays stored traps from the switch to a specified SNMP station.

MIB Objects

```
trapStationTable
   snmpStation Replay
```

show snmp trap filter

Displays the current SNMP trap filter status.

show snmp trap filter

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

To display a list of traps and their ID numbers, use the **show snmp trap config** command.

Examples

```
-> show snmp trap filter
ipAddress       : trapId list
--------------------------------------------------------------------------------
199.199.101.200 :    0   1   2   3
199.199.101.201 : no filter
199.199.105.202 :    0   1   2   3   4   5   6   7   8   9  10  11  12  13  14
                    15  16  17  18  19
199.199.101.203 :   20  22  30
199.199.101.204 : no filter
```

output definitions

IPAddress	IP address of the SNMP management station that recorded the traps.
TrapId List	Identification number for the traps being filtered.

Release History

Release 5.1; command was introduced.

Related Commands

snmp trap filter	Enables or disables SNMP trap filtering.
show snmp trap config	Displays SNMP trap information including trap ID numbers, trap names, command families and absorption rate.

MIB Objects

```
trapFilterTable
   trapFilterEntry
```

show snmp authentication trap

Displays the current authentication failure trap forwarding status (i.e., enable or disable).

show snmp authentication trap

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show snmp authentication trap
snmp authentication trap = disable
```

Release History

Release 5.1; command was introduced.

Related Commands

snmp authentication trap	Enables or disables SNMP authentication failure trap forwarding.

MIB Objects

```
sessionAuthenticationTrap
```

show snmp trap config

Displays SNMP trap information. Information includes trap ID numbers, trap names, command families and absorption rate. This command also displays the Enabled/Disabled status of SNMP absorption and the Traps to WebView service.

show snmp trap config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show snmp trap config
Absorption service : enabled
Traps to WebView : enabled
Id trapName                              family          absorption
--+--------------------------------------+---------------+------------
 0 coldStart                             chassis         15 seconds
 1 warmStart                             chassis         15 seconds
 2 linkDown                              interface       15 seconds
 3 linkUp                                interface       15 seconds
 4 authenticationFailure                 snmp            15 seconds
 5 entConfigChange                       module          15 seconds
...
30 slPesudoCAMStatusTrap                 bridge          15 seconds
31 slbTrapException                      loadbalancing   15 seconds
32 slbTrapConfigChanged                  loadbalancing   15 seconds
33 slbTrapOperStatus                     loadbalancing   15 seconds
34 ifMauJabberTrap                       interface       15 seconds
35 sessionAuthenticationTrap             session         15 seconds
-------------------------------------------------------------------
```

output definitions

Id	Identification number for the trap.
Trap Name	Name of the trap.
Family	Family to which the trap belongs.
Absorption	Time needed for the trap to process.

Release History

Release 5.1; command was introduced.

Related Commands

show snmp mib family	Displays SNMP MIB information.
snmp trap absorption	Enables or disables the trap absorption function.
snmp trap to webview	Enables or disables the forwarding of SNMP traps to WebView.

MIB Objects

```
trapConfigTable
   trapConfigEntry
```

11 Hardware Routing Engine (HRE) Commands

Hardware Routing Engine (HRE) commands are used to view and update the configuration of the OmniSwitch 7700, 7700, and 8800 Layer 3 HRE. This feature is used to manage the HRE ASIC resources that perform IP and IPX packet classification and forwarding. The HRE command set manages five principal resources:

- Header cache entries
- Pseudo-CAM entries
- Hash function registers
- Modes
- Router MAC addresses

MIB information for the HRE commands is as follows:

Filename: AlcatelIND1Pcam.MIB
Module: ALCATEL-IND1-PCAM-MIB

A summary of the available commands is listed here:

hre mode configuration
hre clear changes
hre apply changes
show hre changes
show hre configuration
show hre pcam utilization
show hre statistics
show hre cache utilization

hre mode configuration

Sets the number of hash buckets for a particular mode, as well as the hash function to be used with that mode. Changes are stored in a pending change table and do not take effect until the **hre apply changes** command is issued. Refer to page 11-6 for more information.

hre mode configuration *slot/slice mode* **[***number hash_function***]**

Syntax Definitions

slot/slice	The slot and slice numbers containing the routing ASIC being configured (e.g., 11/0). A *slice* is a logical section of hardware and corresponds to particular ports on the interface. On the OmniSwitch 7700/7800, each network interface module has one slice (slice 0). On the OmniSwitch 8800, each network interface module may have up to 4 slices (slices 0 to 3). On the OmniSwitch 6600, each block of 24 ports makes up a slice (slice 0 and slice 1); the uplink slots are part of slice 0.
mode	An identifier for the Layer 3 HRE mode (0–3). A value of 3 signifies data used for modes 3 through 5 since these modes share hash function and memory space.
number	The number of hash buckets to be used for the specified mode. This value must be either 0 or a power of 2. The power of 2 value may range from 2048–65536.
hash_function	The hash function value. The HRE hash function maps a value to be hashed to an index hash value by selecting and concatenating a subset of bits in the hashed value. The hash function value is a bit-mask containing 80 bits (i.e., 20 hex digits), where a ‘1’ is found in the bit position for each bit that should be included in the hash function.

Defaults

parameter	default
number	16384
hash_function	0

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- You may want to change the hash table configuration to optimize it for your particular data flow. For example, if you want to create an unique flows of the destination IP addresses addresses such as 120.120.1.0, 120.120.2.0, 120.120.3.0, etc., in mode 0, use 0000ffff000000000000 hash function.
- Also, note that optimizing the hash function will cause all the current entries in the HRE to be cleared and then relearned; therefore, this should be done with extreme caution.
- Changes do not take effect until the **hre apply changes** command is issued. Refer to page 11-6 for more information.

Examples

```
-> hre mode configuration 1/0 3 2048 0f0003001f0000000700
-> hre mode configuration 1/0 0
```

Release History

Release 5.1; command was introduced.

Related Commands

hre clear changes	Clears pending changes that have been configured via the **hre mode configuration** command.
show hre configuration	Displays the current hash configuration for all modes on the specified hardware routing ASIC.

MIB Objects

```
alaCoroL3HreChangeTable
   alaCoroL3HreChangeSlotNumber
   alaCoroL3HreChangeSliceNumber
   alaCoroL3HreChangeModeNumber
   alaCoroL3HreChangeHashTableSize
   alaCoroL3HreChangeHashFunction
```

hre clear changes

Clears pending changes that have been configured via the **hre mode configuration** command. This command applies to pending changes only. Changes cannot be cleared after the **hre apply changes** command has been issued.

hre clear changes {all | *slot/slice mode***}**

Syntax Definitions

all	Pending configuration changes for *all* modes will be cleared.
slot/slice	The slot and slice numbers containing the routing ASIC (e.g., 11/0). When entered in the command line, pending configuration changes for only the specified slot, slice, and mode (see below) will be cleared from the pending changes table. The *slot/slice* value must be followed by a *mode* value in the command line. Refer to the examples below for more information.
mode	Specifies a particular mode. Values may range from 0–3. A value of 3 specifies data used for modes 3 through 5 since these modes share hash function and memory space. When entered in the command line, pending configuration changes for only the specified mode will be cleared from the pending changes table. (The *mode* value must be preceded by a *slot/slice* value in the command line. Refer to the examples below for more information.)

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

Changes cannot be cleared after the **hre apply changes** command has been issued.

Examples

```
-> hre clear changes all
-> hre clear changes 11/0 2
```

Release History

Release 5.1; command was introduced.

Related Commands

hre mode configuration	Sets the number of hash buckets for a particular mode, as well as the hash function to be used with that mode.

MIB Objects

```
alcatelIND1PCAMMIBObjects
   alaCoroL3HreUpdateChanges
alaCoroL3HreChangeTable
   alaCoroL3HreChangeSlotNumber
   alaCoroL3HreChangeSliceNumber
   alaCoroL3HreChangeModeNumber
   alaCoroL3HreChangeClear
```

hre apply changes

Applies all current HRE configuration changes to the hardware routing ASIC. To view the current pending changes table before applying a configuration, use the **show hre changes** command.

hre apply changes

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

You must have pending changes configured via the **hre mode configuration** command before issuing the this command.

Examples

```
-> hre apply changes
```

Release History

Release 5.1; command was introduced.

Related Commands

hre mode configuration	Sets the number of hash buckets for a particular mode, as well as the hash function to be used with that mode.
hre clear changes	Clears pending changes that have been configured via the **hre mode configuration** command.
show hre changes	Displays pending configuration changes for a particular slot and slice.

MIB Objects

```
alcatelIND1PCAMMIBObjects
   alaCoroL3HreUpdateChanges
```

show hre changes

Displays pending configuration changes for a particular slot and slice.

show hre changes *slot/slice*

Syntax Definitions

slot/slice	The slot and slice numbers containing the routing ASIC on which pending configuration changes are being displayed (e.g., 11/0). A *slice* is a logical section of hardware and corresponds to particular ports on the interface. On the OmniSwitch 7700/7800, each network interface module has one slice (slice 0). On the OmniSwitch 8800, each network interface module may have up to 4 slices (slices 0 to 3). On the OmniSwitch 6600, each block of 24 ports makes up a slice (slice 0 and slice 1); the uplink slots are part of slice 0.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

If there are no pending changes configured, the current operating configuration for the routing ASIC will display.

Examples

```
-> show hre changes 11/0
HRE Pending Changes
 Slot/
 Slice   Mode    Size   Hash Function
-------+------+-------+----------------------
  11/0      0   16384   ff3f0000000000000000
  11/0      1   16384   7f0000007f0000000000
  11/0      2   16384   3f0000001f0000000700
  11/0      3   16384   0f0003001f0000000700
```

output definitions

Slot/Slice	The slot and slice numbers for the routing ASIC currently being displayed.
Mode	The pending Layer 3 HRE modes in the pending changes table. Values may range from 0–3. A value of 3 signifies data used for modes 3 through 5 since these modes share hash function and memory space.

output definitions

Size	The pending number of hash buckets for the corresponding mode. This value may be either 0 or a power of 2. The power of 2 value may range from 2048–65536. The default value is 16384.
Hash Function	The pending hash function value for the corresponding mode. The HRE hash function maps a value to be hashed to an index hash value by selecting and concatenating a subset of bits in the hashed value. The hash function value is a bit-mask containing 80 bits (i.e., 20 hex digits), where a 1 is found in the bit position for each bit that should be included in the hash function.

Release History

Release 5.1; command was introduced.

Related Commands

hre mode configuration	Sets the number of hash buckets for a particular mode, as well as the hash function to be used with that mode.
hre clear changes	Clears pending changes that have been configured via the **hre mode configuration** command.
hre apply changes	Applies all current HRE configuration changes to the hardware routing ASIC.

show hre configuration

Displays the current hash configuration for all modes on the specified hardware routing ASIC.

show hre configuration *slot/slice*

Syntax Definitions

slot/slice	The slot and slice numbers containing the routing ASIC on which current configuration information is displayed (e.g., 11/0). A *slice* is a logical section of hardware and corresponds to particular ports on the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show hre configuration 10/0
HRE Mode Configuration
 Slot/
 Slice   Mode    Size   Hash Function
-------+------+-------+----------------------
  10/0      0   16384   ff3f0000000000000000
  10/0      1   16384   7f0000007f0000000000
  10/0      2   16384   3f0000001f0000000700
  10/0      3   16384   0f0003001f0000000700
```

output definitions

Slot/Slice	The slot and slice numbers for the Layer 3 HRE routing ASIC currently being displayed.
Mode	The current Layer 3 HRE modes configured on the routing ASIC. Values may range from 0–3. A value of 3 signifies data used for modes 3 through 5 since these modes share hash function and memory space. To specify a mode for a particular slot and slice, use the **hre mode configuration** command.
Size	The number of hash buckets currently being used for the corresponding mode. This value may be either 0 or a power of 2. The power of 2 value may range from 2048–65536. The default value is 16384. To change this value, use the **hre mode configuration** command.
Hash Function	The current hash function for the corresponding mode. For more information, refer to the **hre mode configuration** command on page 11-2.

Release History

Release 5.1; command was introduced.

Related Commands

hre mode configuration	Sets the number of hash buckets for a particular mode, as well as the hash function to be used with that mode.

show hre pcam utilization

Displays the resource utilization of the Layer 3 HRE pseudo-CAM for the specified hardware routing ASIC.

show hre pcam utilization *slot/slice*

Syntax Definitions

slot/slice	The slot and slice numbers containing the routing ASIC on which pseudo-CAM information is displayed (e.g., 11/0). A *slice* is a logical section of hardware and corresponds to particular ports on the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show hre pcam utilization 1/0
HRE PCAM Utilization
 Slot/          PCAM    Hash    Coll     Max     Avg
 Slice   Mode   Total   Inuse   Inuse   Depth   Depth
-------+------+-------+-------+-------+-------+-------
   1/0      0   16384       0       0       0       0
   1/0      1   16384       0       0       0       0
   1/0      2   16384       0       0       0       0
   1/0      3   16384       0       0       0       0
```

output definitions

Slot/Slice	The slot and slice numbers for the Layer 3 HRE routing ASIC currently being displayed.
Mode	The current Layer 3 HRE modes configured on the ASIC. Values may range from 0–3. A value of 3 signifies data used for modes 3 through 5 since these modes share hash function and memory space. To specify a mode for a slot and slice, use the **hre mode configuration** command.
PCAM Total	The number of hash buckets to be used for the corresponding mode. This value may be either 0 or a power of 2. The power of 2 value may range from 2048–65536. The default value is 16384.
Hash Inuse	The number of hash buckets currently in use for the corresponding mode. This value may be either 0 or a power of 2. The power of 2 value may range from 2048–65536. The default value is 0.

output definitions

Coll Inuse	The number of collision entries currently in use for the corresponding mode.
Max Depth	The maximum length for the collision chains in the mode.
Avg Depth	The average length for the collision chains in the mode.

Release History

Release 5.1; command was introduced.

Related Commands

N/A

show hre statistics

Displays the traffic statistics for the Layer 3 HRE.

show hre statistics *slot/slice*

Syntax Definitions

slot/slice	The slot and slice numbers containing the routing ASIC on which traffic statistics are displayed (e.g., 11/0). A *slice* is a logical section of hardware and corresponds to particular ports on the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

The table also reflects statistics changes that have occurred since the last **show hre statistics** command was entered.

Examples

```
-> show hre statistics 1/0
HRE Statistics
   Statistic            Packets                Bytes
---------------+----------------------+----------------------
 IP Received                         0                      0
 IP Forwarded                        0                      0
 IP Discarded                        0                      0
 IP Fragmented                       0                    N/A
 IP Fragments                        0                    N/A
 IP Failed Frag                      0                    N/A
 IPX Received                        0                      0
 IPX Forwarded                       0                      0
 IPX Discarded                       0                      0

Change in the last 22 seconds:
 IP Received                         0                      0
 IP Forwarded                        0                      0
 IP Discarded                        0                      0
 IP Fragmented                       0                    N/A
 IP Fragments                        0                    N/A
 IP Failed Frag                      0                    N/A
 IPX Received                        0                      0
 IPX Forwarded                       0                      0
```

```
IPX Discarded                    0                    0
```

output definitions

IP Received	The number of IP packets and bytes received on the HRE.
IP Forwarded	The number of IP packets and bytes routed on the HRE.
IP Discarded	The number of IP packets and bytes discarded on the HRE.
IP Fragmented	The number of IP packets fragmented on the HRE. (Not applicable to IP bytes.)
IP Fragments	The number of IP packet fragments generated. (Not applicable to IP bytes.)
IP Failed Frag	The number of IP fragments that could not be fragmented because IP flags precluded them. (Not applicable to IP bytes.)
IPX Received	The number of IPX packets and bytes received on the HRE.
IPX Forwarded	The number of IPX packets and bytes routed on the HRE.
IPX Discarded	The number of IPX packets and bytes discarded on the HRE.

Release History

Release 5.1; command was introduced.

Related Commands

N/A

show hre cache utilization

Displays the resource utilization of the Layer 3 HRE cache.

show hre cache utilization *slot/slice*

Syntax Definitions

slot/slice	The slot and slice numbers containing the routing ASIC on which the Layer 3 HRE cache is displayed (e.g., 11/0). A *slice* is a logical section of hardware and corresponds to particular ports on the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show hre cache utilization 1/0
HRE Cache Utilization
 Slot/
 Slice   Total   Inuse
-------+-------+-------
   1/0   65536       2
```

output definitions

Slot/Slice	The slot and slice numbers for the Layer 3 HRE routing ASIC currently being displayed.
Total	The total number of configured route cache entries. The default value is 65536.
Inuse	The number of route cache entries currently in use.

Release History

Release 5.1; command was introduced.

Related Commands

N/A

12 DNS Commands

A Domain Name System resolver is an internet service that translates host names into IP addresses. Every time you use a host name, a DNS service must resolve the name to an IP address. You can configure up to three domain name servers. If the primary DNS server does not know how to translate a particular host name, it asks the secondary DNS server (if specified). If this fails, it asks the third DNS server (if specified), until the correct IP address is returned (resolved). If all DNS servers have been queried and the name is still not resolved to an IP address, the DNS resolver will fail and issue an error message.

MIB information for the DNS commands is as follows:

Filename: AlcatelIND1System.mib
Module: ALCATEL-IND1-SYSTEM.MIB

A summary of the available commands is listed here.

ip domain-lookup
ip name-server
ip domain-name
show dns

ip domain-lookup

Enables or disables the DNS resolver.

ip domain-lookup

no ip domain-lookup

Syntax Definitions

N/A

Defaults

By default, the DNS resolver is disabled.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- You must use the **ip domain-name** command to set a default domain name for your DNS resolver(s) and the **ip name-server** command to specify up to three DNS servers to query on host lookups.
- The **ip domain-lookup** command enables the DNS resolver.
- Use the **no** form of the **ip domain-name** command to disable the DNS resolver.

Examples

```
-> ip domain-lookup
-> no ip domain-lookup
```

Release History

Release 5.1; command was introduced.

Related Commands

ip name-server	Specify the IP addresses of up to three servers to query on a host lookup.
ip domain-name	Sets or deletes the default domain name for DNS lookups.
show dns	Displays the current DNS resolver configuration and status.

MIB Objects

```
systemDNS
   systemDNSEnableDnsResolver
```

ip name-server

Specify the IP addresses of up to three servers to query on a host lookup.

ip name-server *server-address1* **[***server-address2* **[***server-address3***]]**

Syntax Definitions

server-address1	The IP address of the primary DNS server to query for host lookup. This is the only address that is required.
server-address2	The IP address of the secondary DNS server to query for host lookup. This server will be queried only if the desired host name or host IP address is not located by the primary DNS server. A second IP address is optional.
server-address3	The IP address of the DNS server with the lower priority. This server will be queried only if the desired host name or IP address is not located by the primary or secondary DNS servers. A third IP address is optional.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Configuration of the DNS resolver also requires that you first set the default domain name with the **ip domain-name** command. Next you can specify the IP addresses of the DNS servers by using the **ip name-server** command. Last, you must enable the DNS resolver function with the **ip domain-lookup** command.

Examples

```
-> ip name-server 189.202.191.14 189.202.191.15 188.255.19.1
-> ip name-server 10.255.11.66
```

Release History

Release 5.1; command was introduced.

Related Commands

ip domain-lookup	Enables or disables the DNS resolver.
ip domain-name	Sets or deletes the default domain name for DNS lookups.
show dns	Displays the current DNS resolver configuration and status.

MIB Objects

```
systemDNS
   systemDNSNsAddr1
   systemDNSNsAddr2
   systemDNSNsAddr3
```

ip domain-name

Sets or deletes the default domain name for DNS lookups.

ip domain-name *name*

no ip domain-name

Syntax Definitions

name	The default domain name for host lookups.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **ip domain-name** command to set the default domain name for DNS lookups. Use the **no** form of the **ip domain-name** command to delete the default domain name.

Examples

```
-> ip domain-name company.com
-> no ip domain-name
```

Release History

Release 5.1; command was introduced.

Related Commands

ip domain-lookup	Enables or disables the DNS resolver.
ip name-server	Specify the IP addresses of up to three servers to query on a host lookup.
show dns	Displays the current DNS resolver configuration and status.

MIB Objects

```
systemDNS
   systemDNSDomainName
```

show dns

Displays the current DNS resolver configuration and status.

show dns

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Examples

```
-> show dns
Resolver is  : enabled
domainName   : company.com
nameServer(s): 189.202.191.14
             : 189.202.191.15
             : 188.255.19.1
```

output definitions

Resolver is	Indicates whether the DNS resolver is enabled or disabled.
domainName	Indicates the default domain name assigned to the DNS lookups. This value is set by using the **ip domain-name** command.
nameServer(s)	Indicates the IP address(es) of the DNS server(s). These addresses are set by using the **ip name-server** command.

Release History

Release 5.1; command was introduced.

Related Commands

ip domain-lookup	Enables or disables the DNS resolver.
ip name-server	Specify the IP addresses of up to three servers to query on a host lookup.
ip domain-name	Sets or deletes the default domain name for DNS lookups.

MIB Objects

```
systemDNS
   systemDNSEnableDnsResolver
   systemDNSNsAddr1
   systemDNSNsAddr2
   systemDNSNsAddr3
   systemDNSDomainName
```

13 Link Aggregation Commands

Link aggregation is a way of combining multiple physical links between two switches into one logical link. The aggregate group operates within Spanning Tree as one virtual port and can provide more bandwidth than a single link. It also provides redundancy. If one physical link in the aggregate group goes down, link integrity is maintained.

There are two types of aggregate groups: static and dynamic. Static aggregate groups are manually configured on the switch with static links. Dynamic groups are set up on the switch but they aggregate links as necessary according to the Link Aggregation Control Protocol (LACP).

The dynamic aggregation software only is compatible with the following IEEE standard:

802.3ad — Aggregation of Multiple Link Segments

MIB information for the link aggregation commands is as follows:

Filename: AlcatelIND1LAG.MIB
Module: ALCATEL-IND1-LAG-MIB

A summary of available commands is listed here:

Static link aggregates	**static linkagg size** **static linkagg name** **static linkagg admin state** **static agg agg num**
Dynamic link aggregates	**lacp linkagg size** **lacp linkagg name** **lacp linkagg admin state** **lacp linkagg actor admin key** **lacp linkagg actor system priority** **lacp linkagg actor system id** **lacp linkagg partner system id** **lacp linkagg partner system priority** **lacp linkagg partner admin key** **lacp agg actor admin key** **lacp agg actor admin state** **lacp agg actor system id** **lacp agg actor system priority** **lacp agg partner admin state** **lacp agg partner admin system id** **lacp agg partner admin key** **lacp agg partner admin system priority** **lacp agg actor port priority** **lacp agg partner admin port** **lacp agg partner admin port priority**
Static and dynamic	**linkagg slot optimization** **linkagg slot single** **linkagg slot multiple** **show linkagg** **show linkagg port** **show linkagg slot optimization**

static linkagg size

Creates a static aggregate group between two switches. A static aggregate group contains static links.

static linkagg *agg_num* **size** *size* **[name** *name***] [admin state {enable | disable}]**

no static linkagg *agg_num*

Syntax Definitions

agg_num	The number corresponding to the static aggregate group. Must be a unique integer in the range 0–31 on OmniSwitch 7700/7800 switches, 0–29 on OmniSwitch 6600 Family switches, and 0–15 on OmniSwitch 8800 switches.
size	The maximum number of links allowed in the aggregate group. Values may be 2, 4, 8, or 16 on an OmniSwitch 7700, 7800, or 8800 switch. Values may 2, 4, or 8 on individual OmniSwitch 6600 Family switches and 2, 4, 8, or 16 on stack consisting of two to eight OmniSwitch 6600 Family switches.
name	The name of the static aggregate group. May be any alphanumeric string up to 255 characters long. Spaces must be contained within quotes (e.g., “Static Group 1”).
enable	Specifies that the static aggregate group is active and is able to aggregate links.
disable	Specifies that the static aggregate group is inactive and not able to aggregate links.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a static aggregate group from the configuration.
- The maximum number of link aggregate groups on the switch (static and dynamic combined) is 32 on an OmniSwitch 7700 or 7800 switch; 16 on an OmniSwitch 8800 switch; 4 on a single OmniSwitch 6624, 6600-P24, or 6602-24 switch; 8 on a single OmniSwitch 6648 or 6602-48 switch; and 30 on an OmniSwitch 6600 Family stack consisting of up to 8 OmniSwitch 6600 Family switches.
- If the static aggregate has any attached ports you must delete them with the **static agg agg num** command before you can delete it.
- Use the **lacp linkagg size** command to create a dynamic aggregation (i.e., LACP) group. See page 13-9 for more information about this command.

Examples

```
-> static linkagg 3 size 8
-> static linkagg 4 size 2 admin state disable
-> no static linkagg 3
```

Release History

Release 5.1; command was introduced.

Related Commands

show linkagg	Displays information about static and dynamic (LACP) link aggregate groups.

MIB Objects

```
alclnkaggAggTable
   alclnkaggAggNumber
   alclnkaggAggSize
   alclnkaggAggLacpType
   alclnkaggAggName
   alclnkaggAggAdminState
```

static linkagg name

Configures a name for an existing static aggregate group.

static linkagg *agg_num* **name** *name*

static linkagg *agg_num* **no name**

Syntax Definitions

agg_num	The number corresponding to the static aggregate group.
name	The name of the static aggregation group, an alphanumeric string up to 255 characters. Spaces must be contained within quotes (e.g., “Static Group 1”).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **no** form of the command to remove a name from a static aggregate.

Examples

```
-> static linkagg 2 name accounting
-> static linkagg 2 no name
```

Release History

Release 5.1; command was introduced.

Related Commands

static linkagg size	Creates a static aggregate group.
show linkagg	Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

```
alclnkaggAggTable
   alclnkaggAggNumber
   alclnkaggAggName
```

static linkagg admin state

Configures the administrative state (whether the static aggregate group is active or inactive) of a static aggregate group.

static linkagg *agg_num* **admin state {enable | disable}**

Syntax Definitions

agg_num	The number corresponding to the static aggregate group.
enable	Specifies that the static aggregate group is active and is able to aggregate links.
disable	Specifies that the static aggregate group is inactive and not able to aggregate links.

Defaults

parameter	default
enable | disable	enable

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

When the administrative state is set to **disable**, the static aggregate group is disabled.

Examples

```
-> static linkagg 2 admin state disable
```

Release History

Release 5.1; command was introduced.

Related Commands

static linkagg size	Creates a static aggregate group.
show linkagg	Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

```
alclnkaggAggTable
   alclnkaggAggNumber
   alclnkaggAggAdminState
```

static agg agg num

Configures a slot and port for a static aggregate group.

static agg [ethernet | fastethernet | gigaethernet] *slot/port* **agg num** *agg_num*

static agg no [ethernet | fastethernet | gigaethernet] *slot/port*

Syntax Definitions

ethernet	Documents that the port is 10 Mbps Ethernet.
fastethernet	Documents that the port is 100 Mbps Fast Ethernet.
gigaethernet	Documents that the port is 1 Gigabit Ethernet.
slot	The slot number for this aggregate.
port	The port that the switch will initially use as the Spanning Tree virtual port for this aggregate.
agg_num	The number corresponding to the static aggregate group.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove one or more ports from a static aggregate group.
- Mobile ports cannot be aggregated.
- A port may belong to only one aggregate group.
- Ports in a static aggregate must all be the same speed (e.g., all 10 Mbps, all 100 Mbps or all 1 Gigabit).
- On an OmniSwitch 7700, 7800, or 8800 switch, ports that belong to the same static aggregate group do not have to be configured sequentially and can be on any Network Interface (NI) or unit within a stack.
- On an OmniSwitch 6624, 6600-U24, 6600-P24, or 6602-24 switch, ports must be assigned sequentially and the first port configured must begin with port number 1, 9, 17, or 25.
- On an OmniSwitch 6648 switch, ports must be assigned sequentially and the first port configured must begin with port number 1, 9, 17, 25, 33, 41, 49, or 51.
- On an OmniSwitch 6602-48 switch, ports must be assigned sequentially and the first port configured must begin with port number 1, 9, 17, 25, 33, 41, or 49.
- No more than eight (8) ports can be assigned to the same static aggregate group on a single switch in a stack composed of OmniSwitch 6600 Family switches.

- The **ethernet**, **fastethernet**, and **gigaethernet** keywords do not modify a port's configuration. See Chapter 19, "Ethernet Port Commands," for information on CLI commands to configure Ethernet ports.

Examples

```
-> static agg 2/1 agg num 4
-> static agg no 2/1
```

Release History

Release 5.1; command was introduced.

Related Commands

static linkagg size	Creates a static aggregate group.
show linkagg port	Displays information about link aggregation ports.

MIB Objects

```
alclnkaggAggPortTable
   alclnkaggAggPortGlobalPortNumber
   alclnkaggAggPortLacpType
   alclnkaggAggPortSelectedAggNumber
```

lacp linkagg size

Creates a dynamic aggregate group that uses the Link Aggregation Control Protocol (LACP) to establish and maintain link aggregation. The **size** parameter is required to create the link aggregate group.

lacp linkagg *agg_num* **size** *size*
[name *name***]**
[admin state {enable | disable}]
[actor admin key *actor_admin_key***]**
[actor system priority *actor_system_priority***]**
[actor system id *actor_system_id***]**
[partner system id *partner_system_id***]**
[partner system priority *partner_system_priority***]**
[partner admin key *partner_admin_key***]**

no lacp linkagg *agg_num*

Syntax Definitions

agg_num	The number corresponding to the dynamic aggregate group. Must be a unique integer in the range 0–31 on OmniSwitch 7700/7800 switches, 0–29 on OmniSwitch 6600 Family switches, and 0–15 on OmniSwitch 8800 switches.
size	The maximum number of links that may belong to the aggregate. Values may be 2, 4, 8, or 16 on an OmniSwitch 7700, 7800, or 8800 switch. Values may 2, 4, or 8 on individual OmniSwitch 6600 Family switches, and 2, 4, 8, or 16 on stack consisting of two to eight OmniSwitch 6600 Family switches.
name	The name of the dynamic aggregate group. May be any alphanumeric string up to 255 characters long. Spaces must be contained within quotes (e.g., “Dynamic Group 1”).
enable	Specifies that the dynamic aggregate group is active and is able to aggregate links.
disable	Specifies that the dynamic aggregate group is inactive and not able to aggregate links.
actor_admin_key	The administrative key value associated with the dynamic aggregate group. Possible values are 0–65535.
actor_system_priority	The priority of the dynamic aggregate group. Possible values are 0–65535.
actor_system_id	The MAC address of the dynamic aggregate group on the switch.
partner_system_id	The MAC address of the remote system’s aggregate group to which the switch’s aggregate group is attached.
partner_system_priority	The priority of the remote system to which the aggregation group is attached. Possible values are 0–65535.

partner_admin_key	The administrative key for the aggregation group's remote partner. Possible values are 0–65535.

Defaults

parameter	default
enable | disable	enable

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a dynamic aggregate group from the configuration.
- The maximum number of link aggregate groups on the switch (static and dynamic combined) is 32 on an OmniSwitch 7700, or 7800 switch; 16 on an OmniSwitch 8800 switch; 4 on a single OmniSwitch 6624, 6600-P24, or 6602-24 switch; 8 on a single OmniSwitch 6648 or 6602-48 switch; and 30 on an OmniSwitch 6600 Family stack consisting of up to 8 OmniSwitch 6600 Family switches.
- If the dynamic group has any attached ports you must disable the group with the **lacp linkagg admin state** command before you can delete it.
- Optional parameters for the dynamic aggregate group may be configured when the aggregate is created or the dynamic aggregate group may be modified later.
- Use the **static linkagg size** command to create static aggregate groups. See page 13-3 for more information about this command.

Examples

```
-> lacp linkagg 2 size 4
-> lacp linkagg 3 size 2 admin state disable actor system priority 65535
```

Release History

Release 5.1; command was introduced.

Related Commands

show linkagg	Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

```
alclnkaggAggTable
   alclnkaggAggNumber
   alclnkaggAggSize
   alclnkaggAggLacpType
   alclnkaggAggName
   alclnkaggAggAdminState
   alclnkaggAggActorAdminKey
   alclnkaggAggActorSystemPriority
   alclnkaggAggActorSystemID
   alclnkaggAggPartnerSystemID
   alclnkaggAggPartnerSystemPriority
   alclnkaggAggPartnerAdminKey
```

lacp linkagg name

Configures a name for a dynamic aggregate group.

lacp linkagg *agg_num* **name** *name*

lacp linkagg *agg_num* **no name**

Syntax Definitions

agg_num	The number corresponding to the dynamic aggregate group.
name	The name of the dynamic aggregate group. May be any alphanumeric string up to 255 characters long. Spaces must be contained within quotes (e.g., “Dynamic Group 1”).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **no** form of the command to remove a name from a dynamic aggregate group.

Examples

```
-> lacp linkagg 2 name finance
-> lacp linkagg 2 no name
```

Release History

Release 5.1; command was introduced.

Related Commands

lacp linkagg size	Creates a dynamic aggregate group.
show linkagg	Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

```
alclnkaggAggTable
   alclnkaggAggNumber
   alclnkaggAggName
```

lacp linkagg admin state

Configures the administrative state of the dynamic aggregate (whether it is up and active, or down and inactive) group.

lacp linkagg *agg_num* **admin state {enable | disable}**

Syntax Definitions

agg_num	The number corresponding to the dynamic aggregate group.
enable	Specifies that the dynamic aggregate group is active and able to aggregate links.
disable	Specifies that the operation of a dynamic aggregate group cannot be performed.

Defaults

parameter	default
enable | disable	enable

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

When the administrative state is set to **disable**, the operation of a dynamic aggregation (LACP) group cannot be performed.

Examples

```
-> lacp linkagg 2 admin state disable
```

Release History

Release 5.1; command was introduced.

Related Commands

lacp linkagg size	Creates a dynamic aggregate group.
show linkagg	Displays information about static and dynamic (LACP) aggregate groups.
show linkagg port	Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

```
alclnkaggAggTable
   alclnkaggAggNumber
   alclnkaggAggAdminState
```

lacp linkagg actor admin key

Configures the administrative key associated with a dynamic aggregate group.

lacp linkagg *agg_num* **actor admin key** *actor_admin_key*

lacp linkagg *agg_num* **no actor admin key**

Syntax Definitions

agg_num	The number corresponding to the dynamic aggregate group.
actor_admin_key	The administrative key value associated with the dynamic aggregate group. The valid range is 0–65535.

Defaults

parameter	default
actor_admin_key	0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **no** form of the command to remove an actor admin key from a dynamic aggregate group.

Examples

```
-> lacp linkagg 3 actor admin key 2
-> lacp linkagg 3 no actor admin key
```

Release History

Release 5.1; command was introduced.

Related Commands

lacp linkagg size	Creates a dynamic aggregate group.
show linkagg	Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

```
alclnkaggAggTable
   alclnkaggAggNumber
   alclnkaggAggActorAdminKey
```

lacp linkagg actor system priority

Configures the priority of the dynamic aggregate group.

lacp linkagg *agg_num* **actor system priority** *actor_system_priority*

lacp linkagg *agg_num* **no actor system priority**

Syntax Definitions

agg_num	The number corresponding to the link aggregate group.
actor_system_priority	The priority of the switch's dynamic aggregate group in relation to other aggregate groups. Possible values are 0–65535.

Defaults

parameter	default
actor_system_priority	0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to return the value to its default.
- Ports with the same system priority value can join the same dynamic aggregate group.

Examples

```
-> lacp linkagg 3 actor system priority 100
-> lacp linkagg 3 no actor system priority
```

Release History

Release 5.1; command was introduced.

Related Commands

lacp linkagg size	Creates a dynamic aggregate group.
show linkagg	Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

```
alclnkaggAggTable
   alclnkaggAggNumber
   alclnkaggAggActorSystemPriority
```

lacp linkagg actor system id

Configures the MAC address of a dynamic aggregate group on the switch.

lacp linkagg *agg_num* **actor system id** *actor_system_id*

lacp linkagg *agg_num* **no actor system id**

Syntax Definitions

agg_num	The number corresponding to the dynamic aggregate group.
actor_system_id	The MAC address of the dynamic aggregate group on the switch in the hexadecimal format *xx:xx:xx:xx:xx:xx*.

Defaults

parameter	default
actor_system_id	0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **no** form of the command to remove an actor system ID from a dynamic aggregate group.

Examples

```
-> lacp linkagg 3 actor system id 00:20:da:81:d5:b0
-> lacp linkagg 3 no actor system id
```

Release History

Release 5.1; command was introduced.

Related Commands

lacp linkagg size	Creates a dynamic aggregate group.
show linkagg	Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

```
alclnkaggAggTable
   alclnkaggAggNumber
   alclnkaggAggActorSystemID
```

lacp linkagg partner system id

Configures the MAC address of the remote system's dynamic aggregate group to which the local switch's dynamic aggregate group is attached.

lacp linkagg *agg_num* **partner system id** *partner_system_id*

lacp linkagg *agg_num* **no partner system id**

Syntax Definitions

agg_num	The number corresponding to the dynamic aggregate group on the switch.
partner_system_id	The MAC address of the remote switch's dynamic aggregate group in the hexadecimal format *xx:xx:xx:xx:xx:xx*.

Defaults

parameter	default
partner_system_id	0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a partner system ID from a dynamic aggregate group.
- The *partner_system_id* and the *partner_system_priority* specify the remote system's priority.

Examples

```
-> lacp linkagg 2 partner system id 00:20:da4:32:81
-> lacp linkagg 2 no partner system id
```

Release History

Release 5.1; command was introduced.

Related Commands

lacp linkagg size	Creates a dynamic aggregate group.
show linkagg	Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

```
alclnkaggAggTable
   alclnkaggAggNumber
   alclnkaggAggPartnerSystemID
```

lacp linkagg partner system priority

Configures the priority of the remote switch's dynamic aggregate group to which the local switch's aggregate group is attached.

lacp linkagg *agg_num* **partner system priority** *partner_system_priority*

lacp linkagg *agg_num* **no partner system priority**

Syntax Definitions

agg_num	The number corresponding to the dynamic aggregate group.
partner_system_priority	The priority of the remote switch's dynamic aggregate group to which the local switch's aggregate group is attached. Possible values are 0–65535.

Defaults

parameter	default
partner_system_priority	0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **no** form of the command to return to the priority value to its default.

Examples

```
-> lacp linkagg 3 partner system priority 65535
-> lacp linkagg 3 no partner system priority
```

Release History

Release 5.1; command was introduced.

Related Commands

lacp linkagg size	Creates a dynamic aggregate group.
show linkagg	Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

```
alclnkaggAggTable
   alclnkaggAggNumber
   alclnkaggAggPartnerSystemPriority
```

lacp linkagg partner admin key

Configures the administrative key for the dynamic aggregation group's remote partner.

lacp linkagg *agg_num* **partner admin key** *partner_admin_key*

lacp linkagg *agg_num* **no partner admin key**

Syntax Definitions

agg_num	The number corresponding to the dynamic aggregate group.
partner_admin_key	The administrative key for the dynamic aggregation group's remote partner. Possible values are 0–65535.

Defaults

parameter	default
partner_admin_key	0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **no** form of the command to remove a partner admin key from a dynamic aggregate group.

Examples

```
-> lacp linkagg 3 partner admin key 1
-> lacp linkagg 3 no partner admin key
```

Release History

Release 5.1; command was introduced.

Related Commands

lacp linkagg size	Creates a dynamic aggregate group.
show linkagg	Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

```
alclnkaggAggTable
   alclnkaggAggNumber
   alclnkaggAggPartnerAdminKey
```

lacp agg actor admin key

Configures an actor administrative key for port, which allows a port to join a dynamic aggregate group.

lacp agg [ethernet | fastethernet | gigaethernet] *slot/port* **actor admin key** *actor_admin_key*
[actor admin state {[[no] active] [[no] timeout] [[no] aggregate] [[no] synchronize] [[no] collect] [[no] distribute] [[no] default] [[no] expire] | none}]
[actor system id *actor_system_id***]**
[actor system priority *actor_system_priority***]**
[partner admin system id *partner_admin_system_id***]**
[partner admin key *partner_admin_key***]**
[partner admin system priority *partner_admin_system_priority***]**
[partner admin state {[[no] active] [[no] timeout] [[no] aggregate] [[no] synchronize] [[no] collect] [[no] distribute] [[no] default] [[no] expire] | none}]
[actor port priority *actor_port_priority***]**
[partner admin port *partner_admin_port***]**
[partner admin port priority *partner_admin_port_priority***]**

lacp agg no [ethernet | fastethernet | gigaethernet] *slot/port*

Syntax Definitions

ethernet	Documents that the port is 10 Mbps Ethernet.
fastethernet	Documents that the port is 100 Mbps Fast Ethernet.
gigaethernet	Documents that the port is 1 Gigabit Ethernet.
slot	The slot number for this aggregate.
port	The port that the switch will initially use as the Spanning Tree virtual port for this aggregate.
actor_admin_key	The administrative key associated with this dynamic aggregate group. Possible values are 0–65535.
actor admin state	See the **lacp agg actor admin state** command on page 13-25.
actor_system_id	The MAC address of this dynamic aggregate group on the switch.
actor_system_priority	The priority of the dynamic aggregate group. Possible values are 0–255.
partner_admin_system_id	The MAC address of the remote switch's dynamic aggregate group.
partner_admin_key	The administrative key for the dynamic aggregation group's remote partner. Possible values are 0–65535.
partner_admin_system_priority	The priority of the remote system to which the dynamic aggregation group is attached. Possible values are 0–255.
partner admin state	See the **lacp agg partner admin state** command on page 13-31.
actor_port_priority	The priority of the actor port. Possible values are 0–255.

partner_admin_port	The administrative state of the partner port. Possible values are 0–65535.
partner_admin_port_priority	The priority of the partner port. Possible values are 0–255.

Defaults

parameter	default
[active] [timeout]	active, timeout, aggregate

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a slot and port from a dynamic aggregate group.
- Mobile ports cannot be aggregated.
- A port may belong to only one aggregate group.
- Ports in a dynamic aggregate must all be the same speed (e.g., all 100 Mbps or all 1 Gigabit).
- On an OmniSwitch 7700, 7800, or 8800 switch, ports that belong to the same dynamic aggregate group do not have to be configured sequentially and can be on any Network Interface (NI).
- On an OmniSwitch 6624, 6600-U24, 6600-P24, or 6602-24 switch, ports must be assigned sequentially and the first port configured must begin with port number 1, 9, 17, or 25.
- On an OmniSwitch 6648 switch, ports must be assigned sequentially and the first port configured must begin with port number 1, 9, 17, 25, 33, 41, 49, or 51.
- On an OmniSwitch 6602-48 switch, ports must be assigned sequentially and the first port configured must begin with port number 1, 9, 17, 25, 33, 41, or 49.
- No more than eight (8) ports can be assigned the same actor administrative key on a single switch in a stack composed of OmniSwitch 6600 Family switches.
- The **ethernet**, **fastethernet**, and **gigaethernet** keywords do not modify a port's configuration. See Chapter 19, "Ethernet Port Commands," for information on CLI commands to configure Ethernet ports.

Examples

```
-> lacp agg 3/1 actor admin key 0
-> lacp agg no 3/1
```

Release History

Release 5.1; command was introduced.

Related Commands

lacp linkagg size	Creates a dynamic aggregate group.
show linkagg port	Displays information about ports associated with a particular aggregate group or all aggregates.

MIB Objects

```
alclnkaggAggPortTable
   alclnkaggAggPortGlobalPortNumber
   alclnkaggAggActorAdminKey
   alclnkaggAggPortLacpType
   alclnkaggAggPortActorAdminState
   alclnkaggAggPortActorSystemID
   alclnkaggAggPortActorSystemPriority
   alclnkaggAggPortPartnerAdminSystemID
   alclnkaggAggPortPartnerAdminKey
   alclnkaggAggPortPartnerAdminSystemPriority
   alclnkaggAggPortPartnerAdminState
   alclnkaggAggPortActorPortPriority
   alclnkaggAggPortPartnerAdminPort
   alclnkaggAggPortPartnerAdminPortPriority
```

lacp agg actor admin state

Configures the system administrative state of the slot and port for the dynamic aggregate group on the local switch. The state values correspond to bits in the actor state octet in the LACPDU frame.

lacp agg [ethernet | fastethernet | gigaethernet] *slot/port* **actor admin state {[active] [timeout] [aggregate] [synchronize] [collect] [distribute] [default] [expire] | none}**

lacp agg [ethernet | fastethernet | gigaethernet] *slot/port*
actor admin state {[[no] active] [[no] timeout] [[no] aggregate] [[no] synchronize] [[no] collect] [[no] distribute] [[no] default] [[no] expire] | none}

Syntax Definitions

ethernet	Documents that the port is 10 Mbps Ethernet.
fastethernet	Documents that the port is 100 Mbps Fast Ethernet.
gigaethernet	Documents that the port is 1 Gigabit Ethernet.
slot	The slot number for this aggregate.
port	The port that the switch will initially use as the Spanning Tree virtual port for this aggregate.
active	Specifies that bit 0 in the actor state octet is enabled. When this bit is set, the dynamic aggregate group is able to exchange LACPDU frames. By default, this value is set.
timeout	Specifies that bit 1 in the actor state octet is enabled. When this bit is set, a short timeout is used for LACPDU frames. When this bit is disabled, a long timeout is used for LACPDU frames. By default, this value is set.
aggregate	Specifies that bit 2 in the actor state octet is enabled. When this bit is set, the system considers this port to be a potential candidate for aggregation. If this bit is not enabled, the system considers the port to be individual (it can only operate as a single link). By default, this value is set.
synchronize	Specifying this keyword has no effect because the system always determines its value. When this bit (bit 3) is set by the system, the port is allocated to the correct dynamic aggregation group. If this bit is not set by the system, the port is not allocated to the correct dynamic aggregation group.
collect	Specifying this keyword has no effect because the system always determines its value. When this bit (bit 4) is set by the system, incoming LACPDU frames are collected from the individual ports that make up the dynamic aggregate group.
distribute	Specifying this keyword has no effect because the system always determines its value. When this bit (bit 5) is set by the system, distributing outgoing frames on the port is disabled.
default	Specifying this keyword has no effect because the system always determines its value. When this bit (bit 6) is set by the system, it indicates

	that the actor is using defaulted partner information administratively configured for the partner.
expire	Specifying this keyword has no effect because the system always determines its value. When this bit (bit 7) is set by the system, the actor cannot receive LACPDU frames.
none	Resets all administrative states to their default configurations.

Defaults

parameter	default
[active] [timeout]	active, timeout, aggregate

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to restore LACPDU bit settings to their default configuration.
- When the actor admin state is set to **none**, all bit values are restored to their default configurations.
- The **ethernet**, **fastethernet**, and **gigaethernet** keywords do not modify a port's configuration. See Chapter 19, "Ethernet Port Commands," for information on CLI commands to configure Ethernet ports.

Examples

```
-> lacp agg 4/2 actor admin state synchronize no collect distribute
-> lacp agg 4/2 actor admin state no synchronize collect
-> lacp agg 4/2 actor admin state none
```

Release History

Release 5.1; command was introduced.

Related Commands

lacp linkagg size	Creates a dynamic aggregate group.
show linkagg port	Displays information about ports associated with a particular aggregate group or all aggregate groups.

MIB Objects

```
alclnkaggAggPortTable
   alclnkaggAggPortGlobalPortNumber
   alclnkaggAggPortActorAdminState
```

lacp agg actor system id

Configures the system ID (i.e., MAC address) for the local port associated with a dynamic aggregate group.

lacp agg [ethernet | fastethernet | gigaethernet] *slot/port* **actor system id** *actor_system_id*

lacp agg [ethernet | fastethernet | gigaethernet] *slot/port* **no actor system id**

Syntax Definitions

ethernet	Documents that the port is 10 Mbps Ethernet.
fastethernet	Documents that the port is 100 Mbps Fast Ethernet.
gigaethernet	Documents that the port is 1 Gigabit Ethernet.
slot	The slot number for this aggregate.
port	The port that the switch will initially use as the Spanning Tree virtual port for this aggregate.
actor_system_id	The MAC address of the dynamic aggregate group on the switch in the hexadecimal format *xx:xx:xx:xx:xx:xx*.

Defaults

parameter	default
actor_system_id	0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove an actor system ID from a slot and port associated with a dynamic aggregate group.
- The **ethernet**, **fastethernet**, and **gigaethernet** keywords do not modify a port's configuration. See Chapter 19, "Ethernet Port Commands," for information on CLI commands to configure Ethernet ports.

Examples

```
-> lacp 3/1 actor system id 00:20:da:06:ba:d3
-> lacp 3/1 no actor system id
```

Release History

Release 5.1; command was introduced.

Related Commands

lacp linkagg size	Creates a dynamic aggregate group.
show linkagg port	Displays information about ports associated with a particular aggregate group or all aggregate groups.

MIB Objects

```
alclnkaggAggPortTable
   alclnkaggAggPortGlobalPortNumber
   alclnkaggAggPortActorSystemID
```

lacp agg actor system priority

Configures the system priority of the port on the switch that belongs to the dynamic aggregate group.

lacp agg [ethernet | fastethernet | gigaethernet] *slot/port* **actor system priority** *actor_system_priority*

lacp agg [ethernet | fastethernet | gigaethernet] *slot/port*
no actor system priority

Syntax Definitions

ethernet	Documents that the port is 10 Mbps Ethernet.
fastethernet	Documents that the port is 100 Mbps Fast Ethernet.
gigaethernet	Documents that the port is 1 Gigabit Ethernet.
slot	The slot number for this aggregate.
port	The port that the switch will initially use as the Spanning Tree virtual port for this aggregate.
actor_system_priority	The priority of the dynamic aggregate group. Possible values are 0–255.

Defaults

parameter	default
actor_system_priority	0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove an actor system priority value from a slot and port associated with a dynamic aggregate group.
- The **ethernet**, **fastethernet**, and **gigaethernet** keywords do not modify a port's configuration. See Chapter 19, "Ethernet Port Commands," for information on CLI commands to configure Ethernet ports.

Examples

```
-> lacp agg ethernet 3/2 actor system priority 65
-> lacp agg ethernet 3/2 no actor system priority
```

Release History

Release 5.1; command was introduced.

Related Commands

lacp linkagg size	Creates a dynamic aggregate group.
show linkagg port	Displays information about ports associated with a particular aggregate group or all aggregates.

MIB Objects

```
AlcLnkAggAggPortTable
   alclnkaggAggPortGlobalPortNumber
   alclnkaggAggPortActorSystemPriority
```

lacp agg partner admin state

Configures the system administrative state of the slot and port for the dynamic aggregate group on the remote switch. The state values correspond to bits in the actor state octet in the LACPDU frame.

lacp agg [ethernet | fastethernet | gigaethernet] *slot*/*port* **partner admin state {[active] [timeout] [aggregate] [synchronize] [collect] [distribute] [default] [expire] | none}**

lacp agg [ethernet | fastethernet | gigaethernet] *slot*/*port* **partner admin state {[[no] active] [[no] timeout] [[no] aggregate] [[no] synchronize] [[no] collect] [[no] distribute] [[no] default] [[no] expire] | none}**

Syntax Definitions

ethernet	Documents that the port is 10 Mbps Ethernet.
fastethernet	Documents that the port is 100 Mbps Fast Ethernet.
gigaethernet	Documents that the port is 1 Gigabit Ethernet.
slot	The slot number for this aggregate.
port	The port that the switch will initially use as the Spanning Tree virtual port for this aggregate.
active	Specifies that bit 0 in the partner state octet is enabled. When this bit is set, the dynamic aggregate group is able to exchange LACPDU frames. By default, this value is set.
timeout	Specifies that bit 1 in the partner state octet is enabled. When this bit is set, a short timeout is used for LACPDU frames. When this bit is disabled, a long timeout is used for LACPDU frames. By default, this value is set.
aggregate	Specifies that bit 2 in the partner state octet is enabled. When this bit is set, the system considers this port to be a potential candidate for aggregation. If this bit is not enabled, the system considers the port to be individual (it can only operate as a single link). By default, this value is set.
synchronize	Specifies that bit 3 in the partner state octet is enabled. When this bit is set, the port is allocated to the correct dynamic aggregation group. If this bit is not enabled, the port is not allocated to the correct aggregation group. By default, this value is disabled.
collect	Specifying this keyword has no effect because the system always determines its value. When this bit (bit 4) is set by the system, incoming LACPDU frames are collected from the individual ports that make up the dynamic aggregate group.
distribute	Specifying this keyword has no effect because the system always determines its value. When this bit (bit 5) is set by the system, distributing outgoing frames on the port is disabled.
default	Specifying this keyword has no effect because the system always determines its value. When this bit (bit 6) is set by the system, it indicates

	that the partner is using defaulted actor information administratively configured for the actor.
expire	Specifying this keyword has no effect because the system always determines its value. When this bit (bit 7) is set by the system, the partner cannot receive LACPDU frames.
none	Resets all administrative states to their default configurations.

Defaults

parameter	default
[active] [timeout]	active, timeout, aggregate

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to restore LACPDU bit settings to their default configuration.
- When the partner admin state is set to **none**, all bit values are restored to their default configurations.
- The **ethernet**, **fastethernet**, and **gigaethernet** keywords do not modify a port's configuration. See Chapter 19, "Ethernet Port Commands," for information on CLI commands to configure Ethernet ports.

Examples

```
-> lacp agg 4/2 partner admin state synchronize collect distribute
-> lacp agg 4/2 partner admin state no synchronize no collect
```

Release History

Release 5.1; command was introduced.

Related Commands

lacp linkagg size	Creates a dynamic aggregate group.
show linkagg port	Displays information about ports associated with a particular aggregate group or all aggregate groups.

MIB Objects

```
alclnkaggAggPortTable
   alclnkaggAggPortGlobalPortNumber
   alclnkaggAggPortPartnerAdminState
```

lacp agg partner admin system id

Configures the partner administrative system ID for a dynamic aggregate group port.

lacp agg [ethernet | fastethernet | gigaethernet] *slot/port* **partner admin system id** *partner_admin_system_id*

lacp agg [ethernet | fastethernet | gigaethernet] *slot/port*
no partner admin system id

Syntax Definitions

ethernet	Documents that the port is 10 Mbps Ethernet.
fastethernet	Documents that the port is 100 Mbps Fast Ethernet.
gigaethernet	Documents that the port is 1 Gigabit Ethernet.
slot	The slot number for this aggregate.
port	The port that the switch will initially use as the Spanning Tree virtual port for this aggregate.
partner_admin_system_id	The MAC address of the remote dynamic aggregate group in the hexa-decimal format *xx:xx:xx:xx:xx:xx*.

Defaults

parameter	default
partner_admin_system_id	0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a partner administrative system ID from a slot and port associated with a dynamic aggregate group.
- The **ethernet**, **fastethernet**, and **gigaethernet** keywords do not modify a port's configuration. See Chapter 19, "Ethernet Port Commands," for information on CLI commands to configure Ethernet ports.

Examples

```
-> lacp agg 3/1 partner admin system id 00:20:da:05:f6:23
```

Release History

Release 5.1; command was introduced.

Related Commands

lacp linkagg size	Creates a dynamic aggregate group.
show linkagg port	Displays information about ports associated with a particular aggregate group or all aggregate groups.

MIB Objects

```
AlcLnkAggAggPortTable
   alclnkaggAggPortGlobalPortNumber
   alclnkaggAggPortPartnerAdminSystemID
```

lacp agg partner admin key

Configures the partner administrative key for a dynamic aggregate group port.

lacp agg [ethernet | fastethernet | gigaethernet] *slot/port* **partner admin key** *partner_admin_key*

lacp agg [ethernet | fastethernet | gigaethernet] *slot/port* **no partner admin key**

Syntax Definitions

ethernet	Documents that the port is 10 Mbps Ethernet.
fastethernet	Documents that the port is 100 Mbps Fast Ethernet.
gigaethernet	Documents that the port is 1 Gigabit Ethernet.
slot	The slot number for this aggregate.
port	The port that the switch will initially use as the Spanning Tree virtual port for this aggregate.
parnter_admin_key	The administrative key for the dynamic aggregation group's remote partner. Possible values are 0–65535.

Defaults

parameter	default
partner_admin_key	0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a partner admin key value from a slot and port associated with a dynamic aggregate group.
- The **ethernet**, **fastethernet**, and **gigaethernet** keywords do not modify a port's configuration. See Chapter 19, "Ethernet Port Commands," for information on CLI commands to configure Ethernet ports.

Examples

```
-> lacp agg 2/1 partner admin key 0
-> lacp agg 2/1 no partner admin key
```

Release History

Release 5.1; command was introduced.

Related Commands

lacp linkagg size	Creates a dynamic aggregate group.
show linkagg port	Displays detailed information about ports associated with a particular aggregate group or all aggregate groups.
show linkagg port	Displays information about slots and ports associated with all aggregate groups.

MIB Objects

```
AlcLnkAggAggPortTable
   alclnkaggAggPortGlobalPortNumber
   alclnkaggAggPortPartnerAdminKey
```

lacp agg partner admin system priority

Configures the partner system priority for a dynamic aggregate group port.

lacp agg [ethernet | fastethernet | gigaethernet] *slot/port* **partner admin system priority** *partner_admin_system_priority*

lacp agg [ethernet | fastethernet | gigaethernet] *slot/port*
no partner admin system priority

Syntax Definitions

ethernet	Documents that the port is 10 Mbps Ethernet.
fastethernet	Documents that the port is 100 Mbps Fast Ethernet.
gigaethernet	Documents that the port is 1 Gigabit Ethernet.
slot	The slot number for this aggregate.
port	The port that the switch will initially use as the Spanning Tree virtual port for this aggregate.
partner_admin_system_priority	The priority of the remote switch's dynamic aggregate group to which the aggregation group is attached. Possible values are 0–255.

Defaults

parameter	default
partner_admin_system_priority	0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a *partner_system_priority* value from a slot and port associated with a dynamic aggregate group.
- The **ethernet**, **fastethernet**, and **gigaethernet** keywords do not modify a port's configuration. See Chapter 19, "Ethernet Port Commands," for information on CLI commands to configure Ethernet ports.

Examples

```
-> lacp agg 2/1 partner admin system priority 65
-> lacp agg 2/1 no partner admin system priority
```

Release History

Release 5.1; command was introduced.

Related Commands

lacp linkagg size	Creates a dynamic aggregate group.
show linkagg port	Displays information about ports associated with a particular aggregate group or all aggregate groups.

MIB Objects

```
AlcLnkAggAggPortTable
   alclnkaggAggPortGlobalPortNumber
   alclnkaggAggPortAdminSystemPriority
```

lacp agg actor port priority

Configures the priority for an actor port.

lacp agg [ethernet | fastethernet | gigaethernet] *slot/port* **actor port priority** *actor_port_priority*

lacp agg [ethernet | fastethernet | gigaethernet] *slot/port* **no actor port priority**

Syntax Definitions

ethernet	Documents that the port is 10 Mbps Ethernet.
fastethernet	Documents that the port is 100 Mbps Fast Ethernet.
gigaethernet	Documents that the port is 1 Gigabit Ethernet.
slot	The slot number for this aggregate.
port	The port that the switch will initially use as the Spanning Tree virtual port for this aggregate.
actor_port_priority	The priority of the actor port. Possible values are 0–255.

Defaults

parameter	default
actor_port_priority	0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove an *actor_port_priority* value from a slot and port associated with a dynamic aggregate group.
- The **ethernet**, **fastethernet**, and **gigaethernet** keywords do not modify a port's configuration. See Chapter 19, "Ethernet Port Commands," for information on CLI commands to configure Ethernet ports.

Examples

```
-> lacp agg 2/1 actor port priority 100
-> lacp agg 2/1 no actor port priority
```

Release History

Release 5.1; command was introduced.

Related Commands

lacp linkagg size	Creates a dynamic aggregate group.
show linkagg port	Displays information about ports associated with a particular aggregate group or all aggregate groups.

MIB Objects

```
AlcLnkAggAggPortTable
   alclnkaggAggPortGlobalPortNumber
   alclnkaggAggPortActorPortPriority
```

lacp agg partner admin port

Configures the administrative status of a partner port.

lacp agg [ethernet | fastethernet | gigaethernet] *slot/port* **partner admin port** *partner_admin_port*

lacp agg [ethernet | fastethernet | gigaethernet] *slot/port*
no partner admin port

Syntax Definitions

ethernet	Documents that the port is 10 Mbps Ethernet.
fastethernet	Documents that the port is 100 Mbps Fast Ethernet.
gigaethernet	Documents that the port is 1 Gigabit Ethernet.
slot	The slot number for this aggregate.
port	The port that the switch will initially use as the Spanning Tree virtual port for this aggregate.
partner_admin_port	The administrative state of the partner port. Possible values are 0–65535.

Defaults

parameter	default
partner_admin_port	0

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove an *partner_admin_port* value from a slot and port associated with a dynamic aggregate group.
- The **ethernet**, **fastethernet**, and **gigaethernet** keywords do not modify a port's configuration. See Chapter 19, "Ethernet Port Commands," for information on CLI commands to configure Ethernet ports.

Examples

```
-> lacp agg 2/1 partner admin port 255
-> lacp agg 2/1 no partner admin port
```

Release History

Release 5.1; command was introduced.

Related Commands

lacp linkagg size	Creates a dynamic aggregate group.
show linkagg port	Displays information about ports associated with a particular aggregate group or all aggregate groups.

MIB Objects

```
AlcLnkAggAggPortTable
   alclnkaggAggPortGlobalPortNumber
   alclnkaggAggPortPartnerAdminPort
```

lacp agg partner admin port priority

Configures the priority for a partner port.

lacp agg [ethernet | fastethernet | gigaethernet] *slot/port* **partner admin port priority** *partner_admin_port_priority*

lacp agg [ethernet | fastethernet | gigaethernet] *slot/port*
no partner admin port priority

Syntax Definitions

ethernet	Documents that the port is 10 Mbps Ethernet.
fastethernet	Documents that the port is 100 Mbps Fast Ethernet.
gigaethernet	Documents that the port is 1 Gigabit Ethernet.
slot	The slot number for this aggregate.
port	The port that the switch will initially use as the Spanning Tree virtual port for this aggregate.
partner_admin_port_priority	The priority of the partner port. Possible values are 0–255.

Defaults

parameter	default
partner_admin_port_priority	0

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove an *partner_admin_port_priority* value from a slot and port associated with a dynamic aggregate group.
- The **ethernet**, **fastethernet**, and **gigaethernet** keywords do not modify a port's configuration. See Chapter 19, "Ethernet Port Commands," for information on CLI commands to configure Ethernet ports.

Examples

```
-> lacp agg 2/1 partner admin port priority 100
-> lacp agg 2/1 no partner admin port priority
```

Release History

Release 5.1; command was introduced.

Related Commands

lacp linkagg size	Creates a dynamic aggregate group.
show linkagg port	Displays information about ports associated with a particular aggregate group or all aggregate groups.

MIB Objects

```
AlcLnkAggAggPortTable
   alclnkaggAggPortGlobalPortNumber
   alclnkaggAggPortPartnerAdminPortPriority
```

linkagg slot optimization

Optimizes a Network Interface (NI) module on OmniSwitch 7700, 7800, and 8800 switches for static and dynamic link aggregation.

linkagg slot *slot* **optimization {enable | disable}**

Syntax Definitions

slot	The slot number of the NI module.
enable	Enables link aggregation optimization on an NI.
disable	Disables link aggregation optimization on an NI.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Second-generation NI modules are distinguished from first-generation NI modules by “ENI2” or “GNI2” in the part number. (First-generation modules have ENI, GNI, or 10GNI in their part numbers instead.) If the NI is a second-generation module you do not need to optimize it.
- In a chassis with both early-generation and newer NI modules you must configure static link aggregation on all early generation modules before configuring link aggregation on newer NI modules.
- When a port is a member of an aggregate group and optimization is enabled on this NI, all bridged traffic sent from any other port (not part of the aggregate group) on the same switching ASIC to the aggregate will be dropped. In this case, traffic needs to be routed between that port and the aggregate group.

Examples

```
-> linkagg slot 5 optimization enable
-> linkagg slot 2 optimization disable
```

Release History

Release 5.1; command was introduced.

Related Commands

static linkagg size	Creates a static aggregate group.
linkagg slot single	Configures an NI for a single link aggregation group.
linkagg slot multiple	Configures an NI for multiple link aggregation groups.
show linkagg	Displays information about static and dynamic (LACP) link aggregate groups.
show linkagg slot optimization	Displays link aggregation optimization status and configuration on a Network Interface (NI) module.

MIB Objects

```
alclnkaggSlotTable
   alclnkaggSlotStatus
```

linkagg slot single

Enables a single link aggregation group on a Network Interface (NI) module on OmniSwitch 7700, 7800, and 8800 switches.

linkagg slot *slot* **single**

Syntax Definitions

slot	The slot number of the NI module.

Defaults

By default, only a single link aggregation group can be configured on an NI module if the module has been optimized for link aggregation with the **linkagg slot optimization** command.

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Use the **linkagg slot multiple** command to enable multiple link aggregation groups on an NI module if the module has been optimized for link aggregation with the **linkagg slot optimization** command.
- When optimization is enabled on a given NI and multiple link aggregation groups are defined, each aggregate group *must* be part of a different VLAN. In other words, traffic cannot be bridged between aggregate groups on the same NI when optimization is enabled. Instead, traffic must be routed.

Examples

```
-> linkagg slot 5 single
```

Release History

Release 5.1; command was introduced.

Related Commands

static linkagg size	Creates a static aggregate group.
linkagg slot optimization	Optimizes an NI for link aggregation.
linkagg slot multiple	Configures an NI for multiple link aggregation groups.
show linkagg	Displays information about static and dynamic (LACP) link aggregate groups.
show linkagg slot optimization	Displays link aggregation optimization status and configuration on a Network Interface (NI) module.

MIB Objects

```
alclnkaggSlotTable
   alclnkaggMultipleAggPerSlot
```

linkagg slot multiple

Enables multiple link aggregation groups on a Network Interface (NI) module on OmniSwitch 7700, 7800, and 8800 switches.

linkagg slot *slot* **multiple**

Syntax Definitions

slot	The slot number of the NI module.

Defaults

By default, only a single link aggregation group can be configured on an NI module if the module has been optimized for link aggregation with the **linkagg slot optimization** command.

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Use the **linkagg slot single** command to enable a single link aggregation group on an NI module if the module has been optimized for link aggregation with the **linkagg slot optimization** command.
- When optimization is enabled on a given NI and multiple link aggregation groups are defined, each aggregate group *must* be part of a different VLAN. In other words, traffic cannot be bridged between aggregate groups on the same NI when optimization is enabled. Instead, traffic must be routed.

Examples

```
-> linkagg slot 5 multiple
```

Release History

Release 5.1; command was introduced.

Related Commands

static linkagg size	Creates a static aggregate group.
linkagg slot optimization	Optimizes an NI for link aggregation.
linkagg slot single	Configures an NI for a single link aggregation group.
show linkagg	Displays information about static and dynamic (LACP) link aggregate groups.
show linkagg slot optimization	Displays link aggregation optimization status and configuration on a Network Interface (NI) module.

MIB Objects

```
alclnkaggSlotTable
   alclnkaggMultipleAggPerSlot
```

show linkagg

Displays information about static and dynamic (LACP) aggregate groups.

show linkagg [*agg_num***]**

Syntax Definitions

agg_num	Specifies the aggregate group. Configured through the **static linkagg size** or **lacp linkagg size** command.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If no aggregation number is specified, information for all aggregate groups is displayed. If an aggregate number is specified, information about that aggregate group only is displayed. The fields included in the display depend on whether the aggregate group is a static or dynamic.
- Use the **show linkagg port** command to display information about aggregate group ports.

Examples

No aggregate group is specified:

```
-> show linkagg
Number  Aggregate  SNMP Id  Size  Admin State  Oper State     Att/Sel Ports
-------+----------+--------+----+-------------+-------------+-------------
   1     Static    40000001   8    ENABLED      UP             2   2
   2     Dynamic   40000002   4    ENABLED      DOWN           0   0
   3     Dynamic   40000003   8    ENABLED      DOWN           0   2
   4     Dynamic   40000004  16    ENABLED      UP             3   3
   5     Static    40000005   2    DISABLED     DOWN           0   0
```

Output fields are defined here:

output definitions

Number	The aggregate group number.
Aggregate	The type of aggregate group, which can be **Static** or **Dynamic**.
SNMP Id	The SNMP ID associated with the aggregate group.
Size	The number of links in this aggregate group.

output definitions (continued)

Admin State	The current administrative state of the aggregate group, which can be **ENABLED** or **DISABLED**. You can modify this parameter with the **static linkagg admin state** command (see page 13-6) for static aggregate groups and with the **lacp linkagg admin state** command (see page 13-13) for dynamic aggregate groups.
Oper State	The current operational state of the aggregate group, which can be **UP** or **DOWN**.
Att Ports	The number of ports actually attached to this aggregate group.
Sel Ports	The number of ports that could possibly attach to the aggregate group.

A static aggregate is specified:

```
-> show linkagg 5
Static Aggregate
  SNMP Id                  : 40000005,
  Aggregate Number         : 5,
  SNMP Descriptor          : Omnichannel Aggregate Number 5 ref 40000005 size 2,
  Name                     : AGG5,
  Admin State              : ENABLED,
  Operational State        : DOWN,
  Aggregate Size           : 2,
  Number of Selected Ports : 0,
  Number of Reserved Ports : 0,
  Number of Attached Ports : 0,
  Primary Port             : NONE
```

Output fields are defined here:

output definitions

SNMP Id	The SNMP ID associated with this static aggregate group.
Aggregate Number	The group number.
SNMP Descriptor	The standard MIB name for this static aggregate group.
Name	The name of this static aggregate group. You can modify this parameter with the **static linkagg name** command (see page 13-5).
Admin State	The administrative state of this static aggregate group, which can be **ENABLED** or **DISABLED**. You can modify this parameter with the **static linkagg admin state** command (see page 13-6).
Operational State	The operational state of this static aggregate group, which can be **UP** or **DOWN**.
Aggregate Size	The number of links configured for this static aggregate group.
Number of Selected Ports	The number of ports that could possibly attach to this static aggregate group.
Number of Reserved Ports	The total number of ports reserved for use in link aggregation by this static aggregate group. (**Note**: This field is not relevant for static aggregate groups.)

output definitions (continued)

Number of Attached Ports	The number of ports actually attached to this static aggregate group.
Primary Port	The port number of the first port to join this static aggregate group. If the first port to join the aggregate is no longer part of the aggregate group, the switch automatically assigns another port in the aggregate group to be the primary port.

A dynamic aggregate group is specified:

```
-> show linkagg 2
Dynamic Aggregate
  SNMP Id                   : 40000002,
  Aggregate Number          : 2,
  SNMP Descriptor           : Dynamic Aggregate Number 2 ref 40000002 size 4,
  Name                      : AGG 2,
  Admin State               : ENABLED,
  Operational State         : DOWN,
  Aggregate Size            : 4,
  Number of Selected Ports  : 0,
  Number of Reserved Ports  : 0,
  Number of Attached Ports  : 0,
  Primary Port              : NONE,
LACP
  MACAddress                : [00:1f:cc:00:00:00],
  Actor System Id           : [00:20:da:81:d5:b0],
  Actor System Priority     : 50,
  Actor Admin Key           : 120,
  Actor Oper Key            : 0,
  Partner System Id         : [00:20:da:81:d5:b1],
  Partner System Priority   : 70,
  Partner Admin Key         : 220,
  Partner Oper Key          : 0
```

Output fields are defined here:

output definitions

SNMP Id	The SNMP ID associated with this dynamic aggregate group.
Aggregate Number	The group number of this dynamic aggregate group.
SNMP Descriptor	The standard MIB name for this dynamic aggregate group.
Name	The name of this dynamic aggregate group. You can modify this parameter with the **lacp linkagg name** command (see page 13-12).
Admin State	The administrative state of this dynamic aggregate group, which can be **ENABLED** or **DISABLED**. You can modify this parameter with the **lacp linkagg admin state** command (see page 13-13).
Operational State	The operational state of this dynamic aggregate group, which can be **UP** or **DOWN**.
Aggregate Size	The number of links configured for this dynamic aggregate group.
Number of Selected Ports	The number of ports available to this dynamic aggregate group.
Number of Reserved Ports	The total number of ports reserved for use in link aggregation by this dynamic aggregate group.
Number of Attached Ports	The number of ports actually attached to this dynamic aggregate group.

output definitions (continued)

Primary Port	The port number of the first port to join this dynamic aggregate group. If the first port to join the aggregate group is no longer part of the aggregate group, the switch automatically assigns another port in the aggregate group to be the primary port.
MACAddress	The MAC address associated with the primary port.
Actor System Id	The MAC address of this dynamic aggregate group. You can modify this parameter with the **lacp linkagg actor system id** command (see page 13-17).
Actor System Priority	The priority of this dynamic aggregate group. You can modify this parameter with the **lacp linkagg actor system priority** command (see page 13-16).
Actor Admin Key	The administrative key associated with this dynamic aggregate group. You can modify this parameter with the **lacp linkagg actor admin key** command (see page 13-15).
Actor Oper Key	The operational key associated with this dynamic aggregate group.
Partner System Id	The MAC address of the remote dynamic aggregate group. You can modify this parameter with the **lacp linkagg partner system id** command (see page 13-18).
Partner System Priority	The priority of the remote system to which this dynamic aggregation group is attached. You can modify this parameter with the **lacp linkagg partner system priority** command (see page 13-20).
Partner Admin Key	The administrative key for this dynamic aggregation group's remote partner. You can modify this parameter with the **lacp linkagg partner admin key** command (see page 13-21).
Partner Oper Key	The operational key of the remote system to which the dynamic aggregation group is attached.

Release History

Release 5.1; command was introduced.

Related Commands

static linkagg size	Creates a static aggregate group.
lacp linkagg size	Creates a dynamic aggregate group.

MIB Objects

```
alclnkaggAggTable
   alclnkAggSize
   alclnkaggAggNumber
   alclnkaggAggDescr
   alclnkaggAggName
   alclnkaggAggLacpType
   alclnkaggAggAdminState
   alclnkaggAggOperState
   alclnkaggAggNbrSelectedPorts
   alclnkaggAggNbrAttachedPorts
   alclnkaggPrimaryPortIndex
   alclnkaggAggMACAddress
   alclnkaggAggActorSystemPriority
   alclnkaggAggActorSystemID
   alclnkaggAggPartnerAdminKey
   alclnkaggAggActorAdminKey
   alclnkaggAggActorOperKey
   alclnkaggAggPartnerSystemID
   alclnkaggAggPartnerSystemPriority
   alclnkaggAggPartnerOperKey
```

show linkagg port

Displays aggregate group information about a particular slot and port.

show linkagg port [*slot/port***]**

Syntax Definitions

slot	The slot number for this aggregate.
port	The port number for this aggregate.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

If no slot/port is specified, information for all slots/ports is displayed. If a particular slot or port is specified, the fields displayed depend upon whether or not the port belongs to a static aggregate group or dynamic (LACP) aggregate group.

Examples

```
-> show linkagg port

Slot/Port Aggregate SNMP Id   Status   Agg  Oper Link Prim
---------+---------+-------+----------+----+----+----+----
   1/1    Dynamic     1001  ATTACHED     2  UP   UP   YES
   1/2    Dynamic     1002  ATTACHED     2  UP   UP   NO
```

Output fields are defined here:

output definitions

Slot/Port	The slot/port associated with the aggregate group.
Aggregate	The type of aggregate group associated with the port, either **Static** or **Dynamic**.
SNMP Id	The SNMP ID associated with the aggregate group.
`Status`	The current status of the port, which can be which can be **CONFIGURED**, **PENDING**, **SELECTED**, or **RESERVED**.
`Agg`	The number of the aggregate group associated with this port.
`Oper`	The operational status of the port, which can be **Up** or **Down**.
`Link`	The operational status of the link, which can be **Up** or **Down**.
`Prim`	Whether the port is the primary or not.

A port that belongs to a static aggregate is specified:

```
-> show linkagg port 4/1
Static Aggregable Port
  SNMP Id                       : 4001,
  Slot/Port                     : 4/1,
  Administrative State          : ENABLED,
  Operational State             : DOWN,
  Port State                    : CONFIGURED,
  Link State                    : DOWN,
  Selected Agg Number           : 2,
  Port position in the aggregate: 0,
  Primary port                  : NONE
```

Output fields are defined here:

output definitions

SNMP Id	The SNMP ID associated with this port.
Slot/Port	The slot and port number.
Administrative State	The current administrative state of this port, which can be **ENABLED** or **DISABLED**.
Operational State	The current operational state of the port, which can be **UP** or **DOWN**.
Port State	The current operational state of the port, which can be which can be **CONFIGURED**, **PENDING**, **SELECTED**, or **RESERVED**.
Link State	The current operational state of the link from this port to its remote partner, which can be **UP** or **DOWN**.
Selected Agg Number	The number associated with the static aggregate group to which the port is attached.
Port position in the aggregate	The rank of this port within the static aggregate group. Possible values are 0–15.
Primary Port	The port number of the first port to join this static aggregate group. If the first port to join the aggregate is no longer part of the aggregate group, the switch automatically assigns another port in the aggregate group to be the primary port.

A port that belongs to a dynamic aggregate is specified:

```
-> show linkagg port 2/1
Dynamic Aggregable Port
  SNMP Id                       : 2001,
  Slot/Port                     : 2/1,
  Administrative State          : ENABLED,
  Operational State             : DOWN,
  Port State                    : CONFIGURED,
  Link State                    : DOWN,
  Selected Agg Number           : NONE,
  Primary port                  : UNKNOWN,
LACP
  Actor System Priority         : 10,
  Actor System Id               : [00:d0:95:6a:78:3a],
  Actor Admin Key               : 8,
  Actor Oper Key                : 8,
  Partner Admin System Priority : 20,
  Partner Oper System Priority  : 20,
  Partner Admin System Id       : [00:00:00:00:00:00],
  Partner Oper System Id        : [00:00:00:00:00:00],
  Partner Admin Key             : 8,
  Partner Oper Key              : 0,
  Attached Agg Id               : 0,
  Actor Port                    : 7,
  Actor Port Priority           : 15,
  Partner Admin Port            : 0,
  Partner Oper Port             : 0,
  Partner Admin Port Priority   : 0,
  Partner Oper Port Priority    : 0,
  Actor Admin State             : act1.tim1.agg1.syn0.col0.dis0.def1.exp0
  Actor Oper State              : act1.tim1.agg1.syn0.col0.dis0.def1.exp0,
  Partner Admin State           : act0.tim0.agg1.syn1.col1.dis1.def1.exp0,
  Partner Oper State            : act0.tim0.agg1.syn0.col1.dis1.def1.exp0
```

Output fields are defined here:

output definitions

SNMP Id	The SNMP ID associated with this port.
Slot/Port	The slot and port number.
Administrative State	The current administrative state of this port, which can be **ENABLED** or **DISABLED**.
Operational State	The current operational state of the port, which can be **UP** or **DOWN**.
Port State	The current operational state of the port, which can be **CONFIGURED**, **PENDING**, **SELECTED**, or **AGGREGATED**.
Link State	The current operational state of the link from this port to its remote partner, which can be **UP** or **DOWN**.
Selected Agg Number	The number associated with the dynamic aggregate group to which the port is attached.
Primary Port	The port number of the first port to join this dynamic aggregate group. If the first port to join the aggregate is no longer part of the aggregate group, the switch automatically assigns another port in the aggregate group to be the primary port.

output definitions (continued)

Actor System Priority	The actor system priority of this port. You can modify this parameter with the **lacp agg actor system priority** command (see page 13-29).
Actor System Id	The actor system ID (i.e., MAC address) of this port. You can modify this parameter with the **lacp agg actor system id** command (see page 13-27).
Actor Admin Key	The actor administrative key value for this port. You can modify this parameter with the **lacp agg actor admin key** command (see page 13-22).
Actor Oper Key	The actor operational key associated with this port.
Partner Admin System Priority	The administrative priority of the remote system to which this port is attached. You can modify this parameter with the **lacp agg partner admin system priority** command (see page 13-37).
Partner Oper System Priority	The operational priority of the remote system to which this port is attached.
Partner Admin System Id	The administrative MAC address associated with the remote partner's system ID. This value is used along with Partner Admin System Priority, Partner Admin Key, and Partner Admin Port Priority to manually configure aggregation. You can modify this parameter with the **lacp agg partner admin system id** command (see page 13-33).
Partner Oper System id	The MAC address that corresponds to the remote partner's system ID.
Partner Admin Key	The administrative value of the key for the remote partner. This value is used along with Partner Admin System Priority, Partner Admin System, Partner Admin Port, and Partner Admin Port Priority to manually configure aggregation. You can modify this parameter with the **lacp agg partner admin key** command (see page 13-35).
Partner Oper Key	The current operational value of the key for the protocol partner.
Attached Agg ID	The ID of the aggregate group that the port has attached itself to. A value of zero indicates that the port is not attached to an aggregate group.
Actor Port	The port number locally assigned to this port.
Actor Port Priority	The actor priority value assigned to the port. You can modify this parameter with the **lacp agg actor port priority** command (see page 13-39).
Partner Admin Port	The administrative value of the port number for the protocol partner. This value is used along with Partner Admin System Priority, Partner Admin System ID, Partner Admin Key, and Partner Admin Port Priority to manually configure aggregation. You can modify this parameter with the **lacp agg partner admin port** command (see page 13-41).
Partner Oper Port	The operational port number assigned to the port by the port's protocol partner.
Partner Admin Port Priority	The administrative port priority of the protocol partner. This value is used along with Partner Admin System Priority, Partner Admin System ID, and Partner Admin Key to manually configure aggregation. You can modify this parameter with the **lacp agg partner admin port priority** command (see page 13-43).
Partner Oper Port Priority	The priority value assigned to the this port by the partner.

output definitions (continued)

Actor Admin State	The administrative state of the port. You can modify this parameter with the **lacp agg actor admin state** command (see page 13-25).
Actor Oper State	The current operational state of the port.
Partner Admin State	The administrative state of the partner's port. You can modify this parameter with the **lacp agg partner admin state** command (see page 13-31).
Partner Oper State	The current operational state of the partner's port.

Release History

Release 5.1; command was introduced.

Related Commands

static agg agg num	Configures a slot and port for a static aggregate group.
lacp agg actor admin key	Configures a slot and port for a dynamic aggregate group.
show linkagg	Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

```
alclnkaggAggPortTable
   alclnkaggAggPortActorSystem
   alclnkaggAggPortActorSystemPriority
   alclnkaggAggPortActorSystemID
   alclnkaggAggPortActorAdminKey
   alclnkaggAggPortActorOperKey
   alclnkaggAggPortPartnerAdminSystemPriority
   alclnkaggAggPortPartnerOperSystemPriority
   alclnkaggAggPortPartnerAdminSystemID
   alclnkaggAggPortPartnerOperSystemID
   alclnkaggAggPortPartnerAdminKey
   alclnkaggAggPortPartnerOperKey
   alclnkaggAggPortSelectedAggID
   alclnkaggAggPortAttachedAggID
   alclnkaggAggPortActorPort
   alclnkaggAggPortActorPortPriority
   alclnkaggAggPortPartnerAdminPort
   alclnkaggAggPortPartnerOperPort
   alclnkaggAggPortPartnerAdminPortPriority
   alclnkaggAggPortPartnerOperPortPriority
   alclnkaggAggPortActorAdminState
   alclnkaggAggPortActorOperState
   alclnkaggAggPortPartnerAdminState
   alclnkaggAggPortPartnerOperState
```

show linkagg slot optimization

Displays link aggregation optimization status and configuration on a Network Interface (NI) module.

show linkagg slot *slot* **optimization**

Syntax Definitions

slot	The slot number of the NI module.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show linkagg slot 15 optimization
Link aggregation optimization is enabled for slot 15
Multiple aggregates per slot disabled for slot 15
```

Output fields are defined here:

output definitions

Link aggregation optimization	This field displays whether link aggregation optimization has been enabled or disabled (the default) for this NI.
Multiple aggregates per slot	This field displays whether this NI allows a single link aggregation group (the default) or multiple link aggregation groups.

Release History

Release 5.1; command was introduced.

Related Commands

linkagg slot optimization	Optimizes NI modules on OmniSwitch 7700, 7800, and 8800 switches for link aggregation.
linkagg slot single	Enables a single link aggregation group on an NI module on OmniSwitch 7700, 7800, and 8800 switches.
linkagg slot multiple	Enables multiple link aggregation groups on an NI module on OmniSwitch 7700, 7800, and 8800 switches.

MIB Objects

```
alclnkaggSlotTable
   alclnkaggSlotStatus
   alclnkaggMultipleAggPerSlot
```

14 Interswitch Protocol Commands

Alcatel Interswitch Protocols (AIP) are used to discover and advertise adjacent switch information. Only one protocol is supported:

- Alcatel Mapping Adjacency Protocol (AMAP), used to discover the topology of OmniSwitches and Omni Switch/Routers (Omni S/R).

This chapter includes descriptions of AMAP commands.

MIB information for AMAP commands are as follows:

Filename: alcatelIND1InterswitchProtocol.MIB
Module: ALCATEL-IND1-INTERSWITCH-PROTOCOL-MIB

A summary of the available commands is listed here:

Mapping Adjacency Protocol	**amap** **amap discovery time** **amap common time** **show amap**

amap

Enables or disables the Alcatel Mapping Adjacency Protocol (AMAP) on the switch. AMAP discovers adjacent switches by sending and responding to Hello update packets on active Spanning Tree ports.

amap {enable | disable}

Syntax Definitions

enable	Enables AMAP.
disable	Disables AMAP.

Defaults

By default, AMAP is enabled on the switch.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Adjacent switches are defined as those having a Spanning Tree path between them and no other switch between them on the same Spanning Tree path that has AMAP enabled.

Examples

```
-> amap disable
-> amap enable
```

Release History

Release 5.1; command was introduced.

Related Commands

amap discovery time	Sets the discovery transmission time interval used by active Spanning Tree ports in the discovery transmission state.
amap common time	Sets the common transmission time interval used by active Spanning Tree ports in the common transmission state.
show amap	Displays adjacent switches and associated MAC addresses, ports, VLANs, and IP addresses.

MIB Objects

`aipAMAPstate`

amap discovery time

Sets the discovery transmission time interval. In the discovery transmission state, an active port sends AMAP Hello packets to detect adjacent switches. The discovery transmission time specifies the number of seconds to wait between each Hello packet transmission.

amap discovery [time] *seconds*

Syntax Definitions

seconds	Discovery transmission time value, in seconds (1–65535). Do not use commas in the value.

Defaults

By default, the discovery transmission time is set to 30 seconds.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use of the **time** command keyword is optional.
- When AMAP is enabled, all active Spanning Tree ports start out in the discovery transmission state.
- Ports that receive Hello packets before three discovery transmission times expire send a Hello reply and transition to the common transmission state.
- Ports that do not receive Hello packets before three discovery transmission times expire revert to the passive reception state.
- Ports in the passive reception state do not send Hello packets and do not use any timer to determine how long to wait for Hello packets.
- The discovery transmission time value is also used by ports in the common transmission state to determine how long to wait for Hello packets (see page 14-5).

Examples

```
-> amap discovery 1200
-> amap discovery time 600
```

Release History

Release 5.1; command was introduced.

Related Commands

amap	Enables (default) or disables AMAP on a switch.
amap common time	Sets the common transmission time interval used by active Spanning Tree ports in the common transmission state.
show amap	Displays adjacent switches and associated MAC addresses, ports, VLANs, and IP addresses.

MIB Objects

`aipAMAPdisctime`

amap common time

Sets the common phase transmission time interval. In the common transmission state, an active port sends AMAP Hello packets to determine adjacent switch failures and disconnects. The common transmission time specifies the number of seconds to wait between each Hello packet transmission.

amap common [time] *seconds*

Syntax Definitions

seconds	Common transmission time value in seconds (1–65535). Do not use commas in the value.

Defaults

By default, the common transmission time is set to 300 seconds.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use of the **time** command keyword is optional.
- To avoid synchronization with adjacent switches, the common transmission time is jittered randomly by plus or minus ten percent. For example, if the default time is used (300 seconds), the jitter is plus or minus 30 seconds.
- The common transmission time value is only used by ports in the common transmission state.
- If a Hello packet is received from an adjacent switch before the common transmission time has expired, the switch sends a Hello reply and restarts the common transmission timer.
- A port reverts to the discovery transmission state if a Hello response is not received after the discovery time interval (see page 14-3) has expired.

Examples

```
-> amap common 1200
-> amap common time 600
```

Release History

Release 5.1; command was introduced.

Related Commands

amap	Enables (default) or disables AMAP on a switch.
amap discovery time	Sets the discovery transmission time interval used by active Spanning Tree ports in the discovery transmission state.
show amap	Displays adjacent switches and associated MAC addresses, ports, VLANs, and IP addresses.

MIB Objects

`aipAMAPcommontime`

show amap

Displays adjacent switches and associated MAC addresses, ports, VLANs, IP addresses, and system names.

show amap

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Remote switches that stop sending Hello packets and are connected to an AMAP switch via a hub may take up to two times the common transmission time to age out of the AMAP database and no longer appear in this show command display.

Examples

```
-> show amap
AMAP is currently enabled,
AMAP Common    Phase Timeout Interval (seconds) = 300,
AMAP Discovery Phase Timeout Interval (seconds) = 30

Remote Host Description = falconCmm
Remote Host Base MAC    = 00:00:00:00:00:00
Local  Interface        = 1/2, VLAN  = 200
Remote Interface        = 3/1, VLAN  = 200
Remote IP Address Configured = 1
  2.0.0.10

Remote Host Description = falconCmm
Remote Host Base MAC    = 00:d0:95:6b:09:40
Local  Interface        = 3/1, VLAN  = 1
Remote Interface        = 6/1, VLAN  = 1
Remote IP Address Configured = 1
  2.0.0.11
```

output definitions

AMAP is currently	The AMAP status: **enabled** (default) or **disabled**. Use the **amap** command to change the AMAP status for the switch.
AMAP Common Phase Timeout Interval (seconds)	The number of seconds to wait between each Hello packet transmission during the common phase. Use the **amap common time** command to change this value.

output definitions (continued)

AMAP Discovery Phase Time-out Interval (seconds)	The number of seconds to wait between each Hello packet transmission during the discovery phase. Use the **amap discovery time** command to change this value.
Remote Host Description	The system name for the adjacent switch.
Remote Host Base MAC	The chassis base MAC address for the adjacent switch.
Local Interface	The local switch port/VLAN that received the AMAP packet.
Remote Interface	The adjacent switch port/VLAN that sent the AMAP packet.
Remote IP Address Configured	The number of IP addresses configured on the adjacent switch. The actual IP address values are listed below this field.

Release History

Release 5.1; command was introduced.

Related Commands

amap	Enables (default) or disables AMAP on a switch.
amap discovery time	Sets the discovery transmission time interval used by active Spanning Tree ports in the discovery transmission state.
amap common time	Sets the common transmission time interval used by active Spanning Tree ports in the common transmission state.

15 802.1Q Commands

Alcatel's 802.1Q is an IEEE standard for sending frames through the network tagged with VLAN identification. This chapter details configuring and monitoring 802.1Q tagging on a single port in a switch or an aggregate of ports on a switch.

Alcatel's version of 802.1Q complies with the Draft Standard *P802.1Q/D11 IEEE Standards for Local And Metropolitan Area Network: Virtual Bridged Local Area Networks, July 30, 1998.*

MIB information for the 802.1Q commands is as follows:

Filename: alcatelIND1Dot1Q.mib
Module: ALCATEL-IND1-DOT1Q-MIB

A summary of available commands is listed here:

vlan 802.1q
vlan 802.1q frame type
vlan 802.1q force tag internal
debug 802.1q
show 802.1q

Note. Before using 802.1Q, the VLAN for 802.1Q must be created using the commands described in Chapter 21, "VLAN Management Commands."

Configuration procedures for 802.1Q are explained in "Configuring 802.1Q," in the *OmniSwitch 6600 Family 8 Network Configuration Guide* or *OmniSwitch 7700/7800/8800 Network Configuration Guide*.

vlan 802.1q

Creates, deletes, or modifies 802.1Q tagging on a single port or on an aggregate of ports.

vlan *vid* **802.1q {***slot/port* **|** *aggregate_id***} [***description***]**

vlan *vid* **no 802.1q {***slot/port* **|** *aggregate_id***}**

Syntax Definitions

vid	The VLAN identification number for a preconfigured VLAN that will handle the 802.1Q traffic for this port. The valid range is 1 to 4094.
slot	The slot number for the 802.1Q tagging.
port	The port number for the 802.1Q tagging.
aggregate_id	The link aggregation ID, which allows you to configure 802.1Q tagging on an aggregate of ports. The valid range is 1 to 31.
description	An optional textual description (up to 32 characters) for this 802.1Q tag. Spaces must be unclosed within quotation marks (e.g., “802.1Q tag 2”).

Defaults

- The default description for 802.1Q tagging on a port is **TAG PORT** *slot/port* **VLAN** *vid* (where the *slot/port* and *vid* are as entered when inputting the command) when you configure 802.1Q tagging on a single port, and **TAG AGGREGATE** *aggregate_id* **VLAN** *vid* (where the *slot/port* and *vid* are as entered when inputting the command) when you configure 802.1q tagging on an aggregate link.
- The *aggregate_id* value range for link aggregate ID numbers is 0–29 on the OmniSwitch 6600 Family- and 0–15 on the OmniSwitch 8800.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The VLAN specified for the port or aggregate link before 802.1Q tagging can be specified. See Chapter 21, “VLAN Management Commands” for information on how to create a VLAN.
- You *must* enable link aggregation before you can tag an aggregate of ports. See Chapter 13, “Link Aggregation Commands” for more information on link aggregation.
- The port’s default VLAN can never be configured to accepted tagged frames.
- Use the **no** form of the command to delete 802.1Q tagging on a port or an aggregate of ports.

Examples

```
-> vlan 2 802.1q 3/1
-> vlan 10 802.1q 100
-> vlan 5 802.1q 4/2 "802.1q tag 2"
-> vlan 6 no 802.1q 3/1
```

Release History

Release 5.1; command was introduced.

Related Commands

vlan 802.1q frame type	Configures a port to accept only VLAN-tagged frames or all frames.
vlan 802.1q force tag internal	Adds the default VLAN ID (VID) to tagged frames on 802.1Q-tagged ports.
show 802.1q	Displays 802.1Q tagging status and configuration.

MIB Objects

```
QPORTVLANTABLE
   qPortVlanSlot
   qPortVlanPort
   qPortVLanStatus
   qPortVlanTagValue
   qPortVlanDescription
   qAggregateVlanTagValue
   qAggregateVlanAggregateId
   qAggregateVlanStatus
   qAggregateVlanDescription
```

vlan 802.1q frame type

Configures a port to accept all frames or accept only VLAN-tagged frames.

vlan 802.1q *slot/port* **frame type {all | tagged}**

Syntax Definitions

slot	The slot number to configure 802.1Q tagging.
port	The port number to configure 802.1Q tagging.
all	Configures this port to accept all frames.
tagged	Configures this port to accept only VLAN-tagged frames.

Defaults

parameter	default
all | tagged	all

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

If you configure a port to accept only VLAN-tagged frames, then any frames received on this port that do not carry a VLAN ID (i.e., untagged frames or priority-tagged frames) will be discarded by the ingress rules for this port. Frames that are not discarded by this ingress rule are classified and processed according to the ingress rules for this port.

Examples

```
-> vlan 802.1q 3/1 frame type all
```

Release History

Release 5.1; command was introduced.

Related Commands

vlan 802.1q	Creates, modifies, or deletes 802.1Q tagging on a single port or an aggregate of ports.
vlan 802.1q force tag internal	Adds the default VLAN ID (VID) to tagged frames on 802.1Q-tagged ports.
show 802.1q	Displays 802.1Q tagging status and configuration.

MIB Objects

```
DOT1QPORTVLANTABLE
   dot1dBasePort
   dot1qPortAcceptableFrameTypes
```

vlan 802.1q force tag internal

Adds the default VLAN ID (VID) to tagged frames on 802.1Q-tagged ports.

vlan 802.1q *slot/port* **force tag internal {on | off}**

Syntax Definitions

slot	The slot number to configure 802.1Q tagging.
port	The port number to configure 802.1Q tagging.
on	Enables the addition of the of the default VID to tagged frames.
off	Disables the addition of the of the default VID to tagged frames.

Defaults

parameter	default
on | off	on

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- If a tagged packet comes on an untagged or group mobility port, then it can be classified in a VLAN other than the 802.1Q VLAN it currently belongs to. If the classified VLAN (i.e., different than the packet tag) is added to the packet on the egress side, then there are two possible options. One option is to carry the original tag of the packet and other option is to replace it with the classified VLAN as the tag. If force tag internal is **on**, then the tag is replaced with the classified VLAN. If the force tag internal is **off**, then the tag is not replaced with the classified VLAN as the tag.
- You *must* enable 802.1 tagging with the **vlan 802.1q** command before you can use the **force tag internal** command.

Examples

```
-> vlan 802.1q 3/1 force tag internal on
```

Release History

Release 5.1; command was introduced.

Related Commands

vlan 802.1q	Creates, modifies, or deletes 802.1Q tagging on a single port or an aggregate of ports.
vlan 802.1q frame type	Configures a port to accept only VLAN-tagged frames or all frames.
show 802.1q	Displays 802.1Q tagging status and configuration.

MIB Objects

QPORTVLANTABLE

```
qPortVlanSlot
qPortVlanPort
qPortVlanAction
qPortVlanForceTagInternal
qPortVlanTagValue
```

debug 802.1q

Retrieves debugging messages for the tagged port selected.

debug 802.1q {*slot/port* **|** *aggregate_id***}**

Syntax Definitions

slot	The slot number to configure 802.1Q tagging.
port	The port number to configure 802.1Q tagging.
aggregate_id	The aggregate link number to configure 802.1Q tagging.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Retrieves debugging messages for the tagged port selected.

Examples

```
-> debug 802.1q 5
Aggregate Status =         aggregate up

-> debug 802.1q 3/1
Slot Status =              slot up
Port Status =              port up

 GENERAL INFO ESM: USER PORT 1-12  = CORONADO PORT 0-11
 GENERAL INFO ESM: USER PORT 13-24  = CORONADO PORT 16-27
 GENERAL INFO GSM: USER PORT 1  = CORONADO PORT 12
 GENERAL INFO GSM: USER PORT 2  = CORONADO PORT 28
 HARDWARE INFO for slot = 3 and port = 1:
At reg_addr = 660012c, Ingress tag-untag:= 1:
At reg_addr = 6a00010, Eg tag-untag: = 1:
At reg_addr = 6601000,for protocol = 0,ing default vlan: = 1
At reg_addr = 6601080,for protocol = 1,ing default vlan: = 1
At reg_addr = 6601100,for protocol = 2,ing default vlan: = 1
At reg_addr = 6601180,for protocol = 3,ing default vlan: = 1
At reg_addr = 6601200,for protocol = 4,ing default vlan: = 1
At reg_addr = 6601280,for protocol = 5,ing default vlan: = 1
At reg_addr = 6601300,for protocol = 6,ing default vlan: = 1
At reg_addr = 6a70000, egress default vlan: = 1
At reg_addr = 6600118, protocol cam on/off: = 18 :
At reg_addr = 660011c, trusted/untrusted: = fff0fe6
At reg_addr = 6600130, secure/unsecure: = 18
At reg_addr = 6608020, for vlan = 8,spanning tree vector: = 1
At reg_addr = 6a00014, Eg force tag internal: = 0:
```

output definitions

Aggregate/Slot Status	Whether the slot or aggregate link is actively running.
Port Status	Whether the port is actively running.
General Info	Provides general information on the modules in the chassis, including module type, number of ports, and ASIC.
Hardware Info	Lists the various debug messages for the selected slot and port.

Release History

Release 5.1; command was introduced.

Related Commands

N/A

MIB Objects

N/A

show 802.1q

Displays 802.1Q tagging information for a single port or an aggregate of ports.

show 802.1q {*slot*/*port* | *aggregate_id***}**

Syntax Definitions

slot	The slot number to display 802.1Q tagging.
port	The port number to display 802.1Q tagging.
aggregate_id	The link aggregation ID to display 802.1Q tagging. See Chapter 13, "Link Aggregation Commands" for more information on link aggregation.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show 802.1q 3/4

   Acceptable Frame Type   :      Any Frame Type
   Force Tag Internal      :                 off

   Tagged VLANS      Internal Description
   ------------+-------------------------------------------------+
               2      TAG PORT 3/4 VLAN 2


   -> show 802.1q 2

   Tagged VLANS      Internal Description
   ------------+-------------------------------------------------+
               3      TAG AGGREGATE 2 VLAN 3
```

Output fields are described here:

output definitions

Acceptable Frame Type	The acceptable frame type for this port, which can be **Any Frame Type** or **Tagged Only Frame Type**.
Force Tag Internal	This field displays if adding the default VLAN ID (VID) to tagged frames is turned **on** or **off**.

output definitions (continued)

Tagged VLANS	The 802.1Q tag number for this port.
Internal Description	The description of this 802.1Q tag. You can modify this description with the **vlan 802.1q** command, which is described on page 15-2.

Release History

Release 5.1; command was introduced.

Related Commands

vlan 802.1q	Creates, modifies, or deletes 802.1Q tagging on a single port or an aggregate of ports.
vlan 802.1q frame type	Configures a port to accept only VLAN-tagged frames or all frames.
vlan 802.1q force tag internal	Adds the default VLAN ID (VID) to tagged frames on 802.1Q-tagged ports.

MIB Objects

```
QPORTVLANTABLE
   qPortVlanSlot
   qPortVlanPort
   qPortVLanStatus
   qPortVlanTagValue
   qPortVlanDescription
   qAggregateVlanTagValue
   qAggregateVlanAggregateId
   qAggregateVlanStatus
   qAggregateVlanDescription
```

16 Distributed Spanning Tree Commands

The Spanning Tree Algorithm and Protocol (STP) is a self-configuring algorithm that maintains a loop-free topology while providing data path redundancy and network scalability. Based on the IEEE 802.1D standard, the Alcatel STP implementation distributes the Spanning Tree load between the primary management module and the network interface modules. In the case of a stack of switches, the STP load is distributed between the primary management switch and other switches in the stack. This functionality improves network robustness by providing a Spanning Tree that continues to respond to BPDUs and port link up and down states in the event of a fail over to a backup management module or switch.

In addition to a distributed architecture, this implementation also provides the following Spanning Tree features:

- Automatic configuration of a physical topology into a single Spanning Tree to ensure that there is only one data path between any two switches.
- Fault tolerance within the network topology. The Spanning Tree is reconfigured in the event of a data path or bridge failure or when a new switch is added to the topology.
- Support for three Spanning Tree protocols: 802.1D (STP), 802.1W (RSTP), and 802.1S (MSTP).
- A *flat* Spanning Tree operating mode. If the 802.1D or 802.1w protocol is used, this mode applies a single STP instance across all VLANs. If the 802.1S protocol is used, this mode applies a single STP instance to each Multiple Spanning Tree Instance (MSTI), which identifies a set of VLANs.
- Support for up to 16 802.1S MSTIs per switch. In addition, there is always one Common and Internal Spanning Tree (CIST) instance 0 on each switch.
- A *1x1* Spanning Tree operating mode, which applies a single STP instance for each defined VLAN on the switch.
- An STP topology that includes 802.1Q tagged ports and link aggregate logical ports in the calculation of the physical topology.

MIB information for Distributed Spanning Tree commands is as follows:

Filename: AlcatelIND1VlanSTP.MIB
Module: STP-MGMT-MIB

A summary of the available commands is listed here:

Implicit bridge commands	**bridge mode** **bridge protocol** **bridge priority** **bridge hello time** **bridge max age** **bridge forward delay** **bridge bpdu-switching** **bridge path cost mode** **show spantree**
Explicit bridge commands	**bridge cist protocol** **bridge 1x1 protocol** **bridge cist priority** **bridge msti priority** **bridge 1x1 priority** **bridge cist hello time** **bridge 1x1 hello time** **bridge cist max age** **bridge 1x1 max age** **bridge cist forward delay** **bridge 1x1 forward delay** **show spantree cist** **show spantree msti** **show spantree 1x1**
Implicit port commands	**bridge slot/port** **bridge slot/port priority** **bridge slot/port path cost** **bridge slot/port mode** **bridge slot/port connection** **show spantree ports**
Explicit port commands	**bridge cist port** **bridge 1x1 port** **bridge cist slot/port priority** **bridge msti slot/port priority** **bridge 1x1 slot/port priority** **bridge cist slot/port path cost** **bridge msti slot/port path cost** **bridge 1x1 slot/port path cost** **bridge cist slot/port mode** **bridge 1x1 slot/port mode** **bridge cist slot/port connection** **bridge 1x1 slot/port connection** **show spantree cist ports** **show spantree msti ports** **show spantree 1x1 ports**
MST region commands	**bridge mst region name** **bridge mst region revision level** **bridge mst region max hops** **show spantree mst region**

MST instance commands	**bridge msti** **bridge msti vlan** **show spantree msti vlan-map** **show spantree cist vlan-map** **show spantree map-msti** **show spantree mst port**

bridge mode

Selects a flat Spanning Tree or 1x1 Spanning Tree operating mode for the switch. These modes are exclusive; however, it is not necessary to reboot the switch when changing modes.

bridge mode {**flat | 1x1**}

Syntax Definitions

flat	One Spanning Tree instance per switch.
1x1	One Spanning Tree instance for each VLAN configured on a switch.

Defaults

By default, the bridge mode for the switch is set to 1x1 Spanning Tree.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The Multiple Spanning Tree Protocol (MSTP), as defined in the IEEE 802.1S standard, is only supported on switches operating in the flat Spanning Tree mode.
- If the 802.1D or 802.1W protocol is used when the switch is running in the flat mode, a single STP instance is applied across all VLANs. For example, if a port belonging to VLAN 10 and a port belonging to VLAN 20 both connect to the same switch, then STP will block one of these ports.
- If the 802.1S protocol is used when the switch is running in the flat mode, a single STP instance is applied to each Multiple Spanning Tree Instance (MSTI). Each MSTI represents a set of VLANs.
- Flat Spanning Tree mode supports fixed (untagged) and 802.1Q tagged ports in each VLAN. However, Bridge Protocol Data Units (BPDUs) are always untagged.
- If **1x1** mode is selected, a single Spanning Tree instance is enabled for each VLAN configured on the switch. For example, if there are five VLANs configured on the switch, then there are five separate Spanning Tree instances. In essence, a VLAN is a virtual bridge in that it will have its own bridge ID and configurable STP parameters, such as protocol, priority, hello time, max age and forward delay.
- When operating in 1x1 mode, 802.1Q tagged ports participate in an 802.1Q Spanning Tree instance that allows the Spanning Tree to extend across tagged VLANs. As a result, a tagged port may participate in more than one Spanning Tree instance; one for each VLAN that the port carries.
- If a VLAN contains both fixed and tagged ports and the switch is operating in 1x1 Spanning Tree mode, then a hybrid of the two Spanning Tree instances (single and 802.1Q) is applied. If a VLAN appears as a tag on a port, then the BPDU for that VLAN are also tagged. However, if a VLAN appears as the configured default VLAN for the port, then BPDU are not tagged and the single Spanning Tree instance applies.
- Regardless of which mode the switch is running in, it is possible to administratively disable the Spanning Tree status for an individual VLAN (see Chapter 21, “VLAN Management Commands”). Note that active ports associated with such a VLAN are excluded from any Spanning Tree calculations and will remain in a forwarding state.

Examples

```
-> bridge mode flat
-> bridge mode 1x1
```

Release History

Release 5.1; command was introduced.

Related Commands

bridge protocol	Selects the Spanning Tree protocol for the specified instance.
bridge bpdu-switching	Enables the switching of Spanning Tree BPDU on a VLAN that has Spanning Tree disabled.
show spantree	Displays VLAN Spanning Tree parameter values.

MIB Objects

```
vStpTable
   vStpNumber
   vStpMode
```

bridge protocol

Configures the Spanning Tree protocol for the flat mode Common and Internal Spanning Tree (CIST) instance or for an individual VLAN instance if the switch is running in the 1x1 mode.

bridge [*instance***] protocol {stp | rstp | mstp}**

Syntax Definitions

instance	The flat mode CIST instance (1) or an existing 1x1 mode VLAN ID instance number (bridge 1–4094).
stp	IEEE 802.1D standard Spanning Tree Algorithm and Protocol.
rstp	IEEE 802.1W Rapid Spanning Tree Protocol.
mstp	IEEE 802.1S Multiple Spanning Tree Protocol.

Defaults

STP is the default protocol for all instances.

parameter	default
instance	flat mode instance

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Specifying an instance number with this command when the switch is running in the 1x1 Spanning Tree mode implies a VLAN ID and configures the protocol for the associated VLAN instance.
- To configure the protocol for the flat mode CIST instance when the switch is running in either the flat or 1x1 mode, do *not* specify an instance number. The CIST is the instance configured by default with this command.
- If the switch is running in the flat mode and STP (802.1D) or RSTP (802.1W) is the active protocol, entering 1 to specify the CIST instance is optional. If MSTP (802.1S) is the active protocol, however, entering 1 for the instance number is not accepted.
- Note that selecting MSTP (802.1S) is only an option for the flat mode CIST instance and is required to configure 802.1S Multiple Spanning Tree Instances (MSTI).
- MSTP is only active when the switch is operating in the flat Spanning Tree mode. STP and RSTP are active when the switch is operating in either the flat or 1x1 Spanning Tree mode.
- Deleting all existing MSTIs is required before changing the protocol from MSTP to STP or RSTP.
- Note that when changing the protocol to/from MSTP (802.1S), the bridge priority and port path cost values for the flat mode CIST instance are reset to their default values. However, if the path cost mode was set to 32-bit prior to the protocol change, the path cost is *not* reset to its default value. See the **bridge path cost mode** command page for more information.

Examples

```
-> bridge mode flat
-> bridge protocol mstp
-> bridge protocol rstp
-> bridge protocol stp

-> bridge mode 1x1
-> bridge 10 protocol rstp
-> bridge 200 protocol stp
-> bridge protocol mstp
-> bridge protocol rstp
-> bridge protocol stp
```

Release History

Release 5.1; command was introduced.
Release 5.1.6 and 5.3.1; **1d** and **1w** parameters replaced with **stp** and **rstp**, **mstp** parameter added.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge cist protocol	Explicit command for changing the Spanning Tree protocol for the flat mode instance.
bridge 1x1 protocol	Explicit command for changing the Spanning Tree protocol for a VLAN instance.

MIB Objects

```
vStpInsTable
   vStpInsNumber
   vStpInsMode
   vStpInsProtocolSpecification
```

bridge cist protocol

Configures the Spanning Tree protocol for the flat mode Common and Internal Spanning Tree (CIST) instance (bridge 1).

bridge cist protocol {stp | rstp | mstp}

Syntax Definitions

stp	IEEE 802.1D standard Spanning Tree Algorithm and Protocol.
rstp	IEEE 802.1w Rapid Spanning Tree Protocol.
mstp	IEEE 802.1S Multiple Spanning Tree Protocol.

Defaults

STP is the default protocol for the flat mode instance.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The **bridge cist protocol** command is an explicit Spanning Tree command that only applies to the flat mode CIST instance regardless of which operating mode (flat or 1x1) or protocol is active on the switch.
- Use this command to select STP (802.1D), RSTP (802.1W), or MSTP (802.1S) as the protocol for the flat mode CIST instance.
- Note that selecting MSTP (802.1S) is only an option for the flat mode CIST instance and is required to configure 802.1S Multiple Spanning Tree Instances (MSTI).
- MSTP is only active when the switch is operating in the flat Spanning Tree mode. STP and RSTP are active when the switch is operating in either the flat or 1x1 Spanning Tree mode.
- Note that when changing the protocol to/from MSTP (802.1S), the bridge priority and port path cost values for the flat mode CIST instance are reset to their default values. However, if the path cost mode was set to 32-bit prior to the protocol change, the path cost is *not* reset to its default value. See the **bridge path cost mode** command page for more information.
- If the switch is running in 1x1 mode when this command is used, the specified protocol is not active for the CIST instance until the operating mode for the switch is changed to the flat mode.
- Note that when a configuration snapshot is taken of the switch, all Spanning Tree commands are saved in their explicit format.

Examples

```
-> bridge cist protocol rstp
-> bridge cist protocol mstp
-> bridge cist protocol stp
```

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge protocol	Implicit command for changing the Spanning Tree protocol for the flat mode instance or for a 1x1 mode VLAN instance.
bridge 1x1 protocol	Explicit command for changing the Spanning Tree protocol for a VLAN instance.

MIB Objects

```
vStpInsTable
   vStpInsNumber
   vStpInsProtocolSpecification
```

bridge 1x1 protocol

Configures the Spanning Tree protocol for an individual VLAN instance.

bridge 1x1 *vid* **protocol {stp | rstp}**

Syntax Definitions

vid	An existing VLAN ID number (1–4094).
stp	IEEE 802.1D standard Spanning Tree Algorithm and Protocol.
rstp	IEEE 802.1w Rapid Spanning Tree Protocol.

Defaults

STP is the default protocol for a VLAN instance.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The **bridge 1x1 protocol** command is an explicit Spanning Tree command that only applies to the specified VLAN instance regardless of which operating mode (flat or 1x1) is active on the switch.
- If the switch is running in flat mode when this command is used, the specified protocol is not active for the specified VLAN instance until the operating mode for the switch is changed to 1x1.
- Note that when a configuration snapshot is taken of the switch, all Spanning Tree commands are saved in their explicit format.

Examples

```
-> bridge 1x1 2 protocol rstp
-> bridge 1x1 455 protocol stp
```

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge protocol	Implicit command for changing the Spanning Tree protocol for the flat mode instance or for a 1x1 mode VLAN instance.
bridge cist protocol	Explicit command for changing the Spanning Tree protocol for the flat mode instance.

MIB Objects

```
vStpInsTable
   vStpIns1x1VlanNumber
   vStpInsMode
   vStpInsProtocolSpecification
```

bridge mst region name

Defines the name for a Multiple Spanning Tree (MST) region. One of three attributes (name, revision level, and a VLAN to MST instance association table) that defines an MST region as required by the IEEE 802.1S standard. Switches that share the same attribute values are all considered part of the same MST region. Currently each switch can belong to one MST region at a time.

bridge mst region name *name*

bridge mst region no name

Syntax Definitions

name	An alphanumeric string up to 32 characters. Use quotes around string if the name contains multiple words with spaces between them (e.g. “Alcatel Marketing”).

Defaults

By default, the MST region name is left blank.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of this command to remove the MST region name. Note that it is not necessary to specify the region name to remove it.
- To change an existing region name, use this same command but specify a string value that is different than the existing name. It is *not* necessary to first remove the old name.
- Specifying an MST region name is allowed regardless of which Spanning Tree operating mode or protocol is currently active on the switch. However, MST configuration values, such as region name, only apply when the switch is operating in the flat Spanning Tree mode and using the 802.1S protocol.

Examples

```
-> bridge mst region name SalesRegion
-> bridge mst region name “Alcatel Marketing”
-> bridge mst region no name
```

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

bridge mst region revision level	Defines the revision level for an MST region.
bridge mst region max hops	Defines the maximum number of hops for the MST region.
bridge msti	Defines a MSTI number that identifies an association between a range of VLANs and a Spanning Tree instance.
bridge msti vlan	Defines an association between a range of VLANs and a single MSTI.

MIB Objects

```
vStpMstRegionTable
   vStpMstRegionNumber
   vStpMstRegionConfigName
```

bridge mst region revision level

Defines the revision level for a Multiple Spanning Tree (MST) region. One of three attributes (name, revision level, and a VLAN to MST instance association table) that defines an MST region as required by the IEEE 802.1S standard. Switches that share the same attribute values are all considered part of the same MST region. Currently each switch can belong to one MST region at a time.

bridge mst region revision level *rev_level*

Syntax Definitions

rev_level	A numeric value (0–65535) that identifies the MST region revision level for the switch.

Defaults

By default, the MST revision level is set to zero.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Specifying an MST region revision level is allowed regardless of which Spanning Tree operating mode or protocol is currently active on the switch. However, MST configuration values, such as revision level, only apply when the switch is operating in the flat Spanning Tree mode and using the 802.1S protocol.

Examples

```
-> bridge mst region revision level 1000
-> bridge mst region revision level 2000
```

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

bridge mst region name	Defines the name for an MST region.
bridge mst region max hops	Defines the maximum number of hops for the MST region.
bridge msti	Defines a MSTI number that identifies an association between a range of VLANs and a Spanning Tree instance.
bridge msti vlan	Defines an association between a range of VLANs and a single MSTI.

MIB Objects

```
vStpMstRegionTable
   vStpMstRegionNumber
   vStpMstRegionConfigRevisionLevel
```

bridge mst region max hops

Configures the maximum number of hops that are authorized to receive Multiple Spanning Tree (MST) regional information. Use this command to designate how many hops a BPDU is allowed to traverse before it is discarded and related information is aged.

bridge mst region max hops *max_hops*

Syntax Definitions

max_hops	A numeric value (1–40) that designates the maximum number of hops.

Defaults

By default, the maximum number of hops is set to 20.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The value configured with this command is a regional value that applies to all instances and in essence is used to determine the size of the region.
- The maximum hop count value is the initial value of the Remaining Hops parameter in the MST BPDU that originates from the bridge that is serving as the root bridge for the region. Each bridge that in turn receives the MST BPDU decrements the Remaining Hops count value by one and passes the new value along to the next bridge. When the count reaches 0, the BPDU is discarded.
- Specifying an MST maximum hop count is allowed regardless of which Spanning Tree operating mode or protocol is currently active on the switch. However, MST configuration values only apply when the switch is operating in the flat Spanning Tree mode and using the 802.1S protocol.

Examples

```
-> bridge mst region max hops 40
-> bridge mst region max hops 10
```

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

bridge mst region name	Defines the name for an MST region.
bridge mst region revision level	Defines the revision level for an MST region.
bridge msti	Defines a MSTI number that identifies an association between a range of VLANs and a Spanning Tree instance.
bridge msti vlan	Defines an association between a range of VLANs and a single MSTI.

MIB Objects

```
vStpMstRegionTable
   vStpMstRegionNumber
   vStpMstRegionMaxHops
```

bridge msti

Defines a Multiple Spanning Tree Instance (MSTI) number. This number identifies an association between a range of VLANs and a single Spanning Tree instance. In addition, it is possible to assign an optional name to the MSTI for further identification.

bridge msti *msti_id* **[name** *name***]**

bridge no msti *msti_id*

bridge msti *msti_id* **no name**

Syntax Definitions

msti_id	A numeric value (1–4094) that uniquely identifies an MSTI.
name	An alphanumeric string up to 32 characters. Use quotes around string if the name contains multiple words with spaces between them (e.g. “Alcatel Marketing”).

Defaults

By default, a flat mode Common and Internal Spanning Tree (CIST) instance always exists. The MSTI ID number for this instance is 0.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no msti** form of this command to remove the MSTI from the switch configuration.
- Use the **no name** form of this command to remove the optional MSTI name from the specified instance. The instance itself is not removed; only the name.
- Up to 16 MSTIs are allowed per switch; select a number from 1 to 4094 for the MSTI number. In addition, there is always one Common and Internal Spanning Tree (CIST) instance 0 per switch. Initially all VLANs are associated with the CIST instance.
- Creating an MSTI is allowed when the switch is operating in either the 1x1 or flat Spanning Tree mode, as long as MSTP (802.1S) is the selected flat mode protocol. The MSTI configuration, however, is not active unless the switch is running in the flat mode.

Examples

```
-> bridge msti 10
-> bridge msti 20 name BldgOneST10
-> bridge msti 20 no name
-> bridge no msti 10
```

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

bridge mst region name	Defines the name for an MST region.
bridge mst region revision level	Defines the revision level for an MST region.
bridge mst region max hops	Defines the maximum number of hops for the MST region.
bridge msti vlan	Defines an association between a range of VLANs and a single MSTI.

MIB Objects

```
vStpMstInstanceTable
   vStpMstInstanceNumber
   vStpMstInstanceName
   vStpMstInstanceVlanBitmapAddition
   vStpMstInstanceVlanBitmapDeletion
   vStpMstInstanceVlanBitmapState
```

bridge msti vlan

Defines an association between a range of VLANs and a single Multiple Spanning Tree Instance (MSTI). The MSTI-to-VLAN mapping created with this command is one of three attributes (name, revision level, and a VLAN to MST instance association table) that defines an MST region as required by the IEEE 802.1S standard. Switches that share the same attribute values are all considered part of the same MST region. Currently each switch can belong to one MST region at a time.

bridge msti *msti_id* **vlan** *vid_range*

bridge msti *msti_id* **no vlan** *vid_range*

Syntax Definitions

msti_id	An existing MSTI ID number (0–4094).
vid_range	A VLAN ID number (1–4094) To associate multiple VLANS in a single command, use a hyphen to specify a range of VLAN IDs and a space to separate multiple VLAN IDs and/or ranges (e.g. 100-115 122 135 200-210).

Defaults

By default, all VLANs are associated with the flat mode Common and Internal Spanning Tree (CIST) instance, which is also known as MSTI 0.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of this command to remove a VLAN or a range of VLANs from the specified MSTI association.
- Note that the VLAN ID specified with this command does not have to already exist in the switch configuration. This command maps VLAN IDs to MSTIs, but does not create VLANs.
- A VLAN is associated with only one MSTI at a time, but it is possible to move a VLAN from one MSTI to another. In addition, it is also possible to assign only one VLAN to an MSTI; a range of VLANs is not required.
- Configuring an MSTI-to-VLAN mapping is allowed when the switch is operating in either the 1x1 or flat Spanning Tree mode, as long as MSTP (802.1S) is the selected flat mode protocol. The MSTI configuration, however, is not active unless the switch is running in the flat mode.

Examples

```
-> bridge msti 10 vlan 100-115
-> bridge msti 20 vlan 122 135 200-210
-> bridge msti 10 no vlan 112 200-204
```

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

bridge mst region name	Defines the name for an MST region.
bridge mst region revision level	Defines the revision level for an MST region.
bridge mst region max hops	Defines the maximum number of hops for the MST region.
bridge msti	Defines a MSTI number that identifies an association between a range of VLANs and a Spanning Tree instance.

MIB Objects

```
vStpMstVlanAssignmentTable
   vStpMstVlanAssignmentVlanNumber
   vStpMstVlanAssignmentMstiNumber
```

bridge priority

Configures the bridge priority value for the flat mode Common and Internal Spanning Tree (CIST) instance or for a 1x1 mode VLAN instance. Bridge priority is used to determine which bridge the Spanning Tree algorithm designates as the root bridge.

bridge [*instance***] priority** *priority*

Syntax Definitions

instance	The flat mode CIST instance or an existing VLAN ID number (1–4094).
priority	A bridge priority value within the range of 0–65535. Do not use commas in the value. If MSTP is the active protocol on the switch, then a bridge priority value that is a multiple of 4096 is required.

Defaults

By default, the bridge priority value is set to 32768.

parameter	default
instance	flat mode instance

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The bridge priority specifies the priority value for the first two octets of the Bridge ID (eight octets long). The remaining six octets of the Bridge ID contain a dedicated bridge MAC address.
- The lower the bridge priority number, the higher the priority that is associated with the bridge.
- Specifying an instance number with this command when the switch is running in the 1x1 Spanning Tree mode implies a VLAN ID and configures the priority value for the associated VLAN instance.
- To configure the priority value for the flat mode CIST instance when the switch is running in either the flat or 1x1 mode, do *not* specify an instance number. The CIST is the instance configured by default with this command.
- If the switch is running in the flat mode and STP (802.1D) or RSTP (802.1W) is the active protocol, entering 1 to specify the CIST instance is optional. If MSTP (802.1S) is the active protocol, however, entering 1 for the instance number is not accepted. In this case, use the **bridge cist priority** or **bridge msti priority** commands instead.
- Note that when the protocol is changed to/from MSTP (802.1S), the bridge priority for the flat mode CIST instance is reset to the default value.

Examples

```
-> bridge mode flat
-> bridge priority 8192
-> bridge priority 2500
ERROR: Valid bridge priority values are multiples of 4096: 0, 4096,
         8192, 12288, 16384 ... 61440

-> bridge mode 1x1
-> bridge 255 priority 16384
-> bridge 355 priority 3500
-> bridge priority 8192
```

Release History

Release 5.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge cist priority	Explicit command for changing the Spanning Tree priority for the CIST instance when the switch is operating in either the flat or 1x1 mode.
bridge msti priority	Explicit command for changing the Spanning Tree priority for an 802.1S MSTI when the switch is operating in either the flat or 1x1 mode.
bridge 1x1 protocol	Explicit command for changing the Spanning Tree priority for a VLAN instance when the switch is operating in either the flat or 1x1 mode.

MIB Objects

```
vStpInsTable
   vStpInsNumber
   vStpInsMode
   vStpInsPriority
   vStpInsBridgeAddress
```

bridge cist priority

Configures the Spanning Tree priority value for the flat mode Common and Internal Spanning Tree (CIST) instance. Bridge priority is used to determine which bridge the Spanning Tree algorithm designates as the root bridge.

bridge cist priority *priority*

Syntax Definitions

priority	A bridge priority value within the range of 0–65535. Do not use commas in the value. If MSTP (802.1S) is the active protocol on the switch, then a bridge priority value that is a multiple of 4096 is required.

Defaults

By default, the bridge priority value is set to 32768.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The bridge priority specifies the priority value for the first two octets of the Bridge ID (eight octets long). The remaining six octets of the Bridge ID contain a dedicated bridge MAC address.
- The lower the bridge priority number, the higher the priority that is associated with the bridge.
- This command is an explicit Spanning Tree command that only applies to the CIST instance regardless of which operating mode (flat or 1x1) or protocol is active on the switch.
- If the switch is running in 1x1 mode when this command is used, the specified priority value is not active for the CIST instance until the operating mode for the switch is changed to the flat mode.
- Note that when the protocol is changed to/from MSTP (802.1S), the bridge priority for the flat mode CIST instance is reset to the default value.
- In regards to the priority for a Multiple Spanning Tree Instance (MSTI), only the four most significant bits are used.
- Note that when a configuration snapshot is taken of the switch, all Spanning Tree commands are saved in their explicit format.

Examples

```
-> bridge mode flat
-> bridge cist priority 16384
-> bridge cist priority 53800
ERROR: Valid bridge priority values are multiples of 4096: 0, 4096,
         8192, 12288, 16384 ... 61440

-> bridge mode 1x1
-> bridge cist priority 16384
-> bridge cist priority 12288
```

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge priority	Implicit command for changing the Spanning Tree priority for the flat mode CIST instance or a 1x1 mode VLAN instance.
bridge msti priority	Explicit command for changing the Spanning Tree priority for an 802.1S MSTI when the switch is operating in either the flat or 1x1 mode.
bridge 1x1 protocol	Explicit command for changing the Spanning Tree priority for a VLAN instance when the switch is operating in either the flat or 1x1 mode.

MIB Objects

```
vStpInsTable
   vStpInsNumber
   vStpInsPriority
   vStpInsBridgeAddress
```

bridge msti priority

Configures the bridge priority value for an 802.1s Multiple Spanning Tree Instance (MSTI). Bridge priority is used to determine which bridge the Spanning Tree algorithm designates as the root bridge.

bridge mist *msti_id* **priority** *priority*

Syntax Definitions

msti_id	An existing MSTI ID number (0–4094).
priority	A bridge priority value that is a multiple of 4096 and within the range of 0–65535. Do not use commas in the value.

Defaults

By default, the bridge priority value is set to 32768.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The bridge priority specifies the priority value for the first two octets of the Bridge ID (eight octets long). The remaining six octets of the Bridge ID contain a dedicated bridge MAC address.
- The bridge priority value for an MSTI is calculated by adding the configured priority value to the Spanning Tree instance number. For example, if the priority value of MSTI 10 equals 32768 (the default), then the Spanning Tree priority value advertised for this instance is 32770 (32768 + 10).
- The lower the bridge priority number, the higher the priority that is associated with the bridge.
- This command is an explicit Spanning Tree command that only applies to the specified 802.1S MSTI regardless of which operating mode (flat or 1x1) is active on the switch. If MSTP (802.1S) is not the selected flat mode protocol, however, the priority value for any MSTI is not configurable in either mode.
- Note that if zero is entered for the *msti_id* value, the specified priority value is applied to the CIST instance. The flat mode CIST instance 0 is also known as MSTI 0.
- If the switch is running in 1x1 mode when this command is used, the specified priority value is not active for the specified MSTI until the operating mode for the switch is changed to the flat mode.
- Note that when the protocol is changed to/from MSTP (802.1S), the bridge priority for the flat mode CIST instance is reset to the default value.
- In regards to the priority for an MSTI, only the four most significant bits are used.

Examples

```
-> bridge mode flat
-> bridge msti 2 priority 4096
-> bridge msti 10 priority 53800
ERROR: Valid bridge priority values are multiples of 4096: 0, 4096,
         8192, 12288, 16384 ... 61440

-> bridge mode 1x1
-> bridge msti 2 priority 61440
-> bridge msti 10 priority 12288
```

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

bridge mode	Selects a flat Spanning Tree or 1x1 (per VLAN) Spanning Tree operating mode for the switch.
bridge priority	Implicit command for changing the Spanning Tree priority for the flat mode CIST instance or a 1x1 mode VLAN instance.
bridge cist priority	Explicit command for changing the Spanning Tree priority for the CIST instance when the switch is operating in either the flat or 1x1 mode.
bridge 1x1 priority	Explicit command for changing the Spanning Tree priority for a VLAN instance when the switch is operating in either the flat or 1x1 mode.

MIB Objects

```
vStpInsTable
   vStpInsMstiNumber
   vStpInsMode
   vStpInsPriority
   vStpInsBridgeAddress
```

bridge 1x1 priority

Configures the bridge priority value for an individual VLAN instance.

bridge 1x1 *vid* **priority** *priority*

Syntax Definitions

vid	An existing VLAN ID number (1–4094).
priority	A bridge priority value within the range of 0–65535. Do not use commas in the value.

Defaults

By default, the bridge priority value is set to 32768.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The bridge priority specifies the priority value for the first two octets of the Bridge ID (eight octets long). The remaining six octets of the Bridge ID contain a dedicated bridge MAC address.
- The lower the bridge priority number, the higher the priority that is associated with the bridge.
- This command is an explicit Spanning Tree command that only applies to the specified VLAN instance regardless of which operating mode (flat or 1x1) or protocol is active on the switch.
- If the switch is running in the flat mode when this command is used, the specified priority value is not active for the specified VLAN instance until the operating mode for the switch is changed to the 1x1 mode.
- Note that when a configuration snapshot is taken of the switch, all Spanning Tree commands are saved in their explicit format.

Examples

```
-> bridge mode flat
-> bridge 1x1 2 priority 16384
-> bridge 1x1 10 priority 53800

-> bridge mode 1x1
-> bridge 1x1 2 priority 16384
-> bridge 1x1 10 priority 53800
```

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

bridge mode	Selects a flat Spanning Tree or 1x1 (per VLAN) Spanning Tree operating mode for the switch.
bridge priority	Implicit command for changing the Spanning Tree priority for the flat mode CIST instance or a 1x1 mode VLAN instance.
bridge cist priority	Explicit command for changing the Spanning Tree priority for the CIST instance when the switch is operating in either the flat or 1x1 mode.
bridge msti priority	Explicit command for changing the Spanning Tree priority for an 802.1S MSTI when the switch is operating in either the flat or 1x1 mode.

MIB Objects

```
vStpInsTable
   vStpIns1x1VlanNumber
   vStpInsMode
   vStpInsPriority
   vStpInsBridgeAddress
```

bridge hello time

Configures the Spanning Tree hello time value for the flat mode Common and Internal Spanning Tree (CIST) instance or for a 1x1 mode VLAN instance. This value specifies the amount of time, in seconds, between each transmission of a BPDU on any port that is the Spanning Tree root or is attempting to become the Spanning Tree root.

bridge [*instance***] hello time** *seconds*

Syntax Definitions

instance	The flat mode CIST instance or an existing VLAN ID number (1–4094).
seconds	Hello Time value, in seconds (1–10).

Defaults

By default, the bridge hello time value for is set to 2 seconds.

parameter	default
instance	flat mode instance

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Lowering the Hello Time interval improves the robustness of the Spanning Tree Algorithm. Increasing the Hello Time interval lowers the overhead of the Spanning Tree Algorithm.
- Specifying an instance number with this command when the switch is running in the 1x1 Spanning Tree mode implies a VLAN ID and configures the hello time value for the associated VLAN instance.
- To configure the hello time value for the flat mode CIST instance when the switch is running in either the flat or 1x1 mode, do *not* specify an instance number. The CIST is the instance configured by default with this command.
- If the switch is running in the flat mode and STP (802.1D) or RSTP (802.1W) is the active protocol, entering 1 to specify the CIST instance is optional. If MSTP (802.1S) is the active protocol, however, entering 1 for the instance number is not accepted.
- Note that for 802.1S Multiple Spanning Tree Instances (MSTI), the hello time value is inherited from the CIST instance and is not a configurable parameter.

Examples

```
-> bridge mode flat
-> bridge hello time 5

-> bridge mode 1x1
-> bridge 10 hello time 8
-> bridge hello time 5
```

Release History

Release 5.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge cist hello time	Explicit command for changing the Spanning Tree hello time value for the CIST instance when the switch is operating in either the flat or 1x1 mode.
bridge 1x1 hello time	Explicit command for changing the Spanning Tree hello time value for a VLAN instance when the switch is operating in either the flat or 1x1 mode.

MIB Objects

```
vStpInsTable
   vStpInsNumber
   vStpInsMode
   vStpInsBridgeHelloTime
```

bridge cist hello time

Configures the bridge hello time value for the flat mode Common and Internal Spanning Tree (CIST) instance. This value is the amount of time, in seconds, between each transmission of a BPDU on any port that is the Spanning Tree root or is attempting to become the Spanning Tree root.

bridge cist hello time *seconds*

Syntax Definitions

seconds	Hello time value in seconds (1–10).

Defaults

By default, the bridge hello time value is set to 2 seconds.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Lowering the Hello Time interval improves the robustness of the Spanning Tree Algorithm. Increasing the Hello Time interval lowers the overhead of the Spanning Tree Algorithm.
- This command is an explicit Spanning Tree command that only applies to the CIST instance regardless of which operating mode (flat or 1x1) or protocol is active on the switch.
- If the switch is running in 1x1 mode when this command is used, the specified hello time value is not active for the CIST instance until the operating mode for the switch is changed to the flat mode.
- Note that when a configuration snapshot is taken of the switch, all Spanning Tree commands are saved in their explicit format.

Examples

```
-> bridge mode flat
-> bridge cist hello time 5
-> bridge cist hello time 10

-> bridge mode 1x1
-> bridge cist hello time 5
-> bridge cist hello time 10
```

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge hello time	Implicit command for changing the Spanning Tree hello time value for the flat mode CIST instance or for a 1x1 mode VLAN instance.
bridge 1x1 hello time	Explicit command for changing the Spanning Tree hello time value for a VLAN instance when the switch is operating in either the flat or 1x1 mode.

MIB Objects

```
vStpInsTable
   vStpInsNumber
   vStpInsBridgeHelloTime
```

bridge 1x1 hello time

Configures the bridge hello time value for an individual VLAN instance. This value is the amount of time, in seconds, between each transmission of a BPDU on any port that is the Spanning Tree root or is attempting to become the Spanning Tree root.

bridge 1x1 *vid* **hello time** *seconds*

Syntax Definitions

vid	An existing VLAN ID number (1–4094).
seconds	Hello time value in seconds (1–10).

Defaults

By default, the bridge Hello Time value is set to 2 seconds.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Lowering the Hello Time interval improves the robustness of the Spanning Tree Algorithm. Increasing the Hello Time interval lowers the overhead of the Spanning Tree Algorithm.
- This command is an explicit Spanning Tree command that only applies to the specified VLAN instance regardless of which operating mode (flat or 1x1) is active on the switch.
- If the switch is running in the flat mode when this command is used, the specified hello time value is not active for the specified VLAN instance until the operating mode for the switch is changed to the 1x1 mode.
- Note that when a configuration snapshot is taken of the switch, all Spanning Tree commands are saved in their explicit format.

Examples

```
-> bridge mode flat
-> bridge 1x1 2 hello time 5
-> bridge 1x1 10 hello time 10

-> bridge mode 1x1
-> bridge 1x1 255 hello time 5
-> bridge 1x1 455 hello time 10
```

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge hello time	Implicit command for changing the Spanning Tree hello time value for the flat mode CIST instance or for a 1x1 mode VLAN instance.
bridge cist hello time	Explicit command for changing the Spanning Tree hello time value for the CIST instance when the switch is operating in either the flat or 1x1 mode.

MIB Objects

```
vStpInsTable
   vStpIns1x1VlanNumber
   vStpInsMode
   vStpInsBridgeHelloTime
```

bridge max age

Configures the Spanning Tree bridge max age time for the flat mode Common and Internal Spanning Tree (CIST) instance or for a 1x1 mode VLAN instance. This value is the amount of time, in seconds, that Spanning Tree information learned from the network on any port is retained. When this information has aged beyond the max age value, the information is discarded.

bridge [*instance***] max age** *seconds*

Syntax Definitions

instance	The flat mode CIST instance or an existing VLAN ID number (1–4094).
seconds	Max age time in seconds (6–40).

Defaults

By default, the bridge max age time value is set to 20 seconds.

parameter	default
instance	flat mode instance

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- A low max age time causes the Spanning Tree Algorithm to reconfigure more often.
- Specifying an instance number with this command when the switch is running in the 1x1 Spanning Tree mode implies a VLAN ID and configures the max age value for the associated VLAN instance.
- To configure the max age value for the flat mode CIST instance when the switch is running in either the flat or 1x1 mode, do *not* specify an instance number. The CIST is the instance configured by default with this command.
- If the switch is running in the flat mode and STP (802.1D) or RSTP (802.1W) is the active protocol, entering 1 to specify the CIST instance is optional. If MSTP (802.1S) is the active protocol, however, entering 1 for the instance number is not accepted.
- Note that for 802.1S Multiple Spanning Tree Instances (MSTI), the max age value is inherited from the CIST instance and is not a configurable parameter.

Examples

```
-> bridge mode flat
-> bridge max age 40

-> bridge mode 1x1
-> bridge 255 max age 40
-> bridge max age 10
```

Release History

Release 5.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge cist max age	Explicit command for changing the Spanning Tree max age time value for the CIST instance when the switch is operating in either the flat or 1x1 mode.
bridge 1x1 max age	Explicit command for changing the Spanning Tree max age time value for a VLAN instance when the switch is operating in either the flat or 1x1 mode.

MIB Objects

```
vStpInsTable
   vStpInsNumber
   vStpInsMode
   vStpInsBridgeMaxAge
```

bridge cist max age

Configures the bridge max age time value for the flat mode Common and Internal Spanning Tree (CIST) instance. This value is the amount of time, in seconds, that Spanning Tree Protocol information learned from the network on any port is retained. When this information has aged beyond the max age value, the information is discarded.

bridge cist max age *seconds*

Syntax Definitions

seconds	Max age time in seconds (6–40).

Defaults

By default, the bridge max age time value is set to 20 seconds.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- A low max age time causes the Spanning Tree Algorithm to reconfigure more often.
- This command is an explicit Spanning Tree command that only applies to the CIST instance regardless of which operating mode (flat or 1x1) or protocol is active on the switch.
- If the switch is running in 1x1 mode when this command is used, the specified max age time value is not active for the CIST instance until the operating mode for the switch is changed to the flat mode.
- Note that when a configuration snapshot is taken of the switch, all Spanning Tree commands are saved in their explicit format.

Examples

```
-> bridge mode flat
-> bridge cist max age 10
-> bridge cist max age 30

-> bridge mode 1x1
-> bridge cist max age 10
-> bridge cist max age 30
```

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge max age	Implicit command for changing the Spanning Tree max age time value for the flat mode CIST instance or for a 1x1 mode VLAN instance.
bridge 1x1 max age	Explicit command for changing the Spanning Tree max age time value for a VLAN instance when the switch is operating in either the flat or 1x1 mode.

MIB Objects

```
vStpInsTable
   vStpInsNumber
   vStpInsBridgeMaxAge
```

bridge 1x1 max age

Configures the bridge max age time value for an individual VLAN instance. This value is the amount of time, in seconds, that Spanning Tree Protocol information learned from the network on any port is retained. When this information has aged beyond the max age value, the information is discarded.

bridge 1x1 *vid* **max age** *seconds*

Syntax Definitions

vid	An existing VLAN ID number (1–4094).
seconds	Max age time in seconds (6–40).

Defaults

By default, the bridge max age time value is set to 20 seconds.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- A low max age time causes the Spanning Tree Algorithm to reconfigure more often.
- This command is an explicit Spanning Tree command that only applies to the specified VLAN instance regardless of which operating mode (flat or 1x1) is active on the switch.
- If the switch is running in the flat mode when this command is used, the specified max age time value is not active for the specified VLAN instance until the operating mode for the switch is changed to the 1x1 mode.
- Note that when a configuration snapshot is taken of the switch, all Spanning Tree commands are saved in their explicit format.

Examples

```
-> bridge mode flat
-> bridge 1x1 2 max age 10
-> bridge 1x1 10 max age 40

-> bridge mode 1x1
-> bridge 1x1 255 max age 30
-> bridge 1x1 455 max age 10
```

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge max age	Implicit command for changing the Spanning Tree max age time value for the flat mode CIST instance or for a 1x1 mode VLAN instance.
bridge cist max age	Explicit command for changing the Spanning Tree max age time value for the CIST instance when the switch is operating in either the flat or 1x1 mode.

MIB Objects

```
vStpInsTable
   vStpIns1x1VlanNumber
   vStpInsMode
   vStpInsBridgeMaxAge
```

bridge forward delay

Configures the bridge forward delay time for the flat mode Common and Internal Spanning Tree (CIST) instance or for 1x1 mode VLAN instance. This value is the amount of time, in seconds, that determines how fast a port changes its Spanning Tree state until it reaches a forwarding state. The forward delay time specifies how long a port stays in the listening and learning states, which precede the forwarding state.

bridge [*instance***] forward delay** *seconds*

Syntax Definitions

instance	The flat mode CIST instance or an existing VLAN ID number (1–4094).
seconds	Forward delay time, in seconds (4–30).

Defaults

By default, the bridge forward delay time value is set to 15 seconds.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- A low forward delay time can cause temporary loops in the network, because data may get forwarded before the reconfiguration message has reached all nodes on the network.
- The forward delay time is also used to age out all dynamic MAC address entries in the forwarding table (MAC address table) when a topology change occurs.
- Specifying an instance number with this command when the switch is running in the 1x1 Spanning Tree mode implies a VLAN ID and configures the forward delay time for the associated VLAN instance.
- To configure the forward delay time for the flat mode CIST instance when the switch is running in either the flat or 1x1 mode, do *not* specify an instance number. The CIST is the instance configured by default with this command.
- If the switch is running in the flat mode and STP (802.1D) or RSTP (802.1W) is the active protocol, entering 1 to specify the CIST instance is optional. If MSTP (802.1S) is the active protocol, however, entering 1 for the instance number is not accepted.
- Note that for 802.1S Multiple Spanning Tree Instances (MSTI), the forward delay time is inherited from the CIST instance and is not a configurable parameter.

Examples

```
-> bridge mode flat
-> bridge forward delay 30

-> bridge mode 1x1
-> bridge 255 forward delay 10
-> bridge forward delay 30
```

Release History

Release 5.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge cist forward delay	Explicit command for changing the Spanning Tree forward delay time value for the CIST instance when the switch is operating in either the flat or 1x1 mode.
bridge 1x1 forward delay	Explicit command for changing the Spanning Tree forward delay time value for a VLAN instance when the switch is operating in either the flat or 1x1 mode.
show spantree	Displays VLAN Spanning Tree parameter values.

MIB Objects

```
vStpInsTable
   vStpInsNumber
   vStpInsMode
   vStpInsBridgeForwardDelay
```

bridge cist forward delay

Configures the bridge forward delay time value for the flat mode Common and Internal Spanning Tree (CIST) instance. This value is the amount of time, in seconds, that determines how fast a port changes its Spanning Tree state until it reaches a forwarding state. The forward delay time specifies how long a port stays in the listening and learning states, which precede the forwarding state.

bridge cist forward delay *seconds*

Syntax Definitions

seconds	Forward delay time in seconds (4–30).

Defaults

By default, the bridge forward delay time value is set to 15 seconds.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- A low forward delay time can cause temporary loops in the network, because data may get forwarded before the reconfiguration message has reached all nodes on the network.
- The forward delay time is also used to age out all dynamic MAC address entries in the forwarding table (MAC address table) when a topology change occurs.
- This command is an explicit Spanning Tree command that only applies to the flat mode CIST instance regardless of which operating mode (flat or 1x1) or protocol is active on the switch.
- If the switch is running in 1x1 mode when this command is used, the specified forward delay time value is not active for the CIST instance until the operating mode for the switch is changed to the flat mode.
- Note that when a configuration snapshot is taken of the switch, all Spanning Tree commands are saved in their explicit format.

Examples

```
-> bridge mode flat
-> bridge cist forward delay 10
-> bridge cist forward delay 30

-> bridge mode 1x1
-> bridge cist forward delay 25
-> bridge cist forward delay 4
```

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge forward delay	Implicit command for changing the Spanning Tree forward delay time value for the flat mode CIST instance or for a 1x1 mode VLAN instance.
bridge 1x1 forward delay	Explicit command for changing the Spanning Tree forward delay time value for a VLAN instance when the switch is operating in either the flat or 1x1 mode.

MIB Objects

```
vStpInsTable
   vStpInsNumber
   vStpInsBridgeForwardDelay
```

bridge 1x1 forward delay

Configures the bridge forward delay time value for an individual VLAN instance. This value is the amount of time, in seconds, that determines how fast a port changes its Spanning Tree state until it reaches a forwarding state. The forward delay time specifies how long a port stays in the listening and learning states, which precede the forwarding state.

bridge 1x1 *vid* **forward delay** *seconds*

Syntax Definitions

vid	An existing VLAN ID number (1–4094).
seconds	Forward delay time in seconds (4–30).

Defaults

By default, the bridge forward delay time value is set to 15 seconds.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- A low forward delay time can cause temporary loops in the network, because data may get forwarded before the reconfiguration message has reached all nodes on the network.
- The forward delay time is also used to age out all dynamic MAC address entries in the forwarding table (MAC address table) when a topology change occurs.
- This command is an explicit Spanning Tree command that only applies to the specified VLAN instance regardless of which operating mode (flat or 1x1) is active on the switch.
- If the switch is running in the flat mode when this command is used, the specified max age time value is not active for the specified VLAN instance until the operating mode for the switch is changed to the 1x1 mode.
- Note that when a configuration snapshot is taken of the switch, all Spanning Tree commands are saved in their explicit format.

Examples

```
-> bridge mode flat
-> bridge 1x1 2 forward delay 30
-> bridge 1x1 10 forward delay 4

-> bridge mode 1x1
-> bridge 1x1 255 forward delay 25
-> bridge 1x1 455 forward delay 10
```

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge forward delay	Implicit command for changing the Spanning Tree forward delay time value for the flat mode CIST instance or for a 1x1 mode VLAN instance.
bridge cist forward delay	Explicit command for changing the Spanning Tree forward delay time value for the CIST instance when the switch is operating in either the flat or 1x1 mode.

MIB Objects

```
vStpInsTable
   vStpIns1x1VlanNumber
   vStpInsMode
   vStpInsBridgeForwardDelay
```

bridge bpdu-switching

Enables the switching of Spanning Tree BPDU on the flat mode Common and Internal Spanning Tree (CIST) instance or for an individual VLAN instance if the switch is running in the 1x1 mode.

bridge *instance* **bpdu-switching {enable | disable}**

Syntax Definitions

instance	The flat mode CIST instance (bridge 1) or an existing 1x1 mode VLAN ID instance number (bridge 1–4094).
enable	Enables BPDU switching for the specified instance.
disable	Disables BPDU switching for the specified instance.

Defaults

By default, BPDU switching is disabled for an instance.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Specifying the BPDU switching status for a VLAN does not depend on the current VLAN Spanning Tree status. For example, setting the BPDU switching status to enabled is allowed on a VLAN that also has Spanning Tree enabled.
- The **bridge bpdu-switching** command is an implicit Spanning Tree command. When issued in the 1x1 mode, the *instance* number specified implies a VLAN ID. When issued in the flat mode, the *instance* number specified implies an MSTI number.
- Note that if the switch is running in the flat mode, specifying a value greater than 1 for the *instance* will return an error message. BPDU switching is only configured for the flat mode instance (bridge 1), regardless of which protocol is active (STP, RSTP, or MSTP).

Examples

```
-> bridge mode flat
-> bridge bpdu-switching enable
-> bridge 1 bpdu-switching disable

-> bridge mode 1x1
-> bridge 100 bpdu-switching enable
-> bridge 100 bpdu-switching disable
-> bridge bpdu-switching enable
-> bridge bpdu-switching disable
```

Release History

Release 5.1; command was introduced.

Related Commands

vlan stp	Enables or disables Spanning Tree instance for the specified VLAN.
show spantree	Displays Spanning Tree parameter values.

MIB Objects

```
vStpInsTable
   vStpInsBpduSwitching
```

bridge path cost mode

Configures the automatic selection of a 16-bit path cost for STP/RSTP ports and a 32-bit path cost for MSTP ports or sets all path costs to use a 32-bit value.

bridge path cost mode {auto | 32bit}

Syntax Definitions

auto	The port path cost value is automatically set depending on which protocol is active on the switch (32-bit for MSTP, 16-bit for STP/RSTP).
32bit	Specifies that a 32-bit value is used for the port path cost value regardless of which protocol is active on the switch.

Defaults

By default, the path cost mode is set to **auto**.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Note that all path cost values, except those for MSTIs, are reset to the default path cost value when this mode is changed.
- When connecting a switch running in the 32-bit path cost mode to a switch running in the 16-bit mode, the 32-bit switch will have a higher path cost value and thus an inferior path cost to the 16-bit switch. To avoid this, use the **bridge path cost mode** command to change the 32-bit switch to a 16-bit switch.
- Note that when the protocol is changed to/from MSTP (802.1S), the bridge priority and port path cost values for the flat mode CIST instance are reset to their default values. The exception to this is if the path cost mode is set to 32-bit prior to the protocol change, the path cost is not reset to its default value

Examples

```
-> bridge path cost mode 32bit
-> bridge path cost mode auto
```

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

bridge slot/port path cost	Defines a Spanning Tree path cost for a port.
bridge protocol	Configures the protocol for the flat mode CIST instance or a 1x1 mode VLAN instance.

MIB Objects

```
vStpBridge
   vStpPathCostMode
```

bridge slot/port

Enables or disables the Spanning Tree status on a single port or an aggregate of ports for the specified flat mode Common and Internal Spanning Tree (CIST) instance or a 1x1 mode VLAN instance.

bridge *instance* **{***slot/port* **|** *logical_port***} {enable | disable}**

Syntax Definitions

instance	The CIST instance number or an existing VLAN ID number (1–4094).
slot/port	The slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
logical_port	The Link aggregate ID number (0–31).
enable	Enables Spanning Tree on the specified port for the specified instance.
disable	Disables Spanning Tree on the specified port for the specified instance.

Defaults

By default, the Spanning Tree status is enabled on eligible ports.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Specifying an instance number with this command when the switch is running in the 1x1 Spanning Tree mode implies a VLAN ID and configures the port Spanning Tree status for the associated VLAN instance.
- If the switch is running in the flat mode and STP (802.1D) or RSTP (802.1W) is the active protocol, enter 1 to specify the CIST instance. If MSTP (802.1S) is the active protocol, however, entering 1 for the instance number is not accepted. In this case, use the **bridge cist port** command instead.
- Note that for 802.1S Multiple Spanning Tree Instances (MSTI), the port Spanning Tree status is inherited from the CIST instance and is not a configurable parameter.
- When STP is disabled on a port, the port is set to a forwarding state for the specified STP instance.
- If STP is disabled on a VLAN in the 1x1 mode, the port Spanning Tree status is ignored and all active ports associated with the VLAN are put in a forwarding state and not included in the Spanning Tree Algorithm. Note that ports at this point are *not* switching BPDU, unless the BPDU switching status for the VLAN is enabled.
- Physical ports that are reserved for link aggregation do not participate in the Spanning Tree Algorithm. Instead, the algorithm is applied to the aggregate logical link (virtual port) that represents a collection of physical ports.
- The *logical_ port* value range for link aggregate ID numbers is 0–29 on the OmniSwitch 6600 and 0–15 on the OmniSwitch 8800.

Examples

```
-> bridge mode flat
-> bridge 1 4/1 disable
-> bridge 1 1/24 enable

-> bridge mode 1x1
-> bridge 255 5/10 port enable
-> bridge 455 16 port enable
```

Release History

Release 5.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge cist port	Explicit command for configuring the Spanning Tree status on a port or an aggregate of ports for the CIST instance when the switch is operating in either the 1x1 or flat mode.
bridge 1x1 port	Explicit command for configuring the Spanning Tree status on a port or an aggregate of ports for a VLAN instance when the switch is operating in either the 1x1 or flat mode.
vlan stp	Enables or disables the Spanning Tree instance for a VLAN.
bridge bpdu-switching	Enables or disables BPDU switching for the specified VLAN.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortEnable
```

bridge cist port

Enables or disables the Spanning Tree status on a single port or an aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST) instance.

bridge cist {*slot/port* **|** *logical_port***} port {enable | disable}**

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
logical_port	The Link aggregate ID number (0–31).
enable	Enables Spanning Tree on the specified port for the CIST instance.
disable	Disables Spanning Tree on the specified port for the CIST instance.

Defaults

By default, the Spanning Tree status is enabled on eligible ports.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command is an explicit Spanning Tree command that only applies to the port Spanning Tree status for the flat mode CIST instance regardless of which operating mode (flat or 1x1) or protocol is active on the switch.
- If the switch is running in 1x1 mode when this command is used, the Spanning Tree status configured for the port is not active for the CIST instance until the operating mode for the switch is changed to the flat mode.
- Note that when a configuration snapshot is taken of the switch, all Spanning Tree commands are saved in their explicit format.
- When the Spanning Tree status is disabled on a port, the port is set to a forwarding state for the specified instance.
- If STP is disabled on a VLAN in the 1x1 mode, the port Spanning Tree status is ignored and all active ports associated with the VLAN are put in a forwarding state and not included in the Spanning Tree Algorithm. Note that ports at this point are *not* switching BPDU, unless the BPDU switching status for the VLAN is enabled.
- Physical ports that are reserved for link aggregation do not participate in the Spanning Tree Algorithm. Instead, the algorithm is applied to the aggregate logical link (virtual port) that represents a collection of physical ports.
- The *logical_ port* value range for link aggregate ID numbers is 0–29 on the OmniSwitch 6600 and 0–15 on the OmniSwitch 8800.

Examples

```
-> bridge mode flat
-> bridge cist 4/1 port enable
-> bridge cist 16 port enable

-> bridge mode 1x1
-> bridge cist 5/10 port enable
-> bridge cist 22 port enable
```

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge slot/port	Implicit command for configuring the Spanning Tree status on a port for the flat mode CIST instance or for a 1x1 mode VLAN instance.
bridge 1x1 port	Explicit command for configuring the Spanning Tree status on a port or an aggregate of ports for a VLAN instance when the switch is operating in either the 1x1 or flat mode.
vlan stp	Enables or disables the Spanning Tree instance for a VLAN.
bridge bpdu-switching	Enables or disables BPDU switching for the specified VLAN.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortEnable
```

bridge 1x1 port

Enables or disables the Spanning Tree status on a single port or an aggregate of ports for the specified VLAN instance.

bridge 1x1 *vid* **{***slot/port* **|** *logical_port***} port {enable | disable}**

Syntax Definitions

vid	An existing VLAN ID number (1–4094).
slot/port	The slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
logical_port	The Link aggregate ID number (0–31).
enable	Enables Spanning Tree on the specified port for the specified instance.
disable	Disables Spanning Tree on the specified port for the specified instance.

Defaults

By default, the Spanning Tree status is enabled on eligible ports.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command is an explicit Spanning Tree command that only applies to the specified VLAN instance regardless of which operating mode (flat or 1x1) is active on the switch.
- If the switch is running in the flat mode when this command is used, the Spanning Tree status configured for the port is not active for the specified VLAN instance until the operating mode for the switch is changed to the 1x1 mode.
- Note that when a configuration snapshot is taken of the switch, all Spanning Tree commands are saved in their explicit format.
- When the Spanning Tree status is disabled on a port, the port is set to a forwarding state for the specified instance.
- If STP is disabled on a VLAN in the 1x1 mode, the port Spanning Tree status is ignored and all active ports associated with the VLAN are put in a forwarding state and not included in the Spanning Tree Algorithm. Note that ports at this point are *not* switching BPDU, unless the BPDU switching status for the VLAN is enabled.
- Physical ports that are reserved for link aggregation do not participate in the Spanning Tree Algorithm. Instead, the algorithm is applied to the aggregate logical link (virtual port) that represents a collection of physical ports.
- The *logical_ port* value range for link aggregate ID numbers is 0–29 on the OmniSwitch 6600 and 0–15 on the OmniSwitch 8800.

Examples

```
-> bridge mode flat
-> bridge 1x1 2 4/1 port enable
-> bridge 1x1 3 16 port disable

-> bridge mode 1x1
-> bridge 1x1 2 5/10 port enable
-> bridge 1x1 3 22 port disable
```

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge slot/port	Implicit command for configuring the Spanning Tree status on a port for the flat mode CIST instance or for a 1x1 mode VLAN instance.
bridge cist port	Explicit command for configuring the Spanning Tree status on a port or an aggregate of ports for the CIST instance when the switch is operating in either the 1x1 or flat mode.
vlan stp	Enables or disables Spanning Tree instance for the specified VLAN.
bridge bpdu-switching	Enables or disables BPDU switching for the specified VLAN.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortEnable
```

bridge slot/port priority

Configures the Spanning Tree priority for a single port or an aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST) instance or a 1x1 mode VLAN instance. The Spanning Tree Algorithm uses the port priority value to determine the most favorable port when a bridge has multiple ports with the same path cost to the root bridge.

bridge *instance* **{***slot/port* | *logical_port***} priority** *priority*

Syntax Definitions

instance	The flat mode CIST instance or an existing VLAN ID number (1–4094).
slot/port	Enter the slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31).
priority	Port priority value (0–15). The lower the number, the higher the priority.

Defaults

By default, the bridge port priority value is set to 7.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The port priority specifies the value of the priority field contained in the first byte of the Port ID. The second byte contains the physical switch port number.
- Specifying an instance number with this command when the switch is running in the 1x1 Spanning Tree mode implies a VLAN ID and configures the port priority value for the associated VLAN instance.
- If the switch is running in the flat mode and STP (802.1D) or RSTP (802.1W) is the active protocol, enter 1 to specify the CIST instance. If MSTP (802.1S) is the active protocol, however, entering 1 for the instance number is not accepted. In this case, use the **bridge cist slot/port priority** command instead.
- The *logical_ port* value range for link aggregate ID numbers is 0–29 on the OmniSwitch 6600 and 0–15 on the OmniSwitch 8800.

Examples

```
-> bridge mode flat
-> bridge 1 4/1 priority 0

-> bridge mode 1x1
-> bridge 255 1/24 priority 5
-> bridge 455 3/12 priority 15
```

Release History

Release 5.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge cist slot/port priority	Explicit command for configuring the Spanning Tree priority for a port or an aggregate of ports for the CIST instance when the switch is operating in either the 1x1 or flat mode.
bridge msti slot/port priority	Explicit command for configuring the Spanning Tree priority for a port or an aggregate of ports for an MSTI when the switch is operating in either the 1x1 or flat mode.
bridge 1x1 slot/port priority	Explicit command for configuring the Spanning Tree priority for a port or an aggregate of ports for a VLAN instance when the switch is operating in either the 1x1 or flat mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortPriority
```

bridge cist slot/port priority

Configures the Spanning Tree priority value for a port or an aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST) instance. The Spanning Tree algorithm uses the port priority value to determine the most favorable port when a bridge has multiple ports with the same path cost to the root bridge.

bridge cist {*slot/port* | *logical_port***} priority** *priority*

Syntax Definitions

slot/port	Enter the slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31).
priority	Port priority value (0–15). The lower the number, the higher the priority.

Defaults

By default, the bridge port priority value is set to 7.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The port priority specifies the value of the priority field contained in the first byte of the Port ID. The second byte contains the physical switch port number.
- This command is an explicit Spanning Tree command that only applies to the port priority value for the flat mode CIST instance regardless of which operating mode (flat or 1x1) or protocol is active on the switch.
- If the switch is running in 1x1 mode when this command is used, the specified port priority value is not active for the CIST instance until the operating mode for the switch is changed to the flat mode.
- Note that when a configuration snapshot is taken of the switch, all Spanning Tree commands are saved in their explicit format.
- The *logical_ port* value range for link aggregate ID numbers is 0–29 on the OmniSwitch 6600 and 0–15 on the OmniSwitch 8800.

Examples

```
-> bridge mode flat
-> bridge cist 4/1 priority 2
-> bridge cist 10 priority 15

-> bridge mode 1x1
-> bridge cist 5/10 priority 1
-> bridge cist 16 priority 15
```

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge slot/port priority	Implicit command for configuring the Spanning Tree priority value for a port or an aggregate of ports that applies to the specified CIST or VLAN instance.
bridge msti slot/port priority	Explicit command for configuring the Spanning Tree priority value for a port or an aggregate of ports for an MSTI when the switch is operating in either the 1x1 or flat mode.
bridge 1x1 slot/port priority	Explicit command for configuring the Spanning Tree priority value for a port or an aggregate of ports for a VLAN instance when the switch is operating in either the 1x1 or flat mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortPriority
```

bridge msti slot/port priority

Configures the Spanning Tree priority value for a port or an aggregate of ports for the specified flat mode 802.1S Multiple Spanning Tree Instance (MSTI). The Spanning Tree algorithm uses the port priority value to determine the most favorable port when a bridge has multiple ports with the same path cost to the root bridge.

bridge msti *msti_id* **{***slot/port* | *logical_port***} priority** *priority*

Syntax Definitions

msti_id	An existing MSTI ID number (0–4094).
slot/port	Enter the slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31).
priority	Port priority value (0–15). The lower the number, the higher the priority.

Defaults

By default, the bridge port priority value is set to 7.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The port priority specifies the value of the priority field contained in the first byte of the Port ID. The second byte contains the physical switch port number.
- This command is an explicit Spanning Tree command that only applies to the specified MSTI regardless of which operating mode (flat or 1x1) is active on the switch. If MSTP (802.1S) is not the selected flat mode protocol, however, the port priority value for any MSTI is not configurable in either mode.
- Note that if zero is entered for the *msti_id* value, the specified priority value is applied to the CIST instance. The flat mode CIST instance 0 is also known as MSTI 0.
- The port priority value configured with this command is only applied to the specified MSTI. As a result, a single port can have different priority values for each instance. For example, in flat mode, port 1/24 can have a priority value of 7 for MSTI 2 and a priority value of 5 for MSTI 3.
- If the switch is running in 1x1 mode when this command is used, the specified priority value is not active for the specified MSTI until the operating mode for the switch is changed to the flat mode.
- Note that when a configuration snapshot is taken of the switch, all Spanning Tree commands are saved in their explicit format.
- The *logical_ port* value range for link aggregate ID numbers is 0–29 on the OmniSwitch 6600 and 0–15 on the OmniSwitch 8800.

Examples

```
-> bridge mode flat
-> bridge msti 0 1/24 priority 12
-> bridge msti 2 1/24 priority 5

-> bridge mode 1x1
-> bridge msti 0 1/24 priority 12
-> bridge msti 2 1/24 priority 5
```

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge slot/port priority	Implicit command for configuring the Spanning Tree priority value for a port or an aggregate of ports that applies to the specified CIST or VLAN instance.
bridge cist slot/port priority	Explicit command for configuring the Spanning Tree priority value for a port or an aggregate of ports for the CIST instance when the switch is operating in either the 1x1 or Tree mode.
bridge 1x1 slot/port priority	Explicit command for configuring the Spanning Tree priority value for a port or an aggregate of ports for a VLAN instance when the switch is operating in either the 1x1 or flat mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortPriority
```

bridge 1x1 slot/port priority

Configures the Spanning Tree priority value for a port or an aggregate of ports for the specified 1x1 mode VLAN instance. The Spanning Tree algorithm uses the port priority value to determine the most favorable port when a bridge has multiple ports with the same path cost to the root bridge.

bridge 1x1 *vid* **{***slot/port* | *logical_port***} priority** *priority*

Syntax Definitions

vid	An existing VLAN ID number (1–4094).
slot/port	Enter the slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31).
priority	Port priority value (0–15). The lower the number, the higher the priority.

Defaults

By default, the bridge port priority value is set to 7.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The port priority specifies the value of the priority field contained in the first byte of the Port ID. The second byte contains the physical switch port number.
- This command is an explicit Spanning Tree command that only applies to the specified VLAN instance regardless of which operating mode (flat or 1x1) or protocol is active on the switch.
- If the switch is running in the flat mode when this command is used, the specified priority value for the port is not active for the specified VLAN instance until the operating mode for the switch is changed to the 1x1 mode.
- Note that when a configuration snapshot is taken of the switch, all Spanning Tree commands are saved in their explicit format.
- The *logical_ port* value range for link aggregate ID numbers is 0–29 on the OmniSwitch 6600 and 0–15 on the OmniSwitch 8800

Examples

```
-> bridge mode flat
-> bridge 1x1 100 4/1 priority 2
-> bridge 1x1 200 1/24 priority 4

-> bridge mode 1x1
-> bridge 1x1 255 5/10 priority 1
-> bridge 1x1 455 1/16 priority 15
```

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge slot/port priority	Implicit command for configuring the Spanning Tree priority value for a port or an aggregate of ports that applies to the specified CIST or VLAN instance.
bridge slot/port path cost	Explicit command for configuring the Spanning Tree priority value for a port or an aggregate of ports for the CIST instance when the switch is operating in either the 1x1 or flat mode.
bridge msti slot/port priority	Explicit command for configuring the Spanning Tree priority value for a port or an aggregate of ports for an MSTI when the switch is operating in either the 1x1 or flat mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortPriority
```

bridge slot/port path cost

Configures the Spanning Tree path cost value for a single port or an aggregate of ports that applies to the specified flat mode Common and Internal Spanning Tree (CIST) instance or a 1x1 mode VLAN instance. This value is the contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops.

bridge *instance* **{***slot/port* | *logical_port***} path cost** *path_cost*

Syntax Definitions

instance	The flat mode CIST instance or an existing VLAN ID number (1–4094).
slot/port	Enter the slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31).
path_cost	Path cost value (0 - 65535 for 16-bit, 0–200000000 for 32-bit).

Defaults

By default, the path cost is set to zero.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Specifying an instance number with this command when the switch is running in the 1x1 Spanning Tree mode implies a VLAN ID and configures the port path cost for the associated VLAN instance.
- If the switch is running in the flat mode and STP (802.1D) or RSTP (802.1W) is the active protocol, enter 1 to specify the CIST instance. If MSTP (802.1S) is the active protocol, however, entering 1 for the instance number is not accepted. In this case, use the **bridge cist slot/port path cost** command instead.
- Note that when the Spanning Tree protocol is changed to/from MSTP (802.1S), the bridge priority and port path cost values for the flat mode CIST instance are reset to their default values.
- Use the **bridge path cost mode** command to automatically select the path cost value based on the active Spanning Tree protocol (16-bit for STP and RSTP, 32-bit for MSTP) or to use a 32-bit path cost value regardless of which protocol is active.
- The *logical_ port* value range for link aggregate ID numbers is 0–29 on the OmniSwitch 6600 and 0–15 on the OmniSwitch 8800.

- If a 32-bit path cost value is in use and the *path_cost* is set to zero, the following IEEE 802.1S recommended default path cost values based on link speed are used:

Link Speed	IEEE 802.1D Recommended Value
10 MB	2,000,000
100 MB	200,000
1 GB	20,000
10 Gbps	2,000

- Is a 16-bit path cost value is in use and the *path_cost* is set to zero, the following IEEE 802.1D recommended default path cost values based on link speed are used:

Link Speed	IEEE 802.1D Recommended Value
4 Mbps	250
10 Mbps	100
16 Mbps	62
100 Mbps	19
1 Gbps	4
10 Gbps	2

- If a 32-bit path cost value is in use and the *path_cost* for a link aggregate is set to zero, the following default values based on link speed and link aggregate size are used:

Link Speed	Aggregate Size (number of links)	Default Path Cost Value
10 MB	2	1,200,000
	4	800,000
	8	600,000
	16	400,000
100 MB	2	120,000
	4	80,000
	8	60,000
	16	40,000
1 GB	2	12,000
	4	8,000
	8	6,000
	16	4,000
10 GB	2	1,200
	4	800

Link Speed	Aggregate Size (number of links)	Default Path Cost Value
	8	600
	16	400

- If a 16-bit path cost value is in use and the *path_cost* for a link aggregate is set to zero, the following default values based on link speed and link aggregate size are used. Note that for Gigabit ports the aggregate size is not applicable in this case:

Link Speed	Aggregate Size (number of links)	Default Path Cost Value
10 Mbps	2	60
	4	40
	8	30
	16	20
100 Mbps	2	12
	4	9
	8	7
	16	5
1 Gbps	N/A	3
10 Gbps	N/A	1

Examples

```
-> bridge mode flat
-> bridge 1 4/1 path cost 19
-> bridge 1 5/1 path cost 0

-> bridge mode 1x1
-> bridge 455 1/24 path cost 2000
-> bridge 955 3/12 path cost 500
```

Release History

Release 5.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge path cost mode	Selects a 32-bit or automatic path cost mode for the switch.
bridge cist slot/port path cost	Explicit command for configuring the Spanning Tree path cost for a port or an aggregate of ports for the CIST instance when the switch is operating in either the 1x1 or flat mode.
bridge msti slot/port path cost	Explicit command for configuring the Spanning Tree path cost for a port or an aggregate of ports for an MSTI when the switch is operating in either the 1x1 or flat mode.
bridge 1x1 slot/port path cost	Explicit command for configuring the Spanning Tree path cost for a port or an aggregate of ports for a VLAN instance when the switch is operating in either the 1x1 or flat mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortPathCost
```

bridge cist slot/port path cost

Configures the Spanning Tree path cost value for a port or an aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST) instance. This value is the contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops.

bridge cist {*slot/port* | *logical_port***} path cost** *path_cost*

Syntax Definitions

slot/port	Enter the slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31).
path_cost	Path cost value (0 - 65535 for 16-bit, 0–200000000 for 32-bit).

Defaults

By default, the path cost is set to zero.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command is an explicit Spanning Tree command that only applies to the port path cost value for the CIST instance regardless of which operating mode (flat or 1x1) or protocol is active on the switch.
- If the switch is running in 1x1 mode when this command is used, the specified path cost value is not active for the CIST instance until the operating mode for the switch is changed to the flat mode.
- Note that when the Spanning Tree protocol is changed to/from MSTP (802.1S), the bridge priority and port path cost values for the flat mode CIST instance are reset to their default values.
- Use the **bridge path cost mode** command to automatically select the path cost value based on the active Spanning Tree protocol (16-bit for STP and RSTP, 32-bit for MSTP) or to use a 32-bit path cost value regardless of which protocol is active.
- Note that when a configuration snapshot is taken of the switch, all Spanning Tree commands are saved in their explicit format.
- The *logical_ port* value range for link aggregate ID numbers is 0–29 on the OmniSwitch 6600 and 0–15 on the OmniSwitch 8800

- If a 32-bit path cost value is in use and the *path_cost* is set to zero, the following IEEE 802.1S recommended default path cost values based on link speed are used:

Link Speed	IEEE 802.1D Recommended Value
10 MB	2,000,000
100 MB	200,000
1 GB	20,000
10 Gbps	2,000

- Is a 16-bit path cost value is in use and the *path_cost* is set to zero, the following IEEE 802.1D recommended default path cost values based on link speed are used:

Link Speed	IEEE 802.1D Recommended Value
4 Mbps	250
10 Mbps	100
16 Mbps	62
100 Mbps	19
1 Gbps	4
10 Gbps	2

- If a 32-bit path cost value is in use and the *path_cost* for a link aggregate is set to zero, the following default values based on link speed and link aggregate size are used:

Link Speed	Aggregate Size (number of links)	Default Path Cost Value
10 MB	2	1,200,000
	4	800,000
	8	600,000
	16	400,000
100 MB	2	120,000
	4	80,000
	8	60,000
	16	40,000
1 GB	2	12,000
	4	8,000
	8	6,000
	16	4,000
10 GB	2	1,200
	4	800

Link Speed	Aggregate Size (number of links)	Default Path Cost Value
	8	600
	16	400

- If a 16-bit path cost value is in use and the *path_cost* for a link aggregate is set to zero, the following default values based on link speed and link aggregate size are used. Note that for Gigabit ports the aggregate size is not applicable in this case:

Link Speed	Aggregate Size (number of links)	Default Path Cost Value
10 Mbps	2	60
	4	40
	8	30
	16	20
100 Mbps	2	12
	4	9
	8	7
	16	5
1 Gbps	N/A	3
10 Gbps	N/A	1

Examples

```
-> bridge mode flat
-> bridge cist 4/1 path cost 19
-> bridge cist 16 path cost 12000

-> bridge mode 1x1
-> bridge cist 5/10 path cost 19
-> bridge cist 11 path cost 12000
```

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge path cost mode	Selects a 32-bit or automatic path cost mode for the switch.
bridge slot/port path cost	Implicit command for configuring the Spanning Tree path cost value for a port or an aggregate of ports that applies to the specified CIST or VLAN instance.
bridge msti slot/port path cost	Explicit command for configuring the Spanning Tree path cost value for a port or an aggregate of ports for an 802.1S MSTI when the switch is operating in either the 1x1 or flat mode.
bridge 1x1 slot/port path cost	Explicit command for configuring the Spanning Tree path cost value for a port or an aggregate of ports for a VLAN instance when the switch is operating in either the 1x1 or flat mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortPathCost
```

bridge msti slot/port path cost

Configures the Spanning Tree path cost value for a port or an aggregate of ports for the specified flat mode 802.1S Multiple Spanning Tree Instance (MSTI). This value is the contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops.

bridge mist *msti_id* **{***slot/port* | *logical_port***} path cost** *path_cost*

Syntax Definitions

msti_id	An existing MSTI ID number (0–4094).
slot/port	Enter the slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31).
path_cost	Path cost value (0 - 65535 for 16-bit, 0–200000000 for 32-bit).

Defaults

By default, the path cost is set to zero.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command is an explicit Spanning Tree command that only applies to the specified MSTI regardless of which operating mode (flat or 1x1) is active on the switch. If MSTP (802.1S) is not the selected flat mode protocol, however, the path cost value for any MSTI is not configurable.
- Note that if zero is entered for the *msti_id* value, the specified path cost value is applied to the CIST instance. The flat mode CIST instance 0 is also known as MSTI 0.
- Note that when the Spanning Tree protocol is changed to/from MSTP (802.1S), the bridge priority and port path cost values for the flat mode CIST instance are reset to their default values.
- The path cost value configured with this command is only applied to the specified instance. As a result, a single port can have a different path cost for each instance. For example, in flat mode, port 1/24 can have a path cost of 20000 for MSTI 2 and a path cost of 200000 for MSTI 3.
- If the switch is running in 1x1 mode when this command is used, the specified path cost value is not active for the specified MSTI until the operating mode for the switch is changed to the flat mode.
- Note that when a configuration snapshot is taken of the switch, all Spanning Tree commands are saved in their explicit format.
- The *logical_ port* value range for link aggregate ID numbers is 0–29 on the OmniSwitch 6600 and 0–15 on the OmniSwitch 8800.
- When MSTP (802.1S) is the active protocol on the switch, only a 32-bit path cost value is used. Using a 16-bit path cost value is not an option.

- If zero is entered for the *path_cost* value, then the following IEEE 802.1S recommended default path cost values based on link speed are used:

Link Speed	IEEE 802.1D Recommended Value
10 MB	2,000,000
100 MB	200,000
1 GB	20,000
10 Gbps	2,000

- If the *path_cost* value for a link aggregate is set to zero, the following default values based on link speed and link aggregate size are used:

Link Speed	Aggregate Size (number of links)	Default Path Cost Value
10 MB	2	1,200,000
	4	800,000
	8	600,000
	16	400,000
100 MB	2	120,000
	4	80,000
	8	60,000
	16	40,000
1 GB	2	12,000
	4	8,000
	8	6,000
	16	4,000
10 GB	2	1,200
	4	800
	8	600
	16	400

Examples

```
-> bridge mode flat
-> bridge msti 0 4/1 path cost 200000
-> bridge msti 2 4/1 path cost 20000

-> bridge mode 1x1
-> bridge msti 0 1/24 path cost 200000
-> bridge msti 2 1/24 path cost 20000
```

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge slot/port path cost	Implicit command for configuring the Spanning Tree path cost value for a port or an aggregate of ports that applies to the specified CIST or VLAN instance.
bridge cist slot/port path cost	Explicit command for configuring the Spanning Tree path cost value for a port or an aggregate of ports for the CIST instance when the switch is operating in either the 1x1 or flat mode.
bridge 1x1 slot/port path cost	Explicit command for configuring the Spanning Tree path cost value for a port or an aggregate of ports for a VLAN instance when the switch is operating in either the 1x1 or flat mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortPathCost
```

bridge 1x1 slot/port path cost

Configures the Spanning Tree path cost value for a port or an aggregate of ports for the specified 1x1 mode VLAN instance. This value is the contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops.

bridge 1x1 *vid* **{***slot/port* | *logical_port***} path cost** *path_cost*

Syntax Definitions

vid	An existing VLAN ID number (1–4094).
slot/port	Enter the slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31).
path_cost	Path cost value (0 - 65535 for 16-bit, 0–200000000 for 32-bit).

Defaults

By default, the path cost is set to zero.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command is an explicit Spanning Tree command that only applies to the specified VLAN instance regardless of which operating mode (flat or 1x1) is active on the switch.
- If the switch is running in the flat mode when this command is used, the specified path cost for the port is not active for the specified VLAN instance until the operating mode for the switch is changed to the 1x1 mode.
- Note that when the Spanning Tree protocol is changed to/from MSTP (802.1S), the bridge priority and port path cost values for the flat mode CIST instance are reset to their default values.
- Use the **bridge path cost mode** command to automatically select the path cost value based on the active Spanning Tree protocol (16-bit for STP and RSTP, 32-bit for MSTP) or to use a 32-bit path cost value regardless of which protocol is active.
- Note that when a configuration snapshot is taken of the switch, all Spanning Tree commands are saved in their explicit format.
- The *logical_ port* value range for link aggregate ID numbers is 0–29 on the OmniSwitch 6600 and 0–15 on the OmniSwitch 8800.

- If a 32-bit path cost value is in use and the *path_cost* is set to zero, the following IEEE 892.1S recommended default path cost values based on link speed are used:

Link Speed	IEEE 802.1D Recommended Value
10 MB	2,000,000
100 MB	200,000
1 GB	20,000
10 Gbps	2,000

- Is a 16-bit path cost value is in use and the *path_cost* is set to zero, the following IEEE 802.1D recommended default path cost values based on link speed are used:

Link Speed	IEEE 802.1D Recommended Value
4 Mbps	250
10 Mbps	100
16 Mbps	62
100 Mbps	19
1 Gbps	4
10 Gbps	2

- If a 32-bit path cost value is in use and the *path_cost* for a link aggregate is set to zero, the following default values based on link speed and link aggregate size are used:

Link Speed	Aggregate Size (number of links)	Default Path Cost Value
10 MB	2	1,200,000
	4	800,000
	8	600,000
	16	400,000
100 MB	2	120,000
	4	80,000
	8	60,000
	16	40,000
1 GB	2	12,000
	4	8,000
	8	6,000
	16	4,000
10 GB	2	1,200
	4	800

Link Speed	Aggregate Size (number of links)	Default Path Cost Value
	8	600
	16	400

- If a 16-bit path cost value is in use and the *path_cost* for a link aggregate is set to zero, the following default values based on link speed and link aggregate size are used. Note that for Gigabit ports the aggregate size is not applicable in this case:

Link Speed	Aggregate Size (number of links)	Default Path Cost Value
10 Mbps	2	60
	4	40
	8	30
	16	20
100 Mbps	2	12
	4	9
	8	7
	16	5
1 Gbps	N/A	3
10 Gbps	N/A	1

Examples

```
-> bridge mode flat
-> bridge 1x1 200 4/1 path cost 4
-> bridge 1x1 300 16 path cost 200000

-> bridge mode 1x1
-> bridge 1x1 400 5/10 path cost 19
-> bridge 1x1 500 1/24 path cost 20000
```

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge slot/port path cost	Implicit command for configuring the Spanning Tree path cost value for a port or an aggregate of ports that applies to the specified CIST or VLAN instance.
bridge cist slot/port path cost	Explicit command for configuring the Spanning Tree path cost value for a port or an aggregate of ports for the CIST instance when the switch is operating in either the 1x1 or flat mode.
bridge msti slot/port path cost	Explicit command for configuring the Spanning Tree path cost value for a port or an aggregate of ports for an 802.1S MSTI when the switch is operating in either the 1x1 or flat Spanning Tree mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortPathCost
```

bridge slot/port mode

Configures Manual mode (forwarding or blocking) or Dynamic mode to manage the state of a port or an aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST) instance or a 1x1 mode VLAN instance. Dynamic mode defers the configuration of the port state to the Spanning Tree Protocol.

bridge *instance* **{***slot/port* | *logical_port***} mode {forwarding | blocking | dynamic}**

Syntax Definitions

instance	The CIST instance or an existing VLAN ID number (1–4094).
slot/port	Enter the slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31).
forwarding	Set port state to forwarding.
blocking	Set port state to blocking.
dynamic	Port state is determined by Spanning Tree Protocol.

Defaults

By default, the port Spanning Tree mode is set to dynamic.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Specifying an instance number with this command when the switch is running the 1x1 Spanning Tree operating mode implies a VLAN ID and configures the port Spanning Tree mode (**forwarding**, **blocking**, or **dynamic**) for the associated VLAN instance.
- If the switch is running in the flat mode and STP (802.1D) or RSTP (802.1W) is the active protocol, enter 1 to specify the CIST instance. If MSTP (802.1S) is the active protocol, however, entering 1 for the instance number is not accepted. In this case, use the **bridge cist slot/port mode** command instead.
- Note that for 802.1S Multiple Spanning Tree Instances (MSTI), the port Spanning Tree mode is inherited from the CIST instance and is not a configurable parameter.
- When port state is manually set to forwarding or blocking, the port remains in that state until it is changed using this command.
- Ports manually configured to operate in a forwarding or blocking state do not participate in the Spanning Tree Algorithm.
- The *logical_ port* value range for link aggregate ID numbers is 0–29 on the OmniSwitch 6600 and 0–15 on the OmniSwitch 8800.

Examples

```
-> bridge mode flat
-> bridge 1 4/1 mode forwarding

-> bridge mode 1x1
-> bridge 200 4/1 mode dynamic
-> bridge 300 1/24 mode forwarding
```

Release History

Release 5.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge cist slot/port mode	Explicit command for configuring the Spanning Tree mode on a port or an aggregate of ports for the CIST instance when the switch is operating in either the 1x1 or flat mode.
bridge 1x1 slot/port mode	Explicit command for configuring the Spanning Tree mode on a port or an aggregate of ports for a VLAN instance when the switch is operating in either the 1x1 or flat mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortManualMode
```

bridge cist slot/port mode

Configures Manual mode (forwarding or blocking) or Dynamic mode to manage the state of a port or an aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST) instance. Dynamic mode defers the management of the port state to the Spanning Tree algorithm.

bridge cist {*slot/port* | *logical_port***} mode {dynamic | blocking | forwarding}**

Syntax Definitions

slot/port	Enter the slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31).
dynamic	Port state is determined by Spanning Tree algorithm.
blocking	Sets port state to blocking.
forwarding	Sets port state to forwarding.

Defaults

By default, the port Spanning Tree mode is set to dynamic.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command is an explicit Spanning Tree command that only applies to the port Spanning Tree mode for the CIST instance regardless of which operating mode (flat or 1x1) is active on the switch.
- If the switch is running in 1x1 mode when this command is used, the specified port mode is not active for the CIST instance until the operating mode for the switch is changed to the flat mode.
- Note that when a configuration snapshot is taken of the switch, all Spanning Tree commands are saved in their explicit format.
- Ports manually configured to operate in a forwarding or blocking state do not participate in the Spanning Tree algorithm.
- When port state is manually set to forwarding or blocking, the port remains in that state until it is changed using this command.
- The *logical_ port* value range for link aggregate ID numbers is 0–29 on the OmniSwitch 6600 and 0–15 on the OmniSwitch 8800.

Examples

```
-> bridge mode flat
-> bridge cist 4/1 mode forwarding
-> bridge cist 10 mode blocking

-> bridge mode 1x1
-> bridge cist 2/2 mode blocking
-> bridge cist 11 mode forwarding
```

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge slot/port mode	Implicit command for configuring the Spanning Tree mode for a port or an aggregate of ports for the CIST instance or a VLAN instance.
bridge 1x1 slot/port mode	Explicit command for configuring the Spanning Tree mode for a port or an aggregate of ports for the specified VLAN instance when the switch is operating in either the 1x1 or flat Spanning Tree mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortManualMode
```

bridge 1x1 slot/port mode

Configures Manual mode (forwarding or blocking) or Dynamic mode to manage the state of a port or an aggregate of ports for the specified 1x1 mode VLAN instance. Dynamic mode defers the management of the port state to the Spanning Tree algorithm.

bridge 1x1 *vid* **{***slot/port* | *logical_port***} mode {dynamic | blocking | forwarding}**

Syntax Definitions

vid	An existing VLAN ID number (1–4094).
slot/port	Enter the slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31).
dynamic	Port state is determined by Spanning Tree algorithm.
blocking	Set port state to blocking.
forwarding	Set port state to forwarding.

Defaults

By default, the port Spanning Tree mode is set to dynamic.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command is an explicit Spanning Tree command that only applies to the specified VLAN instance regardless of which operating mode (flat or 1x1) is active on the switch.
- If the switch is running in the flat mode when this command is used, the specified mode for the port is not active for the specified VLAN instance until the operating mode for the switch is changed to the 1x1 mode.
- Note that when a configuration snapshot is taken of the switch, all Spanning Tree commands are saved in their explicit format.
- Ports manually configured to operate in a forwarding or blocking state do not participate in the Spanning Tree algorithm.
- When port state is manually set to forwarding or blocking, the port remains in that state until it is changed using this command.
- The *logical_ port* value range for link aggregate ID numbers is 0–29 on the OmniSwitch 6600 and 0–15 on the OmniSwitch 8800

Examples

```
-> bridge mode flat
-> bridge 1x1 255 4/1 mode forwarding
-> bridge 1x1 355 1/24 mode dynamic

-> bridge mode 1x1
-> bridge 1x1 255 2/2 mode blocking
-> bridge 1x1 355 3/12 mode forwarding
```

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge slot/port mode	Implicit command for configuring the Spanning Tree mode for a port or an aggregate of ports for the CIST instance or for a VLAN instance.
bridge cist slot/port mode	Explicit command for configuring the Spanning Tree mode for a port or an aggregate of ports for the CIST instance when the switch is operating in either the 1x1 or flat Spanning Tree mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortManualMode
```

bridge slot/port connection

Configures connection type for a port or an aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST) instance or a 1x1 mode VLAN instance. Some of the 802.1w rapid port state transitions depend on whether a port connects directly to another switch (point to point LAN segment) or connects to multiple switches (no point to point shared media LAN segment) or the port is at the edge of a bridged LAN (edge port). This command allows you to administratively define the point to point status of a port or if the port is considered an edge port.

bridge *instance* **{***slot/port* | *logical_port***} connection {noptp | ptp | autoptp | edgeport}**

Syntax Definitions

instance	The flat mode CIST instance or an existing VLAN ID number (1–4094).
slot/port	Enter the slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31).
noptp	Defines port connection type as no point to point link.
ptp	Defines port connection type as point to point link.
autoptp	Specifies that switch software will automatically define connection type as point to point or no point to point *and* whether or not the port is an edge port.
edgeport	Defines port connection type as an edge port link.

Defaults

By default the link connection type is set to auto point to point.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Specifying an instance number with this command when the switch is running the 1x1 Spanning Tree operating mode implies a VLAN ID and configures the port connection type for the associated VLAN instance.
- If the switch is running in the flat mode and STP (802.1D) or RSTP (802.1W) is the active protocol, enter 1 to specify the CIST instance. If MSTP (802.1S) is the active protocol, however, entering 1 for the instance number is not accepted. In this case, use the **bridge cist slot/port connection** command instead.
- Note that for 802.1S Multiple Spanning Tree Instances (MSTI), the port connection type is inherited from the CIST instance and is not a configurable parameter.
- A port is considered connected to a point to point LAN segment if the port belongs to a link aggregate of ports or if autonegotiation determines if the port should run in full duplex mode or if full duplex

mode was administratively set. Otherwise, the port is considered connected to a no point to point LAN segment.

- Rapid transition of a designated port to forwarding can only occur if the port's connection type is defined as a point to point or an edge port. Rapid transition of an alternate port role to a root port role is not affected by the port connection type definition.
- Configure ports that will connect to a host (PC, workstation, server, etc.) as edge ports to avoid unnecessary topology changes when these ports go active. This will also prevent the flushing of learned MAC addresses on these ports if a topology change occurs as a result of another non-edge port going active. If an edge port receives a BPDU it will operationally revert back to a no point to point connection type.
- The *logical_ port* value range for link aggregate ID numbers is 0–29 on the OmniSwitch 6600 and 0–15 on the OmniSwitch 8800.

Examples

```
-> bridge mode flat
-> bridge 1 1/24 connection noptp

-> bridge mode 1x1
-> bridge 200 8/2 connection edgeport
-> bridge 300 10 connection autoptp
```

Release History

Release 5.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge cist slot/port connection	Explicit command for configuring the Spanning Tree connection type for a port or an aggregate of ports for the CIST instance when the switch is operating in either the 1x1 or flat Spanning Tree mode.
bridge 1x1 slot/port connection	Explicit command for configuring the Spanning Tree connection type for a port or an aggregate of ports for the specified VLAN instance when the switch is operating in either the 1x1 or flat Spanning Tree mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortAdminConnectionType
   vStpInsPortOperConnectionType
```

bridge cist slot/port connection

Configures connection type for a port or an aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST). Some of the 802.1w rapid port state transitions depend on whether a port connects directly to another switch (point to point LAN segment) or connects to multiple switches (no point to point shared media LAN segment) or the port is at the edge of a bridged LAN (edge port). This command allows you to administratively define the point to point status of a port or if the port is considered as an edge port.

bridge cist {*slot/port* | *logical_port***} connection {noptp | ptp | autoptp | edgeport}**

Syntax Definitions

slot/port	Enter the slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31).
noptp	Defines port connection type as no point to point link.
ptp	Defines port connection type as point to point link.
autoptp	Specifies that switch software will automatically define connection type as point to point or no point to point *and* whether or not the port is an edge port.
edgeport	Defines port connection type as an edge port link.

Defaults

By default the link connection type is set to auto point to point.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command is an explicit Spanning Tree command that only applies to the port connection type for the CIST instance regardless of which operating mode (flat or 1x1) is active on the switch.
- If the switch is running in 1x1 mode when this command is used, the specified port connection type is not active for the CIST instance until the operating mode for the switch is changed to the flat mode.
- Note that when a configuration snapshot is taken of the switch, all Spanning Tree commands are saved in their explicit format.
- A port is considered connected to a point to point LAN segment if the port belongs to a link aggregate of ports or if autonegotiation determines the port should run in full duplex mode or if full duplex mode was administratively set. Otherwise, the port is considered connected to a no point to point LAN segment.
- Rapid transition of a designated port to forwarding can only occur if the port's connection type is defined as a point to point or an edge port. Rapid transition of an alternate port role to a root port role is not affected by the port connection type definition.

- Configure ports that will connect to a host (PC, workstation, server, etc.) as edge ports to avoid unnecessary topology changes when these ports go active. This will also prevent the flushing of learned MAC addresses on these ports if a topology change occurs as a result of another non-edge port going active. If an edge port receives a BPDU, it will operationally revert back to a no point to point connection type.
- The *logical_ port* value range for link aggregate ID numbers is 0–29 on the OmniSwitch 6600 and 0–15 on the OmniSwitch 8800.

Examples

```
-> bridge mode flat
-> bridge cist 7/24 connection noptp
-> bridge cist 15 connection edgeport

-> bridge mode 1x1
-> bridge cist 2/2 connection noptp
-> bridge cist 11 connection edgeport
```

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch
bridge slot/port connection	Implicit command for configuring the Spanning Tree connection type for a port or an aggregate of ports for the CIST instance or for a VLAN instance.
bridge 1x1 slot/port connection	Explicit command for configuring the Spanning Tree connection type for a port or an aggregate of ports for the specified VLAN instance when the switch is operating in either the 1x1 or flat Spanning Tree mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortAdminConnectionType
   vStpInsPortOperConnectionType
```

bridge 1x1 slot/port connection

Configures connection type for a port or an aggregate of ports for a 1x1 mode VLAN instance. Some of the 802.1w rapid port state transitions depend on whether a port connects directly to another switch (point to point LAN segment) or connects to multiple switches (no point to point shared media LAN segment) or the port is at the edge of a bridged LAN (edge port). This command allows you to administratively define the point to point status of a port or if the port is considered as an edge port.

bridge 1x1 *vid* **{***slot/port* | *logical_port***} connection {noptp | ptp | autoptp | edgeport}**

Syntax Definitions

vid	An existing VLAN ID number (1–4094).
slot/port	Enter the slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31).
noptp	Defines port connection type as no point to point link.
ptp	Defines port connection type as point to point link.
autoptp	Specifies that switch software will automatically define connection type as point to point or no point to point *and* whether or not the port is an edge port.
edgeport	Defines port connection type as an edge port link.

Defaults

By default the link connection type is set to auto point to point.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command is an explicit Spanning Tree command that only applies to the specified VLAN instance regardless of which operating mode (flat or 1x1) is active on the switch.
- If the switch is running in the flat mode when this command is used, the specified connection type for the port is not active for the specified VLAN instance until the operating mode for the switch is changed to the 1x1 mode.
- Note that when a configuration snapshot is taken of the switch, all Spanning Tree commands are saved in their explicit format.
- A port is considered connected to a point to point LAN segment if the port belongs to a link aggregate of ports or if autonegotiation determines the port should run in full duplex mode or if full duplex mode was administratively set. Otherwise, the port is considered connected to a no point to point LAN segment.

- Rapid transition of a designated port to forwarding can only occur if the port's connection type is defined as a point to point or an edge port. Rapid transition of an alternate port role to a root port role is not affected by the port connection type definition.
- Configure ports that will connect to a host (PC, workstation, server, etc.) as edge ports to avoid unnecessary topology changes when these ports go active. This will also prevent the flushing of learned MAC addresses on these ports if a topology change occurs as a result of another non-edge port going active. If an edge port receives a BPDU, it will operationally revert back to a no point to point connection type.
- The *logical_ port* value range for link aggregate ID numbers is 0–29 on the OmniSwitch 6600 and 0–15 on the OmniSwitch 8800.

Examples

```
-> bridge mode flat
-> bridge 1x1 255 7/24 connection noptp
-> bridge 1x1 355 1/5 connection edgeport

-> bridge mode 1x1
-> bridge 1x1 200 2/2 connection noptp
-> bridge 1x1 300 1/24 connection edgeport
```

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch
bridge slot/port connection	Implicit command for configuring the Spanning Tree connection type for a port or an aggregate of ports for the CIST instance or for a VLAN instance.
bridge cist slot/port connection	Explicit command for configuring the Spanning Tree connection type for a port or an aggregate of ports for the CIST instance when the switch is operating in either the 1x1 or flat Spanning Tree mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortAdminConnectionType
   vStpInsPortOperConnectionType
```

show spantree

Displays Spanning Tree bridge information for the flat mode Common and Internal Spanning Tree (CIST) instance or a 1x1 mode VLAN instance.

show spantree [*instance***]**

Syntax Definitions

instance	The flat mode CIST instance or an existing VLAN ID number (1–4094).

Defaults

parameter	default
instance	all instances

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If an instance number is *not* specified, this command displays the Spanning Tree status, protocol, and priority values for all instances.
- Specifying an instance number with this command when the switch is running the 1x1 Spanning Tree operating mode implies a VLAN ID and displays Spanning Tree bridge information for the associated VLAN instance.
- If the switch is running in the flat mode and STP (802.1D) or RSTP (802.1W) is the active protocol, enter 1 to specify the CIST instance. If MSTP (802.1S) is the active protocol, however, entering 1 for the instance number is not accepted. In this case, use the **show spantree cist** or **show spantree msti** commands instead.

Examples

```
-> bridge mode flat
-> bridge protocol rstp
-> show spantree
  Spanning Tree Path Cost Mode : AUTO
Bridge STP Status Protocol Priority(Prio:SysID)
------+----------+--------+--------------------
    1      ON      RSTP   32768 (0x8000:0x0000

-> show spantree 1
Spanning Tree Parameters
  Spanning Tree Status :                   ON,
  Protocol             :       IEEE Rapid STP,
  mode                 :    FLAT (Single STP),
  Priority             :       32768 (0x8000),
  Bridge ID            :   8000-00:d0:95:57:3a:9e,
  Designated Root      :   8000-00:00:e8:00:00:00,
  Cost to Root Bridge  :                   71,
```

```
Root Port            :   Slot 1 Interface 1,
Next Best Root Cost  :                    0,
Next Best Root Port  :                 None,
Hold Time            :                    1,
Topology Changes     :                    8,
Topology age         :              00:00:02,
  Current Parameters (seconds)
    Max Age              =    20,
    Forward Delay        =    15,
    Hello Time           =     2
  Parameters system uses when attempting to become root
    System Max Age       =    20,
    System Forward Delay =    15,
    System Hello Time    =     2
```

output definitions

Spanning Tree Path Cost Mode	The Spanning Tree path cost mode for the switch (**32 BIT** or **AUTO**) Configured through the **bridge path cost mode** command.
Bridge	The CIST instance, referred to as bridge 1 when either STP (802.1D) or RSTP (802.1W) is the active protocol in the flat mode.
Spanning Tree Status	The Spanning Tree state for the CIST instance (**ON** or **OFF**).
Protocol	The Spanning Tree protocol applied to this instance (**STP** or **RSTP**). Configured through the **bridge protocol** command.
Mode	The Spanning Tree operating mode for the switch (**1x1** or **flat**). Configured through the **bridge mode** command.
Priority	The Spanning Tree bridge priority for the instance. The lower the number, the higher the priority. Configured through the **bridge priority** command.
Bridge ID	The bridge identifier for this Spanning Tree instance. Consists of the bridge priority value (in hex) concatenated with the dedicated bridge MAC address.
Designated Root	The bridge identifier for the root of the Spanning Tree for this instance.
Cost to Root Bridge	The cost of the path to the root for this Spanning Tree instance.
Root Port	The port that offers the lowest cost path from this bridge to the root bridge for this Spanning Tree instance.
Next Best Root Cost	The cost of the next best root port for this Spanning Tree instance.
Next Best Root Port	The port that offers the next best (second lowest) cost path to the root bridge for this Spanning Tree instance.
Hold Time	The amount of time (in hundreths of a second) in which this Spanning Tree instance can transmit no more than two Configuration Bridge Protocol Data Units (BPDUs).
Topology Changes	The number of topology changes detected by this Spanning Tree instance since the management entity was last reset or initialized.
Topology age	The amount of time (in hundredths of seconds) since the last topology change was detected by this Spanning Tree instance (**hh:mm:ss** or **dd days and hh:mm:ss**).

output definitions

Max Age	The amount of time (in seconds) that Spanning Tree Protocol information is retained before it is discarded. Configured through the **bridge max age** command.
Forward Delay	The amount of time (in seconds) that a port will remain in the Listening state and then the Learning state until it reaches the forwarding state. This is also the amount of time used to age out all dynamic entries in the Forwarding Database when a topology change occurs. Configured through the **bridge forward delay** command.
Hello Time	The amount of time (in seconds) between the transmission of Configuration BPDUs on any port that is the Spanning Tree root or is attempting to become the Spanning Tree root. Configured through the **bridge hello time** command.
System Max Age	The Max Age value for the root bridge.
System Forward Delay	The Forward Delay value for the root bridge.
System Hello Time	The Hello Time value for the root bridge.

```
-> bridge mode flat
-> bridge protocol mstp
-> show spantree
  Spanning Tree Path Cost Mode : AUTO
 Msti STP Status Protocol Priority (Prio:SysID)
-----+----------+--------+--------------------
    0      ON      MSTP   32768 (0x8000:0x0000)
    2      ON      MSTP   32770 (0x8000:0x0002)
    3      ON      MSTP   32771 (0x8000:0x0003)
```

output definitions

Spanning Tree Path Cost Mode	The Spanning Tree path cost mode for the switch (**32 BIT** or **AUTO**) Configured through the **bridge path cost mode** command.
Msti	The 802.1S Multiple Spanning Tree Instance (MSTI) instance number. Configured through the **bridge msti** command. Note that MSTI 0 also represents the CIST instance that is always present on the switch.
Spanning Tree Status	The Spanning Tree state for the MSTI (**ON** or **OFF**).
Protocol	The Spanning Tree protocol applied to this instance. Configured through the **bridge protocol** command.
Priority	The Spanning Tree bridge priority for the instance. The lower the number, the higher the priority. Configured through the **bridge priority** command.

```
-> bridge mode 1x1
-> show spantree
  Spanning Tree Path Cost Mode : AUTO
 Vlan STP Status Protocol Priority
-----+----------+--------+--------------
    1      ON        STP   32768 (0x8000)
    2      ON        STP   32768 (0x8000)
    3      ON        STP   32768 (0x8000)
    4      ON        STP   32768 (0x8000)
    5      ON        STP   32768 (0x8000)
    6      ON        STP   32768 (0x8000)
    7      ON        STP   32768 (0x8000)

-> show spantree 2
Spanning Tree Parameters for Vlan 2
  Spanning Tree Status :                    ON,
  Protocol             :       IEEE STP,
  mode                 : 1X1 (1 STP per Vlan),
  Priority             :       32768 (0x8000),
  Bridge ID            :   8000-00:d0:95:6a:f4:58,
  Designated Root      :   0000-00:00:00:00:00:00,
  Cost to Root Bridge  :                     0,
  Root Port            :   Slot 1 Interface 1,
  Next Best Root Cost  :                     0,
  Next Best Root Port  :   Slot 1 Interface 1,
  Hold Time            :                     1,
  Topology Changes     :                     0,
  Topology age         :             00:00:00,
    Current Parameters (seconds)
      Max Age              =    20,
      Forward Delay        =    15,
      Hello Time           =     2
    Parameters system uses when attempting to become root
      System Max Age       =    20,
      System Forward Delay =    15,
      System Hello Time    =     2
```

output definitions

Spanning Tree Path Cost Mode	The Spanning Tree path cost mode for the switch (**32 BIT** or **AUTO**) Configured through the **bridge path cost mode** command.
Vlan	The VLAN ID associated with the VLAN Spanning Tree instance. Configured through the **vlan** commands
STP Status	The Spanning Tree state for the instance (**ON** or **OFF**). Configured through the **vlan stp** command.
Protocol	The Spanning Tree protocol applied to the instance (**STP** or **RSTP**). Configured through the **bridge protocol** command.
Mode	The Spanning Tree operating mode for the switch (**1x1** or **flat**). Configured through the **bridge mode** command.
Priority	The Spanning Tree bridge priority for the instance. The lower the number, the higher the priority. Configured through the **bridge priority** command.

output definitions (continued)

Bridge ID	The bridge identifier for this Spanning Tree instance. Consists of the bridge priority value (in hex) concatenated with the dedicated bridge MAC address.
Designated Root	The bridge identifier for the root of the Spanning Tree for this instance.
Cost to Root Bridge	The cost of the path to the root for this Spanning Tree instance.
Root Port	The port that offers the lowest cost path from this bridge to the root bridge for this Spanning Tree instance.
Next Best Root Cost	The cost of the next best root port for this Spanning Tree instance.
Next Best Root Port	The port that offers the next best (second lowest) cost path to the root bridge for this Spanning Tree instance.
Hold Time	The amount of time (in hundreths of a second) in which this Spanning Tree instance can transmit no more than two Configuration Bridge Protocol Data Units (BPDUs).
Topology Changes	The number of topology changes detected by this Spanning Tree instance since the management entity was last reset or initialized.
Topology age	The amount of time (in hundredths of seconds) since the last topology change was detected by this Spanning Tree instance (**hh:mm:ss** or **dd days and hh:mm:ss**).
Max Age	The amount of time (in seconds) that Spanning Tree Protocol information is retained before it is discarded. Configured through the **bridge max age** command.
Forward Delay	The amount of time (in seconds) that a port will remain in the Listening state and then the Learning state until it reaches the forwarding state. This is also the amount of time used to age out all dynamic entries in the Forwarding Database when a topology change occurs. Configured through the **bridge forward delay** command.
Hello Time	The amount of time (in seconds) between the transmission of Configuration BPDUs on any port that is the Spanning Tree root or is attempting to become the Spanning Tree root. Configured through the **bridge hello time** command.
System Max Age	The Max Age value for the root bridge.
System Forward Delay	The Forward Delay value for the root bridge.
System Hello Time	The Hello Time value for the root bridge.

Release History

Release 5.1; command was introduced.
Release 5.1.6 and 5.3.1; fields added for 802.1S support.

Related Commands

show spantree cist	Explicit command for displaying the Spanning Tree bridge configuration for the CIST instance regardless of which mode (1x1 or flat) is active on the switch.
show spantree msti	Explicit command for displaying the Spanning Tree bridge configuration for an MSTI regardless of which mode (1x1 or flat) is active on the switch.
show spantree 1x1	Explicit command for displaying the Spanning Tree bridge configuration for a VLAN instance regardless of which mode (1x1 or flat) is active on the switch.

MIB Objects

```
vStpInsTable
   vStpInsNumber
   vStpInsProtocolSpecification
   vStpInsMode
   vStpInsPriority
   vStpInsBridgeAddress
   vStpInsDesignatedRoot
   vStpInsRootCost
   vStpInsRootPortNumber
   vStpInsNextBestRootCost
   vStpInsNextBestRootPortNumber
   vStpInsHoldTime
   vStpInsTopChanges
   vStpInsTimeSinceTopologyChange
   vStpInsMaxAge
   vStpInsForwardDelay
   vStpInsHelloTime
```

show spantree cist

Displays the Spanning Tree bridge configuration for the flat mode Common and Internal Spanning Tree (CIST) instance.

show spantree cist

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guideline

This is an explicit Spanning Tree command that displays Spanning Tree bridge information for the flat mode CIST instance regardless of which mode (1x1 or flat) is active on the switch. Note that minimal information is displayed when this command is used in the 1x1 mode, as the CIST is not active in this mode. See second example below.

Examples

```
-> bridge mode flat
-> show spantree cist
Spanning Tree Parameters for Cist
  Spanning Tree Status :                   ON,
  Protocol             :       IEEE Multiple STP,
  mode                 :    FLAT (Single STP),
  Priority             :       32768 (0x8000),
  Bridge ID            :   8000-00:d0:95:6a:f4:58,
  CST Designated Root  :   0001-00:d0:95:6a:79:50,
  Cost to CST Root     :                   19,
  Next CST Best Cost   :                    0,
  Designated Root      :   8000-00:d0:95:6a:f4:58,
  Cost to Root Bridge  :                    0,
  Root Port            :   Slot 1 Interface 12,
  Next Best Root Cost  :                    0,
  Next Best Root Port  :                 None,
  Hold Time            :                    1,
  Topology Changes     :                    7,
  Topology age         :             00:00:07,
    Current Parameters (seconds)
      Max Age              =    20,
      Forward Delay        =    15,
      Hello Time           =     2
    Parameters system uses when attempting to become root
      System Max Age       =    20,
      System Forward Delay =    15,
      System Hello Time    =     2
```

```
-> bridge mode 1x1
-> show spantree cist
Per Vlan Spanning Tree is enforced !! (1x1 mode)
INACTIVE Spanning Tree Parameters for Cist
  Spanning Tree Status :                ON,
  Protocol             :       IEEE Multiple STP,
  Priority             :    32768 (0x8000),
  System Max Age (seconds)       =      20,
  System Forward Delay (seconds) =      15,
  System Hello Time (seconds)    =       2
```

output definitions

STP Status	The Spanning Tree state for the instance (**on** or **off**).
Protocol	The Spanning Tree protocol applied to the CIST (**STP, RSTP,** or **MSTP**). Configured through the **bridge protocol** command.
Mode	The Spanning Tree operating mode for the switch (**1x1** or **flat**). Configured through the **bridge mode** command.
Priority	The Spanning Tree bridge priority for the instance. The lower the number, the higher the priority. Configured through the **bridge priority** command.
Bridge ID	The bridge identifier for this Spanning Tree instance. Consists of the bridge priority value (in hex) concatenated with the dedicated bridge MAC address.
CST Designated Root	The bridge identifier for the root of the flat mode CIST instance. This field only appears when the 802.1S protocol is active on the switch.
Cost to CST Root	The cost of the path to the root of the flat mode CIST instance. This field only appears when the 802.1S protocol is active on the switch.
Next CST Best Cost	The cost of the next best root port for the flat mode CIST instance. This field only appears when the 802.1S protocol is active on the switch.
Designated Root	The bridge identifier for the root of the Spanning Tree for this instance.
Cost to Root Bridge	The cost of the path to the root for this Spanning Tree instance.
Root Port	The port that offers the lowest cost path from this bridge to the root bridge for this Spanning Tree instance.
Next Best Root Cost	The cost of the next best root port for this Spanning Tree instance.
Next Best Root Port	The port that offers the next best (second lowest) cost path to the root bridge for this Spanning Tree instance.
Hold Time	The amount of time (in hundreths of a second) in which this Spanning Tree instance can transmit no more than two Configuration BPDUs.
Topology Changes	The number of topology changes detected by this Spanning Tree instance since the management entity was last reset or initialized.
Topology age	The amount of time (in hundredths of seconds) since the last topology change was detected by this Spanning Tree instance (**hh:mm:ss** or **dd days and hh:mm:ss**).
Max Age	The amount of time (in seconds) that Spanning Tree Protocol information is retained before it is discarded. Configured through the **bridge max age** command.

output definitions (continued)

Forward Delay	The amount of time (in seconds) that a port will remain in the Listening state and then the Learning state until it reaches the forwarding state. This is also the amount of time used to age out all dynamic entries in the Forwarding Database when a topology change occurs. Configured through the **bridge forward delay** command.
Hello Time	The amount of time (in seconds) between the transmission of Configuration BPDUs on any port that is the Spanning Tree root or is attempting to become the Spanning Tree root. Configured through the **bridge hello time** command.
System Max Age	The Max Age value for the root bridge.
System Forward Delay	The Forward Delay value for the root bridge.
System Forward Delay	The Forward Delay value for the root bridge.

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

show spantree	Implicit command for displaying the Spanning Tree bridge configuration for the flat mode CIST instance or a 1x1 mode VLAN instance.
show spantree msti	Explicit command for displaying the Spanning Tree bridge configuration for an 802.1S MSTI regardless of which mode (1x1 or flat) is active on the switch.
show spantree 1x1	Explicit command for displaying the Spanning Tree bridge configuration for a VLAN instance regardless of which mode (1x1 or flat) is active on the switch.

MIB Objects

```
vStpInsTable
   vStpInsNumber
   vStpInsMode
   vStpInsProtocolSpecification
   vStpInsPriority
   vStpInsBridgeAddress
   vStpInsTimeSinceTopologyChange
   vStpInsTopChanges
   vStpInsDesignatedRoot
   vStpInsRootCost
   vStpInsRootPortNumber
   vStpInsNextBestRootCost
   vStpInsNextBestRootPortNumber
   vStpInsMaxAge
   vStpInsHelloTime
   vStpInsHoldTime
   vStpInsForwardDelay
   vStpInsBridgeMaxAge
   vStpInsBridgeHelloTime
   vStpInsBridgeForwardDelay
   vStpInsCistRegionalRootId
   vStpInsCistPathCost
```

show spantree msti

Displays Spanning Tree bridge information for an 802.1S Multiple Spanning Tree Instance (MSTI).

show spantree msti [*msti_id***]**

Syntax Definitions

msti_id	An existing MSTI ID number (0-4094).

Defaults

parameter	default
instance	all MSTIs

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If an *msti_id* number is *not* specified, this command displays the Spanning Tree status, protocol, and priority values for all MSTIs.
- This is an explicit Spanning Tree command that displays Spanning Tree bridge information for an MSTI regardless of which mode (1x1 or flat) is active on the switch.
- Note that minimal information is displayed when this command is used in the 1x1 mode, as MSTIs are not active in this mode. In addition, This command will fail if MSTP (802.1S) is not the selected flat mode protocol.
- Note that MSTI 0 also represents the CIST instance that is always present on the switch. To view the CIST instance using this command, specify zero (0) for the *msti_id* number.

Examples

```
-> bridge mode flat
-> bridge protocol mstp
-> show spantree msti
  Spanning Tree Path Cost Mode : AUTO
 Msti STP Status Protocol Priority (Prio:SysID)
-----+----------+--------+--------------------
    0      ON    MSTP   32768 (0x8000:0x0000)
    2      ON    MSTP   32770 (0x8000:0x0002)
    3      ON    MSTP   32771 (0x8000:0x0003)

-> show spantree msti 0
Spanning Tree Parameters for Cist
  Spanning Tree Status :                   ON,
  Protocol             :    IEEE Multiple STP,
  mode                 :    FLAT (Single STP),
  Priority             :       32768 (0x8000),
  Bridge ID            :   8000-00:d0:95:6b:08:40,
```

```
  CST Designated Root  :   0001-00:10:b5:58:9d:39,
  Cost to CST Root     :                  39,
  Next CST Best Cost   :                   0,
  Designated Root      :   8000-00:d0:95:6b:08:40,
  Cost to Root Bridge  :                   0,
  Root Port            :   Slot 9 Interface 2,
  Next Best Root Cost  :                   0,
  Next Best Root Port  :                None,
  Hold Time            :                   1,
  Topology Changes     :                   1,
  Topology age         :          0:30:46
    Current Parameters (seconds)
      Max Age              =     6,
      Forward Delay        =     4,
      Hello Time           =     2
    Parameters system uses when attempting to become root
      System Max Age       =    20,
      System Forward Delay =    15,
      System Hello Time    =     2

-> show spantree msti 1
Spanning Tree Parameters for Msti 1
  Spanning Tree Status :                  ON,
  Protocol             :    IEEE Multiple STP,
  mode                 :    FLAT (Single STP),
  Priority             :       32769 (0x8001),
  Bridge ID            :   8001-00:d0:95:6b:08:40,
  Designated Root      :   8001-00:d0:95:6b:08:40,
  Cost to Root Bridge  :                   0,
  Root Port            :                None,
  Next Best Root Cost  :                   0,
  Next Best Root Port  :                None,
  Hold Time            :                   1,
  Topology Changes     :                   0,
  Topology age         :           0:0:0
    Current Parameters (seconds)
      Max Age              =    20,
      Forward Delay        =    15,
      Hello Time           =     2
    Parameters system uses when attempting to become root
      System Max Age       =    20,
      System Forward Delay =    15,
      System Hello Time    =     2

-> bridge mode 1x1
-> show spantree msti
  Spanning Tree Path Cost Mode : AUTO
 ** Inactive flat mode instances: **
 Msti STP Status Protocol Priority (Prio:SysID)
-----+----------+--------+--------------------
    0      ON    MSTP   32768 (0x8000:0x0000)
    2      ON    MSTP   32770 (0x8000:0x0002)
    3      ON    MSTP   32771 (0x8000:0x0003)

-> show spantree msti 0
Per Vlan Spanning Tree is enforced !! (1x1 mode)
INACTIVE Spanning Tree Parameters for Cist
  Spanning Tree Status :               ON,
```

```
  Protocol             :       IEEE Multiple STP,
  Priority             :    32768 (0x8000),
  System Max Age (seconds)       =      20,
  System Forward Delay (seconds) =      15,
  System Hello Time (seconds)    =       2

-> show spantree msti 2
Per Vlan Spanning Tree is enforced !! (1x1 mode)
INACTIVE Spanning Tree Parameters for Msti 2
  Spanning Tree Status :                ON,
  Protocol             :       IEEE Multiple STP,
  Priority             :    32770 (0x8002),
  System Max Age (seconds)       =      20,
  System Forward Delay (seconds) =      15,
  System Hello Time (seconds)    =       2
```

output definitions

Spanning Tree Path Cost Mode	The Spanning Tree path cost mode for the switch (**32 BIT** or **AUTO**) Configured through the **bridge path cost mode** command.
Msti	The 802.1S Multiple Spanning Tree Instance (MSTI) number. MSTI 0 represents the CIST. Configured through the **bridge msti** command.
STP Status	The Spanning Tree state for the instance (**ON** or **OFF**).
Protocol	The Spanning Tree protocol applied to the instance (**STP, RSTP,** or **MSTP**). This value is not configurable for an MSTI. Configured through the **bridge protocol** command.
Mode	The Spanning Tree operating mode for the switch (**1x1** or **flat**). Configured through the **bridge mode** command.
Priority	The Spanning Tree bridge priority for the instance. The lower the number, the higher the priority. Configured through the **bridge msti priority** command.
Bridge ID	The bridge identifier for this Spanning Tree instance. Consists of the bridge priority value (in hex) concatenated with the dedicated bridge MAC address.
CST Designated Root	The bridge identifier for the root of the flat mode CIST instance. This field only appears when the 802.1S protocol is active on the switch.
Cost to CST Root	The cost of the path to the root for the flat mode CIST instance. This field only appears when the 802.1S protocol is active on the switch.
Next CST Best Cost	The cost of the next best root port for the flat mode CIST instance. This field only appears when the 802.1S protocol is active on the switch.
Designated Root	The bridge identifier for the root of the Spanning Tree for this instance.
Cost to Root Bridge	The cost of the path to the root for this Spanning Tree instance.
Root Port	The port that offers the lowest cost path from this bridge to the root bridge for this Spanning Tree instance.
Next Best Root Cost	The cost of the next best root port for this Spanning Tree instance.
Next Best Root Port	The port that offers the next best (second lowest) cost path to the root bridge for this Spanning Tree instance.

output definitions (continued)

Hold Time	The amount of time (in hundreths of a second) in which this Spanning Tree instance can transmit no more than two Configuration Bridge Protocol Data Units (BPDUs).
Topology Changes	The number of topology changes detected by this Spanning Tree instance since the management entity was last reset or initialized.
Topology age	The amount of time (in hundredths of seconds) since the last topology change was detected by this Spanning Tree instance (**hh:mm:ss** or **dd days and hh:mm:ss**).
Max Age	The amount of time (in seconds) that Spanning Tree Protocol information is retained before it is discarded. MSTIs inherit this value from the CIST instance.
Forward Delay	The amount of time (in seconds) that a port will remain in the Listening state and then the Learning state until it reaches the forwarding state. This is also the amount of time used to age out all dynamic entries in the Forwarding Database when a topology change occurs. MSTIs inherit this value from the CIST instance.
Hello Time	The amount of time (in seconds) between the transmission of Configuration BPDUs on any port that is the Spanning Tree root or is attempting to become the Spanning Tree root. MSTIs inherit this value from the CIST instance.
System Max Age	The Max Age value for the root bridge.
System Forward Delay	The Forward Delay value for the root bridge.
System Forward Delay	The Forward Delay value for the root bridge.

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

show spantree	Implicit command for displaying the Spanning Tree bridge configuration for the flat mode CIST instance or a 1x1 mode VLAN instance.
show spantree cist	Explicit command for displaying the Spanning Tree bridge configuration for the CIST instance regardless of which mode (1x1 or flat) is active on the switch.
show spantree 1x1	Explicit command for displaying the Spanning Tree bridge configuration for a VLAN instance regardless of which mode (1x1 or flat) is active on the switch.

MIB Objects

```
vStpInsTable
   vStpInsNumber
   vStpInsMode
   vStpInsProtocolSpecification
   vStpInsPriority
   vStpInsBridgeAddress
   vStpInsTimeSinceTopologyChange
   vStpInsTopChanges
   vStpInsDesignatedRoot
   vStpInsRootCost
   vStpInsRootPortNumber
   vStpInsNextBestRootCost
   vStpInsNextBestRootPortNumber
   vStpInsMaxAge
   vStpInsHelloTime
   vStpInsHoldTime
   vStpInsForwardDelay
   vStpInsBridgeMaxAge
   vStpInsBridgeHelloTime
   vStpInsBridgeForwardDelay
   vStpInsCistRegionalRootId
   vStpInsCistPathCost
   vStpInsMstiNumber
```

show spantree 1x1

Displays Spanning Tree bridge information for a 1x1 mode VLAN instance.

show spantree 1x1 [*vid***]**

Syntax Definitions

vid	An existing VLAN ID number (1-4094).

Defaults

parameter	default
instance	all VLAN instances

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If a *vid* number is *not* specified, this command displays the Spanning Tree status, protocol, and priority values for all VLAN instances.
- This is an explicit Spanning Tree command that displays Spanning Tree bridge information for a VLAN instance regardless of which mode (1x1 or flat) is active on the switch. Note that minimal information is displayed when this command is used in the flat mode, as VLAN instances are not active in this mode.

Examples

```
-> bridge mode flat
-> show spantree 1x1
  Spanning Tree Path Cost Mode : AUTO
 ** Inactive 1x1 mode instances: **
 Vlan STP Status Protocol Priority
-----+----------+--------+-------------
    1      ON        STP   32768 (0x8000)
    2      ON        STP   32768 (0x8000)
    3      ON        STP   32768 (0x8000)
    4      ON        STP   32768 (0x8000)
    5      ON        STP   32768 (0x8000)
    6      ON        STP   32768 (0x8000)

-> show spantree 1x1 7
Single/Multiple Spanning Tree is enforced !! (flat mode)
INACTIVE Spanning Tree Parameters for Vlan 7
  Spanning Tree Status :                ON,
  Protocol             :          IEEE STP,
  Priority             :    32768 (0x8000),
  System Max Age (seconds)       =      20,
  System Forward Delay (seconds) =      15,
  System Hello Time (seconds)    =       2
```

```
-> bridge mode 1x1
-> show spantree 1x1
  Spanning Tree Path Cost Mode : AUTO
 Vlan STP Status Protocol Priority
-----+----------+--------+-------------
    1      ON        STP   32768 (0x8000)
    2      ON        STP   32768 (0x8000)
    3      ON        STP   32768 (0x8000)
    4      ON        STP   32768 (0x8000)
    5      ON        STP   32768 (0x8000)
    6      ON        STP   32768 (0x8000)

-> show spantree 1x1 7
Spanning Tree Parameters for Vlan 7
  Spanning Tree Status :                   ON,
  Protocol             :       IEEE STP,
  mode                 : 1X1 (1 STP per Vlan),
  Priority             :       32768 (0x8000),
  Bridge ID            :   8000-00:d0:95:6a:f4:58,
  Designated Root      :   0000-00:00:00:00:00:00,
  Cost to Root Bridge  :                    0,
  Root Port            :   Slot 1 Interface 1,
  Next Best Root Cost  :                    0,
  Next Best Root Port  :   Slot 1 Interface 1,
  Hold Time            :                    1,
  Topology Changes     :                    0,
  Topology age         :             00:00:00,
    Current Parameters (seconds)
      Max Age              =    20,
      Forward Delay        =    15,
      Hello Time           =     2
    Parameters system uses when attempting to become root
      System Max Age       =    20,
      System Forward Delay =    15,
      System Hello Time    =     2
```

output definitions

Spanning Tree Path Cost Mode	The Spanning Tree path cost mode for the switch (**32 BIT** or **AUTO**) Configured through the **bridge path cost mode** command.
Vlan	The VLAN ID associated with the VLAN Spanning Tree instance. Configured through the **vlan** commands
STP Status	The Spanning Tree state for the instance (**ON** or **OFF**).
Protocol	The Spanning Tree protocol applied to the VLAN instance (**STP** or **RSTP**). Note that MSTP (802.1S) is not supported for a VLAN instance. Configured through the **bridge protocol** command.
Mode	The Spanning Tree operating mode for the switch (**1x1** or **flat**). Configured through the **bridge mode** command.
Priority	The Spanning Tree bridge priority for the instance. The lower the number, the higher the priority. Configured through the **bridge priority** command.
Bridge ID	The bridge identifier for this Spanning Tree instance. Consists of the bridge priority value (in hex) concatenated with the dedicated bridge MAC address.

output definitions (continued)

Designated Root	The bridge identifier for the root of the Spanning Tree for this instance.
Cost to Root Bridge	The cost of the path to the root for this Spanning Tree instance.
Root Port	The port that offers the lowest cost path from this bridge to the root bridge for this Spanning Tree instance.
Next Best Root Cost	The cost of the next best root port for this Spanning Tree instance.
Next Best Root Port	The port that offers the next best (second lowest) cost path to the root bridge for this Spanning Tree instance.
Hold Time	The amount of time (in hundreths of a second) in which this Spanning Tree instance can transmit no more than two Configuration BPDUs.
Topology Changes	The number of topology changes detected by this Spanning Tree instance since the management entity was last reset or initialized.
Topology age	The amount of time (in hundredths of seconds) since the last topology change was detected by this Spanning Tree instance (**hh:mm:ss** or **dd days and hh:mm:ss**).
Max Age	The amount of time (in seconds) that Spanning Tree Protocol information is retained before it is discarded. Configured through the **bridge max age** command.
Forward Delay	The amount of time (in seconds) that a port will remain in the Listening state and then the Learning state until it reaches the forwarding state. This is also the amount of time used to age out all dynamic entries in the Forwarding Database when a topology change occurs. Configured through the **bridge forward delay** command.
Hello Time	The amount of time (in seconds) between the transmission of Configuration BPDUs on any port that is the Spanning Tree root or is attempting to become the Spanning Tree root. Configured through the **bridge hello time** command.
System Max Age	The Max Age value for the root bridge.
System Forward Delay	The Forward Delay value for the root bridge.
System Forward Delay	The Forward Delay value for the root bridge.

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

show spantree	Implicit command for displaying the Spanning Tree bridge configuration for the flat mode CIST instance or a 1x1 mode VLAN instance.
show spantree cist	Explicit command for displaying the Spanning Tree bridge configuration for the CIST instance regardless of which mode (1x1 or flat) is active on the switch.
show spantree msti	Explicit command for displaying the Spanning Tree bridge information for an 802.1S MSTI when the switch is operating in the 1x1 or flat Spanning Tree mode.

MIB Objects

```
vStpInsTable
   vStpInsNumber
   vStpInsMode
   vStpInsProtocolSpecification
   vStpInsPriority
   vStpInsBridgeAddress
   vStpInsTimeSinceTopologyChange
   vStpInsTopChanges
   vStpInsDesignatedRoot
   vStpInsRootCost
   vStpInsRootPortNumber
   vStpInsNextBestRootCost
   vStpInsNextBestRootPortNumber
   vStpInsMaxAge
   vStpInsHelloTime
   vStpInsHoldTime
   vStpInsForwardDelay
   vStpInsBridgeMaxAge
   vStpInsBridgeHelloTime
   vStpInsBridgeForwardDelay
   vStpIns1x1VlanNumber
```

show spantree ports

Displays Spanning Tree port information for the flat mode Common and Internal Spanning Tree (CIST) instance or a 1x1 mode VLAN instance.

show spantree [*instance***] ports [forwarding | blocking | active | configured]**

Syntax Definitions

instance	The CIST instance or an existing VLAN ID number (1–4094).
forwarding	Displays Spanning Tree operational port parameters for ports that are forwarding for the specified instance.
blocking	Displays Spanning Tree operational port parameters for ports that are blocked for the specified instance.
active	Displays a list of active ports associated with the specified instance.
configured	Displays Spanning Tree administrative port parameters for all ports associated with the specified instance. Note that this parameter is only available if an *instance* value is specified with this command.

Defaults

parameter	default
instance	all instances
forwarding | blocking | active | configured	all ports

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If an instance number is *not* specified, this command displays the Spanning Tree operational status, path cost, and role for all ports and their associated instances.
- Specifying an instance number with this command when the switch is running the 1x1 Spanning Tree operating mode implies a VLAN ID and displays Spanning Tree port information for the associated VLAN instance.
- If the switch is running in the flat mode and STP (802.1D) or RSTP (802.1W) is the active protocol, enter 1 to specify the CIST instance. If MSTP (802.1S) is the active protocol, however, entering 1 for the instance number is not accepted. In this case, use the **show spantree cist ports** or **show spantree msti ports** commands instead.
- The **configured** keyword is only available when an instance number is specified with this command. In addition, this keyword cannot be used in combination with either the **forwarding** or **blocking** keywords.

Examples

```
-> bridge mode flat
-> show spantree ports
Bridge Port  Oper Status  Path Cost  Role
------+-----+------------+---------+-----
    1  1/1      FORW          19   ROOT
    1  1/2       DIS           0    DIS
    1  1/3       DIS           0    DIS
    1  1/4       DIS           0    DIS
    1  1/5       DIS           0    DIS
    1  1/6       DIS           0    DIS
    1  1/7       DIS           0    DIS
    1  1/8       DIS           0    DIS
    1  1/9       DIS           0    DIS
    1  1/10      DIS           0    DIS
    1  1/11      DIS           0    DIS
    1  1/12      DIS           0    DIS

-> show spantree 1 ports
Spanning Tree Port Summary
      Oper  Path   Desig        Fw  Prim. Op
Port   St   Cost    Cost   Role Tx  Port  Cnx  Desig Bridge ID
-----+----+-------+-------+----+---+-----+---+---------------------
 1/1  FORW      19      52 ROOT   1  1/1  PTP 8000-00:30:f1:5b:37:73
 1/2   DIS       0       0  DIS   0  1/2   NS 0000-00:00:00:00:00:00
 1/3   DIS       0       0  DIS   0  1/3   NS 0000-00:00:00:00:00:00
 1/4   DIS       0       0  DIS   0  1/4   NS 0000-00:00:00:00:00:00
 1/5   DIS       0       0  DIS   0  1/5   NS 0000-00:00:00:00:00:00
 1/6   DIS       0       0  DIS   0  1/6   NS 0000-00:00:00:00:00:00
 1/7   DIS       0       0  DIS   0  1/7   NS 0000-00:00:00:00:00:00
 1/8   DIS       0       0  DIS   0  1/8   NS 0000-00:00:00:00:00:00
 1/9   DIS       0       0  DIS   0  1/9   NS 0000-00:00:00:00:00:00
 1/10  DIS       0       0  DIS   0  1/10  NS 0000-00:00:00:00:00:00
 1/11  DIS       0       0  DIS   0  1/11  NS 0000-00:00:00:00:00:00
 1/12  DIS       0       0  DIS   0  1/12  NS 0000-00:00:00:00:00:00

-> show spantree 1 ports active
Spanning Tree Port Summary
      Oper  Path   Desig        Fw  Prim. Op
Port   St   Cost    Cost   Role Tx  Port  Cnx  Desig Bridge ID
-----+----+-------+-------+----+---+-----+---+---------------------
 1/1  FORW      19      52 ROOT   1  1/1  PTP 8000-00:30:f1:5b:37:73
```

output definitions

Bridge	The CIST instance, referred to as bridge 1 when either STP (802.1D) or RSTP (802.1W) is the active protocol in the flat mode.
Port	The slot number for the module and the physical port number or a logical port. If the slot number is 0, then the port number refers to a link aggregate logical port number (e.g., 0/31).
Oper St	The port operational state as defined by application of the Spanning Tree Protocol. Possible port operational states include: disabled, blocking, learning, and forwarding.

output definitions (continued)

Path Cost	The contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops. Configured through the **bridge slot/port path cost** command.
Desig Cost	The path cost of the Designated Port of the segment connected to this port. If this is the root bridge or the Spanning Tree status of the port is administratively disabled, this value is 0.
Role	The role of the port for this Spanning Tree instance. Possible port roles are: **root, designated, alternate**, and **backup**.
Fw Tx	Forward Transmission. The number of times the port has transitioned from the learning state to the forwarding state.
Prim. Port	The slot number for the module and the physical port number on that module for the primary port associated with this Spanning Tree instance. This information is only available if the port role is backup.
Op Cnx	Operational connection type: **PTP, NPT**, **NS** (nonsignificant), or **EDG.** Shows the current operational state of the port's connection type. See the **bridge slot/port connection** command on page 16-86 for more information.
Desig Bridge ID	The bridge identifier for the designated bridge for this port's segment.

```
-> show spantree 1 ports configured
Spanning Tree Port Admin Configuration
      Port  Adm Man. Config  Adm  OS8800
Port  Pri   St. Mode   Cost  Cnx  10G Opt.
-----+----+----+----+-------+----+--------
 1/1     7  ENA  No        0  AUT    DIS
 1/2     7  ENA  No        0  AUT    DIS
 1/3     7  ENA  No        0  AUT    DIS
 1/4     7  ENA  No        0  AUT    DIS
 1/5     7  ENA  No        0  AUT    DIS
 1/6     7  ENA  No        0  AUT    DIS
 1/7     7  ENA  No        0  AUT    DIS
 1/8     7  ENA  No        0  AUT    DIS
 1/9     7  ENA  No        0  AUT    DIS
 1/10    7  ENA  No        0  AUT    DIS
 1/11    7  ENA  No        0  AUT    DIS
 1/12    7  ENA  No        0  AUT    DIS
```

output definitions

Port	The slot number for the module and the physical port number or a logical port. If the slot number is 0, then the port number refers to a link aggregate logical port number (e.g., 0/31).
Port Pri	The Spanning Tree priority for the port (0–15). The lower the number, the higher the priority. Configured through the **bridge slot/port priority** command.
Adm St	The Spanning Tree administrative status of the port: **enabled** or **disabled**. Configured through the **bridge slot/port** command to enable or disable Spanning Tree on a port.

output definitions (continued)

Man. Mode	The manual mode setting for the port: **yes** indicates that the blocking or forwarding state of the port was manually set and the port does not participate in the Spanning Tree Algorithm; **no** indicates that the Spanning Tree Algorithm is managing the port state. Configured through the **bridge slot/port mode** command.
Config Cost	The configured path cost value for this port. Configured through the **bridge slot/port path cost** command.
Adm Cnx	Administrative connection type: **PTP, NPT, AUT**, or **EDG.** Configured through the **bridge slot/port connection** command.
OS8800 10G Opt.	Indicates whether the 10 GB port interoperability status is enabled (**ENA**) or disabled (**DIS**).

```
-> bridge mode flat
-> bridge protocol mstp
-> show spantree ports
 Msti  Port Oper Status  Path Cost  Role
-----+-----+------------+---------+-----
    0  1/1      FORW       200000   ROOT
    0  1/2       DIS           0    DIS
    0  1/3       DIS           0    DIS
    0  1/4       DIS           0    DIS
    0  1/5       DIS           0    DIS
    0  1/6       DIS           0    DIS
    0  1/7       DIS           0    DIS
    0  1/8       DIS           0    DIS
    0  1/9       DIS           0    DIS
    0  1/10      DIS           0    DIS
    0  1/11      DIS           0    DIS
    0  1/12      DIS           0    DIS
    0  1/13      DIS           0    DIS
    0  1/14      DIS           0    DIS
    0  1/15      DIS           0    DIS
    0  1/16      DIS           0    DIS
    0  1/17      DIS           0    DIS
    0  1/18      DIS           0    DIS
    0  1/19      DIS           0    DIS
    0  1/20      DIS           0    DIS
    0  1/21      DIS           0    DIS
    0  1/22      DIS           0    DIS
    0  1/23      DIS           0    DIS
    0  1/24      DIS           0    DIS
    0  5/1       DIS           0    DIS
    0  5/2       DIS           0    DIS
    1  1/1      FORW       200000   MSTR
    1  1/2       DIS           0    DIS
    1  1/3       DIS           0    DIS
    1  1/4       DIS           0    DIS
    1  1/5       DIS           0    DIS
    1  1/6       DIS           0    DIS
    1  1/7       DIS           0    DIS
    1  1/8       DIS           0    DIS
    1  1/9       DIS           0    DIS
    1  1/10      DIS           0    DIS
    1  1/11      DIS           0    DIS
    1  1/12      DIS           0    DIS
```

```
    1  1/13      DIS           0    DIS
    1  1/14      DIS           0    DIS
    1  1/15      DIS           0    DIS
    1  1/16      DIS           0    DIS
    1  1/17      DIS           0    DIS
    1  1/18      DIS           0    DIS
    1  1/19      DIS           0    DIS
    1  1/20      DIS           0    DIS
    1  1/21      DIS           0    DIS
    1  1/22      DIS           0    DIS
    1  1/23      DIS           0    DIS
    1  1/24      DIS           0    DIS

-> show spantree ports active
 Msti  Port Oper Status  Path Cost  Role
-----+-----+------------+---------+-----
    0  1/1      FORW       200000   ROOT
    1  1/1      FORW       200000   MSTR
    2  1/1      FORW       200000   MSTR
```

output definitions

Msti	The 802.1S Multiple Spanning Tree Instance (MSTI) instance number. Configured through the **bridge msti** command. Note that MSTI 0 also represents the CIST instance that is always present on the switch.
Port	The slot number for the module and the physical port number or a logical port. If the slot number is 0, then the port number refers to a link aggregate logical port number (e.g., 0/31).
Oper St	The port operational state as defined by application of the Spanning Tree Protocol. Possible port operational states include: disabled, blocking, learning, and forwarding.
Path Cost	The contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops. Configured through the **bridge slot/port path cost** command.
Role	The role of the port for this Spanning Tree instance. Possible port roles are: **root, designated, alternate**, and **backup**.

```
-> bridge mode 1x1
-> show spantree ports
 Vlan  Port Oper Status  Path Cost  Role
-----+-----+------------+---------+-----
    1  1/1       DIS           0    DIS
    1  1/2       DIS           0    DIS
    1  1/3       DIS           0    DIS
    1  1/4       DIS           0    DIS
    1  1/5       DIS           0    DIS
    1  1/6       DIS           0    DIS
    1  1/7       DIS           0    DIS
    1  1/8       DIS           0    DIS
    1  1/9       DIS           0    DIS
    1  1/10      DIS           0    DIS
    1  1/11      DIS           0    DIS
    1  1/12     FORW          19    ROOT
-> show spantree 1 ports
Spanning Tree Port Summary for Vlan 1
```

```
      Oper  Path   Desig        Fw  Prim. Op
Port   St   Cost    Cost   Role Tx  Port  Cnx  Desig Bridge ID
-----+----+-------+-------+----+---+-----+---+---------------------
 1/1   DIS       0       0  DIS   0  1/1   NS 0000-00:00:00:00:00:00
 1/2   DIS       0       0  DIS   0  1/2   NS 0000-00:00:00:00:00:00
 1/3   DIS       0       0  DIS   0  1/3   NS 0000-00:00:00:00:00:00
 1/4   DIS       0       0  DIS   0  1/4   NS 0000-00:00:00:00:00:00
 1/5   DIS       0       0  DIS   0  1/5   NS 0000-00:00:00:00:00:00
 1/6   DIS       0       0  DIS   0  1/6   NS 0000-00:00:00:00:00:00
 1/7   DIS       0       0  DIS   0  1/7   NS 0000-00:00:00:00:00:00
 1/8   DIS       0       0  DIS   0  1/8   NS 0000-00:00:00:00:00:00
 1/9   DIS       0       0  DIS   0  1/9   NS 0000-00:00:00:00:00:00
 1/10  DIS       0       0  DIS   0  1/10  NS 0000-00:00:00:00:00:00
 1/11  DIS       0       0  DIS   0  1/11  NS 0000-00:00:00:00:00:00
 1/12 FORW      19       0 ROOT   1  1/12 PTP 0001-00:d0:95:6a:79:50

-> show spantree 1 ports active
Spanning Tree Port Summary for Vlan 1
      Oper  Path   Desig        Fw  Prim. Op
Port   St   Cost    Cost   Role Tx  Port  Cnx  Desig Bridge ID
-----+----+-------+-------+----+---+-----+---+---------------------
 1/12 FORW      19       0 ROOT   1  1/12 PTP 0001-00:d0:95:6a:79:50
```

output definitions

Vlan	The VLAN ID associated with the VLAN Spanning Tree instance. Configured through the **vlan** commands
Port	The slot number for the module and the physical port number or a logical port. If the slot number is 0, then the port number refers to a link aggregate logical port number (e.g., 0/31).
Oper St	The port operational state as defined by application of the Spanning Tree Protocol. Possible port operational states include: disabled, blocking, listening, learning, and forwarding.
Path Cost	The contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops. Configured through the **bridge slot/port path cost** command.
Desig Cost	The path cost of the Designated Port of the segment connected to this port. If this is the root bridge or the Spanning Tree status of the port is administratively disabled, this value is 0.
Role	The role of the port for this Spanning Tree instance. Possible port roles are: **root, designated, alternate**, and **backup**.
Fw Tx	Forward Transmission. The number of times the port has transitioned from the learning state to the forwarding state.
Prim. Port	The slot number for the module and the physical port number on that module for the primary port associated with this Spanning Tree instance. This information is only available if the port role is backup.
Op Cnx	Operational connection type: **PTP, NPT**, **NS** (nonsignificant), or **EDG.** Shows the current operational state of the port's connection type. See the **bridge slot/port connection** command on page 16-86 for more information.
Desig Bridge ID	The bridge identifier for the designated bridge for this port's segment.

```
-> show spantree 1 ports configured
Spanning Tree Port Admin Configuration for Vlan 1
      Port  Adm Man. Config  Adm  OS8800
Port  Pri   St. Mode   Cost  Cnx  10G Opt.
-----+----+----+----+-------+----+--------
 1/1     7  ENA  No        0  AUT    DIS
 1/2     7  ENA  No        0  AUT    DIS
 1/3     7  ENA  No        0  AUT    DIS
 1/4     7  ENA  No        0  AUT    DIS
 1/5     7  ENA  No        0  AUT    DIS
 1/6     7  ENA  No        0  AUT    DIS
 1/7     7  ENA  No        0  AUT    DIS
 1/8     7  ENA  No        0  AUT    DIS
 1/9     7  ENA  No        0  AUT    DIS
 1/10    7  ENA  No        0  AUT    DIS
 1/11    7  ENA  No        0  AUT    DIS
 1/12    7  ENA  No        0  AUT    DIS
```

output definitions

Port	The slot number for the module and the physical port number or a logical port. If the slot number is 0, then the port number refers to a link aggregate logical port number (e.g., 0/31).
Port Pri	The Spanning Tree priority for the port (0–15). The lower the number, the higher the priority. Configured through the **bridge slot/port priority** command.
Adm St	The Spanning Tree administrative status of the port: **enabled** or **disabled**. Configured through the **bridge slot/port** command to enable or disable Spanning Tree on a port.
Man. Mode	The manual mode setting for the port: **yes** indicates that the blocking or forwarding state of the port was manually set and the port does not participate in the Spanning Tree Algorithm; **no** indicates that the Spanning Tree Algorithm is managing the port state. Configured through the **bridge slot/port mode** command.
Config Cost	The configured path cost value for this port. Configured through the **bridge slot/port path cost** command.
Adm Cnx	Administrative connection type: **PTP, NPT, AUT**, or **EDG.** Configured through the **bridge slot/port connection** command.
OS8800 10G Opt.	Indicates whether the 10 GB port interoperability status is enabled (**ENA**) or disabled (**DIS**).

Release History

Release 5.1; command was introduced.
Release 5.1.6; fields added for 802.1S support.

Related Commands

show spantree cist ports	Implicit command for displaying Spanning Tree port information for the flat mode CIST when the switch is operating in the 1x1 or flat Spanning Tree mode.
show spantree msti ports	Explicit command for displaying Spanning Tree port information for an 802.1S MSTI when the switch is operating in the 1x1 or flat Spanning Tree mode.
show spantree 1x1 ports	Explicit command for displaying Spanning Tree port information for a VLAN instance when the switch is operating in the 1x1 or flat Spanning Tree mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortPriority
   vStpInsPortEnable
   vStpInsPortState
   vStpInsPortManualMode
   vStpInsPortPathCost
   vStpInsPortDesignatedCost
   vStpInsPortRole
   vStpInsPortForwardTransitions
   vStpInsPrimaryPortNumber
   vStpInsPortDesignatedRoot
   vStpInsPortDesignatedBridge
```

show spantree cist ports

Displays Spanning Tree port information for the flat mode Common and Internal Spanning Tree (CIST) instance.

show spantree cist ports [forwarding | blocking | active | configured]

Syntax Definitions

forwarding	Displays Spanning Tree operational port parameters for ports that are forwarding for the CIST instance.
blocking	Displays Spanning Tree operational port parameters for ports that are blocked for the CIST instance.
active	Displays a list of active ports associated with the specified instance.
configured	Displays Spanning Tree administrative port parameters for the CIST instance.

Defaults

parameter	default
forwarding | blocking | active | configured	all ports

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This is an explicit Spanning Tree command that displays Spanning Tree port information for the flat mode CIST instance regardless of which mode (1x1 or flat) is active on the switch.
- Note that minimal information is displayed when this command is used in the 1x1 mode, as the CIST is not active in this mode.

Examples

```
-> show spantree cist ports
Spanning Tree Port Summary for Cist
      Oper  Path   Desig        Fw  Prim. Op
Port   St   Cost    Cost   Role Tx  Port  Cnx  Desig Bridge ID
-----+----+-------+-------+----+---+-----+---+---------------------
 1/1  FORW  200000      52 ROOT   1  1/1  PTP 8000-00:30:f1:5b:37:73
 1/2   DIS       0       0  DIS   0  1/2   NS 0000-00:00:00:00:00:00
 1/3   DIS       0       0  DIS   0  1/3   NS 0000-00:00:00:00:00:00
 1/4   DIS       0       0  DIS   0  1/4   NS 0000-00:00:00:00:00:00
 1/5   DIS       0       0  DIS   0  1/5   NS 0000-00:00:00:00:00:00
 1/6   DIS       0       0  DIS   0  1/6   NS 0000-00:00:00:00:00:00
 1/7   DIS       0       0  DIS   0  1/7   NS 0000-00:00:00:00:00:00
 1/8   DIS       0       0  DIS   0  1/8   NS 0000-00:00:00:00:00:00
```

```
-> show spantree cist ports active
Spanning Tree Port Summary for Cist
      Oper  Path   Desig        Fw  Prim. Op
Port   St   Cost    Cost   Role Tx  Port  Cnx  Desig Bridge ID
-----+----+-------+-------+----+---+-----+---+--------------------
1/1  FORW  200000      52 ROOT   1  1/1  PTP 8000-00:30:f1:5b:37:73
```

output definitions

Port	The slot number for the module and the physical port number or a logical port. If the slot number is 0, then the port number refers to a link aggregate logical port number (e.g., 0/31).
Oper St	The port operational state as defined by application of the Spanning Tree Protocol. Possible port operational states include: disabled, blocking, listening, learning, and forwarding.
Path Cost	The contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops. Configured through the **bridge slot/port path cost** command.
Desig Cost	The path cost of the Designated Port of the segment connected to this port. If this is the root bridge or the Spanning Tree status of the port is administratively disabled, this value is 0.
Role	The role of the port for this Spanning Tree instance. Possible port roles are: **root, designated, alternate**, and **backup**.
Fw Tx	Forward Transmission. The number of times the port has transitioned from the learning state to the forwarding state.
Prim. Port	The slot number for the module and the physical port number on that module for the primary port associated with this Spanning Tree instance. This information is only available if the port role is backup.
Op Cnx	Operational connection type: **PTP, NPT**,**NS** (nonsignificant), or **EDG.** Shows the current operational state of the port's connection type. See the **bridge slot/port connection** command on page 16-86 for more information.
Desig Bridge ID	The bridge identifier for the designated bridge for this port's segment.

```
-> show spantree cist ports configured
Spanning Tree Port Admin Configuration for Cist
      Port  Adm Man. Config  Adm  OS8800
Port  Pri   St. Mode   Cost  Cnx  10G Opt.
-----+----+----+----+-------+----+--------
 1/1     7  ENA  No        0  AUT    DIS
 1/2     7  ENA  No        0  AUT    DIS
 1/3     7  ENA  No        0  AUT    DIS
 1/4     7  ENA  No        0  AUT    DIS
 1/5     7  ENA  No        0  AUT    DIS
 1/6     7  ENA  No        0  AUT    DIS
 1/7     7  ENA  No        0  AUT    DIS
 1/8     7  ENA  No        0  AUT    DIS
 1/9     7  ENA  No        0  AUT    DIS
```

output definitions

Port	The slot number for the module and the physical port number or a logical port. If the slot number is 0, then the port number refers to a link aggregate logical port number (e.g., 0/31).
Port Pri	The Spanning Tree priority for the port (0–15). The lower the number, the higher the priority. Configured through the **bridge slot/port priority** command.
Adm St	The Spanning Tree administrative status of the port: **enabled** or **disabled**. Configured through the **bridge slot/port** command to enable or disable Spanning Tree on a port.
Man. Mode	The manual mode setting for the port: **yes** indicates that the blocking or forwarding state of the port was manually set and the port does not participate in the Spanning Tree Algorithm; **no** indicates that the Spanning Tree Algorithm is managing the port state. Configured through the **bridge slot/port mode** command.
Config Cost	The configured path cost value for this port. Configured through the **bridge slot/port path cost** command.
Adm Cnx	Administrative connection type: **PTP, NPT, AUT**, or **EDG.** Configured through the **bridge slot/port connection** command.
OS8800 10G Opt.	Indicates whether the 10 GB port interoperability status is enabled (**ENA**) or disabled (**DIS**).

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

show spantree ports	Implicit command for displaying Spanning Tree port information for the flat mode CIST instance or a 1x1 mode VLAN instance.
show spantree msti ports	Explicit command for displaying Spanning Tree port information for an 802.1S MSTI when the switch is operating in the 1x1 or flat Spanning Tree mode.
show spantree 1x1 ports	Explicit command for displaying Spanning Tree port information for a VLAN instance when the switch is operating in the 1x1 or flat Spanning Tree mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortPriority
   vStpInsPortState
   vStpInsPortEnable
   vStpInsPortPathCost
   vStpInsPortDesignatedCost
   vStpInsPortDesignatedBridge
   vStpInsPortForwardTransitions
   vStpInsPortManualMode
   vStpInsPortRole
   vStpInsPrimaryPortNumber
   vStpInsPortAdminConnectionType
   vStpInsPortOperConnectionType
```

show spantree msti ports

Displays Spanning Tree port information for a flat mode 802.1S Multiple Spanning Tree Instance (MSTI).

show spantree msti [*msti_id***] ports [forwarding | blocking | active | configured]**

Syntax Definitions

msti_id	An existing MSTI ID number (0-4094).
forwarding	Displays Spanning Tree operational port parameters for ports that are forwarding for the CIST instance.
blocking	Displays Spanning Tree operational port parameters for ports that are blocked for the CIST instance.
active	Displays a list of active ports associated with the specified instance.
configured	Displays Spanning Tree administrative port parameters for the CIST instance.

Defaults

parameter	default
msti_id	all MSTIs
forwarding | blocking | active | configured	all ports

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If an *msti_id* number is *not* specified, this command displays the Spanning Tree port operational status, path cost, and role values for all associated MSTIs.
- This is an explicit Spanning Tree command that displays Spanning Tree port information for an MSTI regardless of which mode (1x1 or flat) is active on the switch.
- Note that minimal information is displayed when this command is used in the 1x1 mode, as MSTIs are not active in this mode. In addition, if MSTP (802.1S) is not the selected flat mode protocol, this command will fail.
- The **configured** keyword is only available when an instance number is specified with this command. In addition, this keyword cannot be used in combination with either the **forwarding** or **blocking** keywords.
- Note that MSTI 0 also represents the CIST instance that is always present on the switch. To view the CIST instance using this command, specify zero (0) for the *msti_id* number.

Examples

```
-> show spantree msti ports
 Msti  Port Oper Status  Path Cost  Role
-----+-----+-----------+---------+-----
    0  1/1      FORW       200000   ROOT
    0  1/2       DIS           0    DIS
    0  1/3       DIS           0    DIS
    0  1/4       DIS           0    DIS
    0  1/5       DIS           0    DIS
    0  1/6       DIS           0    DIS
    0  1/7       DIS           0    DIS
    0  1/8       DIS           0    DIS
    0  1/9       DIS           0    DIS
    0  1/10      DIS           0    DIS
    0  1/11      DIS           0    DIS
    0  1/12      DIS           0    DIS
    0  1/13      DIS           0    DIS
    0  1/14      DIS           0    DIS
    0  1/15      DIS           0    DIS
    0  1/16      DIS           0    DIS
    0  1/17      DIS           0    DIS
    0  1/18      DIS           0    DIS
    0  1/19      DIS           0    DIS
    0  1/20      DIS           0    DIS
    0  1/21      DIS           0    DIS
    0  1/22      DIS           0    DIS
    0  1/23      DIS           0    DIS
    0  1/24      DIS           0    DIS
    0  5/1       DIS           0    DIS
    0  5/2       DIS           0    DIS
    1  1/1      FORW       200000   MSTR
    1  1/2       DIS           0    DIS
    1  1/3       DIS           0    DIS
    1  1/4       DIS           0    DIS
    1  1/5       DIS           0    DIS
    1  1/6       DIS           0    DIS
    1  1/7       DIS           0    DIS
    1  1/8       DIS           0    DIS
    1  1/9       DIS           0    DIS
    1  1/10      DIS           0    DIS
    1  1/11      DIS           0    DIS
    1  1/12      DIS           0    DIS
    1  1/13      DIS           0    DIS
    1  1/14      DIS           0    DIS
    1  1/15      DIS           0    DIS
    1  1/16      DIS           0    DIS
    1  1/17      DIS           0    DIS
    1  1/18      DIS           0    DIS
    1  1/19      DIS           0    DIS
    1  1/20      DIS           0    DIS
    1  1/21      DIS           0    DIS
    1  1/22      DIS           0    DIS
    1  1/23      DIS           0    DIS
    1  1/24      DIS           0    DIS
    1  5/1       DIS           0    DIS
    1  5/2       DIS           0    DIS
```

```
-> show spantree msti 2 ports
Spanning Tree Port Summary for Msti 2
      Oper  Path   Desig        Fw  Prim. Op
Port   St   Cost    Cost   Role Tx  Port  Cnx  Desig Bridge ID
-----+----+-------+-------+----+---+-----+---+---------------------
 1/1  FORW  200000       0 MSTR   1  1/1  PTP 8002-00:d0:95:57:3a:9e
 1/2   DIS       0       0  DIS   0  1/2   NS 0000-00:00:00:00:00:00
 1/3   DIS       0       0  DIS   0  1/3   NS 0000-00:00:00:00:00:00
 1/4   DIS       0       0  DIS   0  1/4   NS 0000-00:00:00:00:00:00
 1/5   DIS       0       0  DIS   0  1/5   NS 0000-00:00:00:00:00:00
 1/6   DIS       0       0  DIS   0  1/6   NS 0000-00:00:00:00:00:00
 1/7   DIS       0       0  DIS   0  1/7   NS 0000-00:00:00:00:00:00
 1/8   DIS       0       0  DIS   0  1/8   NS 0000-00:00:00:00:00:00
 1/9   DIS       0       0  DIS   0  1/9   NS 0000-00:00:00:00:00:00
 1/10  DIS       0       0  DIS   0  1/10  NS 0000-00:00:00:00:00:00
 1/11  DIS       0       0  DIS   0  1/11  NS 0000-00:00:00:00:00:00
 1/12  DIS       0       0  DIS   0  1/12  NS 0000-00:00:00:00:00:00
 1/13  DIS       0       0  DIS   0  1/13  NS 0000-00:00:00:00:00:00
 1/14  DIS       0       0  DIS   0  1/14  NS 0000-00:00:00:00:00:00
 1/15  DIS       0       0  DIS   0  1/15  NS 0000-00:00:00:00:00:00
 1/16  DIS       0       0  DIS   0  1/16  NS 0000-00:00:00:00:00:00
 1/17  DIS       0       0  DIS   0  1/17  NS 0000-00:00:00:00:00:00
 1/18  DIS       0       0  DIS   0  1/18  NS 0000-00:00:00:00:00:00
 1/19  DIS       0       0  DIS   0  1/19  NS 0000-00:00:00:00:00:00
 1/20  DIS       0       0  DIS   0  1/20  NS 0000-00:00:00:00:00:00
 1/21  DIS       0       0  DIS   0  1/21  NS 0000-00:00:00:00:00:00
 1/22  DIS       0       0  DIS   0  1/22  NS 0000-00:00:00:00:00:00
 1/23  DIS       0       0  DIS   0  1/23  NS 0000-00:00:00:00:00:00
 1/24  DIS       0       0  DIS   0  1/24  NS 0000-00:00:00:00:00:00
 5/1   DIS       0       0  DIS   0  5/1   NS 0000-00:00:00:00:00:00
 5/2   DIS       0       0  DIS   0  5/2   NS 0000-00:00:00:00:00:00

-> show spantree msti 2 ports active
Spanning Tree Port Summary for Msti 2
      Oper  Path   Desig        Fw  Prim. Op
Port   St   Cost    Cost   Role Tx  Port  Cnx  Desig Bridge ID
-----+----+-------+-------+----+---+-----+---+---------------------
 1/1  FORW  200000       0 MSTR   1  1/1  PTP 8002-00:d0:95:57:3a:9e
```

output definitions

Msti	The 802.1S Multiple Spanning Tree Instance (MSTI) number. MSTI 0 represents the CIST. Configured through the **bridge msti** command.
Port	The slot number for the module and the physical port number or a logical port. If the slot number is 0, then the port number refers to a link aggregate logical port number (e.g., 0/31).
Oper St	The port operational state as defined by application of the Spanning Tree Protocol. Possible port operational states include: disabled, blocking, listening, learning, and forwarding.
Path Cost	The contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops. Configured through the **bridge msti slot/port path cost** command.

output definitions (continued)

Desig Cost	The path cost of the Designated Port of the segment connected to this port. If this is the root bridge or the Spanning Tree status of the port is administratively disabled, this value is 0.
Role	The role of the port for this Spanning Tree instance. Possible port roles are: **root, designated, alternate, master**, and **backup**.
Fw Tx	Forward Transmission. The number of times the port has transitioned from the learning state to the forwarding state.
Prim. Port	The slot number for the module and the physical port number on that module for the primary port associated with this Spanning Tree instance. This information is only available if the port role is backup.
Op Cnx	Operational connection type: **PTP, NPT**, **NS** (nonsignificant), or **EDG.** Shows the current operational state of the port's connection type. See the **bridge slot/port connection** command on page 16-86 for more information.
Desig Bridge ID	The bridge identifier for the designated bridge for this port's segment.

```
-> show spantree msti 2 ports configured
Spanning Tree Port Admin Configuration for Msti 2
      Port  Adm Man. Config  Adm  OS8800
Port  Pri   St. Mode   Cost  Cnx  10G Opt.
-----+----+----+----+-------+----+--------
 1/1     7  ENA  No        0  AUT    DIS
 1/2     7  ENA  No        0  AUT    DIS
 1/3     7  ENA  No        0  AUT    DIS
 1/4     7  ENA  No        0  AUT    DIS
 1/5     7  ENA  No        0  AUT    DIS
 1/6     7  ENA  No        0  AUT    DIS
 1/7     7  ENA  No        0  AUT    DIS
 1/8     7  ENA  No        0  AUT    DIS
 1/9     7  ENA  No        0  AUT    DIS
 1/10    7  ENA  No        0  AUT    DIS
 1/11    7  ENA  No        0  AUT    DIS
 1/12    7  ENA  No        0  AUT    DIS
```

output definitions

Port	The slot number for the module and the physical port number or a logical port. If the slot number is 0, then the port number refers to a link aggregate logical port number (e.g., 0/31).
Port Pri	The Spanning Tree priority for the port (0–15). The lower the number, the higher the priority. Configured through the **bridge msti slot/port priority** command.
Adm St	The Spanning Tree administrative status of the port: **enabled** or **disabled**. Configured through the **bridge slot/port** command to enable or disable Spanning Tree on a port.
Man. Mode	The manual mode setting for the port: **yes** indicates that the blocking or forwarding state of the port was manually set and the port does not participate in the Spanning Tree Algorithm; **no** indicates that the Spanning Tree Algorithm is managing the port state. Configured through the **bridge slot/port mode** command.

output definitions (continued)

Config Cost	The configured path cost value for this port. Configured through the **bridge msti slot/port path cost** command.
Adm Cnx	Administrative connection type: **PTP, NPT, AUT**, or **EDG.** Configured through the **bridge slot/port connection** command.
OS8800 10G Opt.	Indicates whether the 10 GB port interoperability status is enabled (**ENA**) or disabled (**DIS**).

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

show spantree ports	Implicit command for displaying Spanning Tree port information for the flat mode CIST instance or a 1x1 mode VLAN instance.
show spantree cist ports	Explicit command for displaying Spanning Tree port information for a CIST instance when the switch is operating in the 1x1 or flat Spanning Tree mode.
show spantree 1x1 ports	Explicit command for displaying Spanning Tree port information for a VLAN when the switch is operating in the 1x1 or flat Spanning Tree mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortPriority
   vStpInsPortState
   vStpInsPortEnable
   vStpInsPortPathCost
   vStpInsPortDesignatedCost
   vStpInsPortDesignatedBridge
   vStpInsPortForwardTransitions
   vStpInsPortManualMode
   vStpInsPortRole
   vStpInsPrimaryPortNumber
   vStpInsPortAdminConnectionType
   vStpInsPortOperConnectionType
```

show spantree 1x1 ports

Displays Spanning Tree port information for a 1x1 mode VLAN instance.

show spantree 1x1 [*vid*] ports [forwarding | blocking | active | configured]

Syntax Definitions

vid	An existing VLAN ID number (1-4094).
forwarding	Displays Spanning Tree operational port parameters for ports that are forwarding for the CIST instance.
blocking	Displays Spanning Tree operational port parameters for ports that are blocked for the CIST instance.
active	Displays a list of active ports associated with the specified instance.
configured	Displays Spanning Tree administrative port parameters for the CIST instance.

Defaults

parameter	default
vid	all VLAN instances
forwarding | blocking | active | configured	all ports

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If a *vid* number is *not* specified, this command displays the Spanning Tree port operational status, path cost, and role values for all VLAN instances.
- This is an explicit Spanning Tree command that displays Spanning Tree port information for a VLAN instance regardless of which mode (1x1 or flat) is active on the switch.
- Note that minimal information is displayed when this command is used in the flat mode, as VLAN instances are not active in this mode.
- The **configured** keyword is only available when an instance number is specified with this command. In addition, this keyword cannot be used in combination with either the **forwarding** or **blocking** keywords.

Examples

```
-> show spantree 1x1 ports
 Vlan  Port Oper Status  Path Cost  Role
-----+-----+-----------+---------+-----
    1  1/1       DIS           0    DIS
    1  1/2       DIS           0    DIS
    1  1/3       DIS           0    DIS
    1  1/4       DIS           0    DIS
    1  1/5       DIS           0    DIS
    1  1/6       DIS           0    DIS
    1  1/7       DIS           0    DIS
    1  1/8       DIS           0    DIS
    1  1/9       DIS           0    DIS
    1  1/10      DIS           0    DIS
    1  1/11      DIS           0    DIS
    1  1/12     FORW          19    DIS

-> show spantree 1x1 1 ports
Spanning Tree Port Summary for Vlan 1
      Oper  Path   Desig        Fw  Prim. Op
Port   St   Cost    Cost   Role Tx  Port  Cnx  Desig Bridge ID
-----+----+-------+-------+----+---+-----+---+---------------------
 1/1   DIS       0       0  DIS   0  1/1   NS 0000-00:00:00:00:00:00
 1/2   DIS       0       0  DIS   0  1/2   NS 0000-00:00:00:00:00:00
 1/3   DIS       0       0  DIS   0  1/3   NS 0000-00:00:00:00:00:00
 1/4   DIS       0       0  DIS   0  1/4   NS 0000-00:00:00:00:00:00
 1/5   DIS       0       0  DIS   0  1/5   NS 0000-00:00:00:00:00:00
 1/6   DIS       0       0  DIS   0  1/6   NS 0000-00:00:00:00:00:00
 1/7   DIS       0       0  DIS   0  1/7   NS 0000-00:00:00:00:00:00
 1/8   DIS       0       0  DIS   0  1/8   NS 0000-00:00:00:00:00:00
 1/9   DIS       0       0  DIS   0  1/9   NS 0000-00:00:00:00:00:00
 1/10  DIS       0       0  DIS   0  1/10  NS 0000-00:00:00:00:00:00
 1/11  DIS       0       0  DIS   0  1/11  NS 0000-00:00:00:00:00:00
 1/12 FORW      19       0  DIS   1  1/12 PTP 0001-00:d0:95:6a:79:50

-> show spantree 1x1 1 ports active
Spanning Tree Port Summary for Vlan 1
      Oper  Path   Desig        Fw  Prim. Op
Port   St   Cost    Cost   Role Tx  Port  Cnx  Desig Bridge ID
-----+----+-------+-------+----+---+-----+---+---------------------
 1/12 FORW      19       0  DIS   1  1/12 PTP 0001-00:d0:95:6a:79:50
```

output definitions

Vlan	The VLAN ID associated with the VLAN Spanning Tree instance. Configured through the **vlan** commands
Port	The slot number for the module and the physical port number or a logical port. If the slot number is 0, then the port number refers to a link aggregate logical port number (e.g., 0/31).
Oper St	The port operational state as defined by application of the Spanning Tree Protocol. Possible port operational states include: disabled, blocking, listening, learning, and forwarding.

output definitions (continued)

Path Cost	The contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops. Configured through the **bridge 1x1 slot/port path cost** command.
Desig Cost	The path cost of the Designated Port of the segment connected to this port. If this is the root bridge or the Spanning Tree status of the port is administratively disabled, this value is 0.
Role	The role of the port for this Spanning Tree instance. Possible port roles are: **root, designated, alternate, master**, and **backup**.
Fw Tx	Forward Transmission. The number of times the port has transitioned from the learning state to the forwarding state.
Prim. Port	The slot number for the module and the physical port number on that module for the primary port associated with this Spanning Tree instance. This information is only available if the port role is backup.
Op Cnx	Operational connection type: **PTP, NPT**, **NS** (nonsignificant), or **EDG.** Shows the current operational state of the port's connection type. See the **bridge slot/port connection** command on page 16-86 for more information.
Desig Bridge ID	The bridge identifier for the designated bridge for this port's segment.

```
-> show spantree 1x1 1 ports configured
Spanning Tree Port Admin Configuration for Vlan 1
Port  Adm Man. Config  Adm  OS8800
Port  Pri   St. Mode   Cost  Cnx  10G Opt.
-----+----+----+----+-------+----+--------
 1/1     7  ENA  No        0  AUT    DIS
 1/2     7  ENA  No        0  AUT    DIS
 1/3     7  ENA  No        0  AUT    DIS
 1/4     7  ENA  No        0  AUT    DIS
 1/5     7  ENA  No        0  AUT    DIS
 1/6     7  ENA  No        0  AUT    DIS
 1/7     7  ENA  No        0  AUT    DIS
 1/8     7  ENA  No        0  AUT    DIS
 1/9     7  ENA  No        0  AUT    DIS
 1/10    7  ENA  No        0  AUT    DIS
 1/11    7  ENA  No        0  AUT    DIS
 1/12    7  ENA  No        0  AUT    DIS
```

output definitions

Port	The slot number for the module and the physical port number or a logical port. If the slot number is 0, then the port number refers to a link aggregate logical port number (e.g., 0/31).
Port Pri	The Spanning Tree priority for the port (0–15). The lower the number, the higher the priority. Configured through the **bridge 1x1 slot/port priority** command.
Adm St	The Spanning Tree administrative status of the port: **enabled** or **disabled**. Configured through the **bridge slot/port** command to enable or disable Spanning Tree on a port.

output definitions (continued)

Man. Mode	The manual mode setting for the port: **yes** indicates that the blocking or forwarding state of the port was manually set and the port does not participate in the Spanning Tree Algorithm; **no** indicates that the Spanning Tree Algorithm is managing the port state. Configured through the **bridge slot/port mode** command.
Config Cost	The configured path cost value for this port. Configured through the **bridge 1x1 slot/port path cost** command.
Adm Cnx	Administrative connection type: **PTP, NPT, AUT**, or **EDG.** Configured through the **bridge slot/port connection** command.
OS8800 10G Opt.	Indicates whether the 10 GB port interoperability status is enabled (**ENA**) or disabled (**DIS**).

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

show spantree ports	Implicit command for displaying Spanning Tree port information for the flat mode CIST instance or a 1x1 mode VLAN instance.
show spantree cist ports	Explicit command for displaying Spanning Tree port information for a CIST instance when the switch is operating in the 1x1 or flat Spanning Tree mode.
show spantree msti ports	Explicit command for displaying Spanning Tree port information for an MSTI when the switch is operating in the 1x1 or flat Spanning Tree mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortPriority
   vStpInsPortState
   vStpInsPortEnable
   vStpInsPortPathCost
   vStpInsPortDesignatedCost
   vStpInsPortDesignatedBridge
   vStpInsPortForwardTransitions
   vStpInsPortManualMode
   vStpInsPortRole
   vStpInsPrimaryPortNumber
   vStpInsPortAdminConnectionType
   vStpInsPortOperConnectionType
```

show spantree mst region

Displays the Multiple Spanning Tree (MST) region information for the switch.

show spantree mst region

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Three MST region attributes (configuration name, revision level, and configuration digest) define an MST region as required by the IEEE 802.1S standard. Switches that share the same values for these attributes are all considered part of the same region. Currently each switch can belong to one MST region at a time.
- This command is available when the switch is operating in either the 1x1 or flat Spanning Tree mode.

Examples

```
-> show spantree mst region
Configuration Name : Region 1
Revision Level : 0
Configuration Digest : 0xac36177f 50283cd4 b83821d8 ab26de62
Revision Max hops : 20
Cist Instance Number : 0
```

output definitions

Configuration Name	An alphanumeric string up to 32 characters that identifies the name of the MST region. Use the **bridge mst region name** command to define this value.
Revision Level	A numeric value (0–65535) that identifies the MST region revision level for the switch.
Configuration Digest	An MST region identifier consisting of a 16 octet hex value (as per the IEEE 802.1S standard) that represents all defined MSTIs and their associated VLAN ranges. Use the **bridge msti** and **bridge msti vlan** commands to define VLAN to MSTI associations.

output definitions (continued)

Revision Max hops	The number of maximum hops authorized for region information. Configured through the **bridge mst region max hops** command.
Cist Instance Number	The number of the CIST instance, which is currently zero as there is only one region per switch. Therefore, only one CIST exists per switch Note that this instance is also known as the flat mode instance and is known as bridge 1 when using STP or RSTP.

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

show spantree msti vlan-map	Displays the range of VLANs associated to the specified MSTI.
show spantree cist vlan-map	Displays the range of VLANs associated to the CIST instance.
show spantree map-msti	Displays the MSTI that is associated to the specified VLAN

MIB Objects

```
vStpMstRegionTable
   vStpMstRegionNumber
   vStpMstRegionConfigDigest
   vStpMstRegionConfigName
   vStpMstRegionConfigRevisionLevel
   vStpMstRegionCistInstanceNumber
   vStpMstRegionMaxHops
```

show spantree msti vlan-map

Displays the range of VLANs associated with the specified Multiple Spanning Tree Instance (MSTI).

show spantree mst [*msti_id***] vlan-map**

Syntax Definitions

msti_id	An existing MSTI ID number (0–4094).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If an *msti_id* is not specified, then the VLAN to MSTI mapping for all defined MSTIs is displayed.
- This command is available when the switch is operating in either the 1x1 or flat Spanning Tree mode.
- Initially all VLANs are associated with the flat mode CIST instance (also known as MSTI 0).

Examples

```
-> show spantree msti vlan-map
 Spanning Tree Msti/Cist Vlan map
-----------------------------------

 Cist
 Name                :
 VLAN list           : 1-9,14-4094

 Msti 1
 Name                :
 VLAN list           : 10-11

 Msti 2
 Name                :
 VLAN list           : 12-13

-> show spantree msti 2 vlan-map
 Spanning Tree Msti Vlan map
-----------------------------

 Msti 2
 Name                :
 VLAN list           : 12-13
```

output definitions

Cist Instance	Identifies MSTI VLAN mapping information for the CIST instance.
Msti	The MSTI ID number that identifies an association between a Spanning Tree instance and a range of VLANs.
Name	An alphanumeric value that identifies an MSTI name. Use the **bridge msti** command to define an MSTI name.
VLAN list	The range of VLAN IDs that are associated with this MSTI.

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

show spantree mst region	Displays the MST region information for the switch.
show spantree cist vlan-map	Displays the range of VLANs associated to the CIST instance.
show spantree map-msti	Displays the MSTI that is associated to the specified VLAN

MIB Objects

```
vStpMstInstanceTable
   vStpMstInstanceNumber
   vStpMstInstanceName
   vStpMstInstanceVlanBitmapState
```

show spantree cist vlan-map

Displays the range of VLANs associated with the flat mode Common and Internal Spanning Tree (CIST) instance.

show spantree cist vlan-map

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command is available when the switch is operating in either the 1x1 or flat Spanning Tree mode.
- Initially all VLANs are associated with the flat mode CIST instance 0 (also known as MSTI 0).

Examples

```
-> show spantree cist vlan-map
 Spanning Tree Cist Vlan map
----------------------------

 Cist
 Name           :
 VLAN list      : 1-9,14-4094
```

output definitions

Name	An alphanumeric value that identifies the name of the CIST. Use the **bridge msti** command to define a name for this instance.
VLAN list	The range of VLAN IDs that are associated with the CIST instance.

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

show spantree mst region	Displays the MST region information for the switch.
show spantree msti vlan-map	Displays the range of VLANs associated to the specified MSTI.
show spantree map-msti	Displays the MSTI that is associated to the specified VLAN

MIB Objects

```
vStpMstInstanceTable
   vStpMstInstanceNumber
   vStpMstInstanceName
   vStpMstInstanceVlanBitmapState
```

show spantree map-msti

Displays the Multiple Spanning Tree Instance (MSTI) that is associated to the specified VLAN.

show spantree mst *vid* **vlan-map**

Syntax Definitions

vid	An existing VLAN ID number (1–4094).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command is available when the switch is operating in either the 1x1 or flat Spanning Tree mode.
- Initially all VLANs are associated with the flat mode CIST instance (also known as MSTI 0).

Examples

```
-> show spantree 200 map-msti
 Vlan   Msti/Cist(0)
------+--------------------------
   200     0
```

Release History

Release 5.1.6 and 5.3.1; command was introduced.

Related Commands

show spantree mst region	Displays the MST region information for the switch.
show spantree msti vlan-map	Displays the range of VLANs associated to the specified MSTI.
show spantree cist vlan-map	Displays the range of VLANs associated to the CIST instance.

MIB Objects

```
vStpMstVlanAssignmentTable
   vStpMstVlanAssignmentVlanNumber
   vStpMstVlanAssignmentMstiNumber
```

show spantree mst port

Displays a summary of Spanning Tree connection information and instance associations for the specified port or a link aggregate of ports.

show spantree mst port {*slot/port* **|** *logical_port***}**

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
logical_port	The Link aggregate ID number (0–31).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command is only available when the switch is running in the flat Spanning Tree mode.
- The *logical_ port* value range for link aggregate ID numbers is 0–29 on the OmniSwitch 6600 and 0–15 on the OmniSwitch 8800.
- Note that MST 0 also represents the flat mode CIST instance, which all ports are associated with when the switch is running in the flat Spanning Tree mode.

Examples

```
-> bridge mode flat
-> show spantree mst port 1/10
MST parameters for interface 1/10:
  Conection Type:  NS
  Edge Port: YES
  Boundary Port: YES

 MST |  Role  | State | Pth Cst | Vlans
-----------------------------------------------------
 0       DIS      DIS          0   200
 2       DIS      DIS          0

-> show spantree mst port 1/1
MST parameters for interface 1/1 :
  Conection Type: PTP
  Edge Port: NO
  Boundary Port: YES

 MST |  Role  | State | Pth Cst | Vlans
-----------------------------------------------------
 0      ROOT     FORW         19   1
```

```
-> bridge mode 1x1
-> show spantree mst port 1/10
Current STP mode is 1x1, MSTI instances are inactive
```

output definitions

Connection Type	Operational connection type: **PTP, NPT**, **NS** (nonsignificant) or **EDG.** Shows the current operational state of the port's connection type. See the **bridge slot/port connection** command on page 16-86 for more information.
Edge Port	Indicates whether or not the port is an edge port (**YES** or **NO**).
Boundary Port	Indicates whether or not the port is a boundary port (**YES** or **NO**). A boundary port connects an MST bridge to a LAN that belongs to a different MST region.
MST	The Multiple Spanning Tree Instance (MSTI) number that is associated with this port.
Role	The role of the port for this Spanning Tree instance. Possible port roles are: **root, designated, alternate, master**, and **backup**.
State	The port operational state as defined by application of the Spanning Tree Protocol. Possible port operational states include: disabled, blocking, listening, learning, and forwarding.
Pth Cst	The contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops.
Vlans	The VLAN ID of the default VLAN for the port.

17 Source Learning Commands

Source Learning is responsible for creating, updating, and deleting source and destination MAC Address entries in the MAC Address Table. This chapter includes descriptions of Source Learning commands used to create or delete static MAC addresses, define the aging time value for static and dynamically learned MAC addresses, and display MAC Address Table entries and statistics.

MIB information for Source Learning commands is as follows:

Filename: AlcatelInd1MacAddress.mib
Module: ALCATEL-IND1-MAC-ADDRESS-MIB

A summary of the available commands is listed here:

mac-address-table
mac-address-table static-multicast
mac-address-table aging-time
show mac-address-table
show mac-address-table static-multicast
show mac-address-table count
show mac-address-table aging-time

mac-address-table

Configures a destination unicast MAC address. The configured (static) MAC address is assigned to a non-mobile switch port or link aggregate ID and VLAN. Packets received on ports associated with the specified VLAN that contain a destination MAC address that matches the static MAC address are forwarded to the specified port. Static destination MAC addresses are maintained in the Source Learning MAC address table.

mac-address-table [permanent | reset | timeout] *mac_address* **{***slot/port* | **linkagg** *link_agg***}** *vid* **[bridging | filtering]**

no mac-address-table [permanent | reset | timeout | learned] *mac_address* **{***slot/port* | **linkagg** *link_agg***}** *vid*

Syntax Definitions

permanent	Defines a permanent static MAC Address that is not removed when the switch reboots.
reset	Defines a static MAC Address that is removed after the next switch reboot.
timeout	Defines a static MAC Address that is deleted if the MAC ages beyond the aging timer value.
learned	Specifies that the MAC address is a dynamically learned address.
mac_address	Enter the destination MAC Address to add to the MAC Address Table (e.g., 00:00:39:59:f1:0c).
slot/port	Enter the slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
link_agg	Enter a link aggregate ID number (0–31). See Chapter 13, "Link Aggregation Commands."
vid	VLAN ID number (1–4094).
bridging	Specifies that all packets to or from this MAC address are bridged.
filtering	Specifies that all packets to or from this MAC address are dropped.

Defaults

parameter	default
permanent | reset | timeout	**permanent**
bridging | filtering	**bridging**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no mac-address-table** command to remove a MAC address from the Source Learning MAC Address Table.
- The *link_agg* value range for link aggregate ID numbers is 0–29 on the OmniSwitch 6600 Family and 0–15 on the OmniSwitch 8800.
- The specified slot/port or link aggregate ID must already belong to the specified VLAN. Use the **vlan port default** command to assign a port or link aggregate ID to a VLAN before you configure the static MAC address. Only traffic from other ports associated with the same VLAN is directed to the static MAC address slot/port.
- Select the **filtering** parameter to set up a denial of service to block potential hostile attacks. Traffic sent to or from a filtered MAC address is dropped. Select the **bridging** parameter for regular traffic flow to or from the MAC address.
- If a packet received on a port associated with the same VLAN contains a source address that matches a static MAC address, the packet is discarded. On an OmniSwitch 6600 Family, however, the packet's source MAC address is still learned on the receiving port but with a filtering operational status. The same source address on different ports within the same VLAN is not supported.
- Static MACs are not supported on mobile ports.
- Only static MAC address entries with a **permanent** management status are captured when a snapshot of the switch's running configuration is taken.
- Use the **mac-address-table aging-time** command (see page 17-7) to set the aging time value for all static and dynamically learned MAC addresses. This is the value applied to static MAC addresses defined using the **mac-address-table timeout** form of this command.

Examples

```
-> mac-address-table permanent 00:00:39:59:f1:0c 4/2 355
-> mac-address-table reset 00:00:40:5a:f2:0d 8/1 456
-> mac-address-table timeout 00:00:41:5b:f3:0e 2/16 254 filtering
-> no mac-address-table
-> no mac-address-table 5/1 755
-> no mac-address-table permanent
```

Release History

Release 5.1; command was introduced.

Related Commands

mac-address-table aging-time	Configures aging time, in seconds, for static and dynamically learned MAC addresses.
show mac-address-table	Displays Source Learning MAC Address Table information.
show mac-address-table count	Displays Source Learning MAC Address Table statistics.
show mac-address-table aging-time	Displays the current aging time value for the Source Learning MAC Address Table.

MIB Objects

```
slMacAddressTable
   slMacAddress
   slMacAddressManagement
   slMacAddressDisposition
```

mac-address-table static-multicast

Configures a static multicast MAC address and assigns the address to one or more egress ports. Packets received on ports associated with the specified VLAN that contain a destination MAC address that matches the static multicast address are forwarded to the specified egress ports. Static destination multicast MAC addresses are maintained in the Source Learning MAC address table.

mac-address-table static-multicast *multicast_address* **{***slot1/port1***[-***port1a***] [***slot2/port2***[-***port2a***]...]** | **linkagg** *link_agg***}** *vid*

no mac-address-table static-multicast [*multicast_address* **{***slot1/port1***[-***port1a***] [***slot2/port2***[-***port2a***]...]** | **linkagg** *link_agg***}** *vid***]**

Syntax Definitions

multicast_address	Enter the destination multicast MAC Address to add to the MAC Address Table (e.g., 01:00:39:59:f1:0c).
*slot1/port1***[-***port1a***]**	The egress slot and port combination that is assigned to the static multicast MAC address. You may enter multiple ports and port ranges.
*slot2/port2***[-***port2a***]**	Additional egress slot and port combinations may be assigned to the static multicast MAC address. You may enter multiple ports and port ranges.
link_agg	Enter a link aggregate ID number (0–29). See Chapter 13, "Link Aggregation Commands."
vid	VLAN ID number (1–4094).

Defaults

N/A

Platforms Supported

OmniSwitch 6600

Usage Guidelines

- Use the **no mac-address-table static-multicast** command to remove a static multicast MAC address from the Source Learning MAC Address Table. Note that if no parameters are specified with this form of the command, then all static multicast addresses are removed.
- Note that multicast MAC addresses begin with **01**. This value is a prefix that identifies a MAC address as a multicast MAC address. If this prefix is not present, then the address is treated as a regular MAC address and not allowed when using the **mac-address-table static-multicast** command.
- The configured (static) multicast MAC address is assigned to a non-mobile switch port or link aggregate ID and VLAN. Static multicast MACs are not supported on mobile ports.
- The specified slot/port or link aggregate ID must already belong to the specified VLAN. Use the **vlan port default** command to assign a port or link aggregate ID to a VLAN before you configure the static MAC address. Only traffic from other ports associated with the same VLAN is directed to the static multicast MAC address slot/port.

- If a packet received on a port associated with the same VLAN contains a source address that matches a static multicast MAC address, the packet's source MAC address is learned on the receiving port but with a filtering operational status. The same source address on different ports within the same VLAN is not supported.

Examples

```
-> mac-address-table static-multicast 02:00:39:59:f1:0c 4/2 355
-> mac-address-table static-multicast 01:00:00:3a:44:11 1/12-24 255
-> mac-address-table static-multicast 03:00:00:3a:44:12 1/10 2/1-6 3/1-8 1500
-> mac-address-table static-multicast 04:00:00:3a:44:13 linkagg 10 455
-> no mac-address-table static-multicast 03:00:00:3a:44:12 1/10 1500
-> no mac-address-table static-multicast 04:00:00:3a:44:13 linkagg 10 455
-> no mac-address-table static-multicast
```

Release History

Release 5.4.1; command was introduced.

Related Commands

show mac-address-table	Displays Source Learning MAC Address Table information.
show mac-address-table static-multicast	Displays a list of static multicast MAC addresses that are configured in the Source Learning MAC Address Table.
show mac-address-table count	Displays Source Learning MAC Address Table statistics.

MIB Objects

```
slMacAddressTable
   slMacAddress
   slMacAddressManagement
   slMacAddressDisposition
```

mac-address-table aging-time

Configures aging time, in seconds, for static and dynamically learned MAC addresses. When a MAC address has aged beyond the aging-time value, the MAC address is discarded.

mac-address-table aging-time *seconds* **[vlan** *vid***]**

no mac-address-table aging-time [vlan *vid***]**

Syntax Definitions

seconds	Aging time value (in seconds). Do not use commas in value. The range is 10—1000000.
vid	VLAN ID number. The range is 1–4094.

Defaults

By default, the aging time is set to 300 seconds.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of this command to set the aging-time back to the default value of 300 seconds.
- If a *vid* is not specified, then the aging time applies to all VLANs configured on the switch.
- If the **timeout** parameter is not specified when using the **mac-address-table** command (see page 17-2) to configure a static MAC address, then the aging time value is not applied to the static MAC address.
- When using this command in a switch configuration file (e.g., **boot.cfg**), include the VLAN ID for each entry of the command. If a VLAN ID is not specified, only the aging time for VLAN 1 is changed when the configuration file is applied to the switch.
- The MAC address table aging time is also used as the timeout value for the Address Resolution Protocol (ARP) table. This timeout value determines how long the switch retains dynamically learned ARP table entries.

Examples

```
-> mac-address-table aging-time 1200
-> mac-address-table aging-time 60 vlan 255
-> no mac-address-table aging-time
-> no mac-address-table aging-time vlan 355
```

Release History

Release 5.1; command was introduced.

Related Commands

mac-address-table	Configures a static destination Unicast MAC address for a VLAN bridge.
show mac-address-table	Displays Source Learning MAC Address Table information.
show mac-address-table count	Displays Source Learning MAC Address Table statistics.
show mac-address-table aging-time	Displays the current aging time value for the Source Learning MAC Address Table.

MIB Objects

```
slMacAddressAgingTable
   slMacAgingValue
```

show mac-address-table

Displays Source Learning MAC Address Table information.

show mac-address-table [permanent | reset | timeout | learned] [*mac_address***] [slot** *slot* **|** *slot/port***] [linkagg** *link_agg***] [***vid***]**

Syntax Definitions

permanent	Display static MAC addresses with a permanent status.
reset	Display static MAC addresses with a reset status.
timeout	Display static MAC addresses with a timeout status.
learned	Display dynamically learned MAC addresses.
mac_address	Enter a MAC Address (e.g., 00:00:39:59:f1:0c).
slot	Enter the slot number for a module to specify that the command should include all ports on that module (e.g., 6 specifies all ports on the module found in slot 6 of the switch chassis).
slot/port	Enter the slot number and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
link_agg	Enter a link aggregate ID number (0–31). See Chapter 13, "Link Aggregation Commands."
vid	VLAN ID number (1–4094).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If no parameters are specified, then information is displayed for all MAC addresses contained in the table.
- The *link_agg* value range for link aggregate ID numbers is 0–29 on the OmniSwitch 6600 Family and 0–15 on the OmniSwitch 8800.
- If a static MAC address is configured on a port link that is down or disabled, an asterisk appears to the left of the MAC address in the **show mac-address-table** command display. The asterisk indicates that this is an invalid MAC address. When the port link comes up, however, the MAC address is then considered valid and the asterisk no longer appears next to the address in the display.

Examples

```
-> show mac-address-table
Legend: Mac Address: * = address not valid

   Vlan      Mac Address          Type       Protocol    Operation    Interface
  ------+------------------+-------------+-----------+------------+-----------
     1   00:00:00:00:00:01     learned        0800        bridging      8/ 1
     1   00:d0:95:6a:73:9a     learned        aaaa0003    bridging     10/23
Total number of Valid MAC addresses above = 2
```

output definitions

VLAN	Vlan ID number associated with the MAC address and slot/port.
Mac Address	MAC address that is currently learned or statically assigned.
Type	MAC address management status: **permanent, reset, timeout,** or **learned**. Use the **mac-address-table** command on page 17-2 to configure the management status for a static MAC address.
Protocol	Protocol type for the MAC address entry.
Operation	The disposition of the MAC address: **bridging** (default) or **filtering**. Use the **mac-address-table** command on page 17-2 to configure the disposition for a static MAC address.
Interface	The slot number for the module and the physical port number on that module that is associated with the static or dynamically learned MAC address. If the interface is a link aggregate ID, zero is displayed as the slot number (e.g., 0/29).

Release History

Release 5.1; command was introduced.

Related Commands

show mac-address-table count	Displays Source Learning MAC Address Table statistics.
show mac-address-table aging-time	Displays the current aging time value for the Source Learning MAC Address Table.

MIB Objects

```
slMacAddressTable
   slMacAddress
   slMacAddressManagement
   slMacAddressDisposition
   slMacAddressProtocol
```

show mac-address-table static-multicast

Displays the static multicast MAC address configuration for the switch.

show mac-address-table static-multicast [*multicast_address***] [slot** *slot* **|** *slot/port***] [linkagg** *link_agg***] [***vid***]**

Syntax Definitions

multicast_address	Enter a multicast MAC Address (e.g., 01:00:39:59:f1:0c).
slot	Enter the slot number for a module to specify that the command should include all ports on that module (e.g., 6 specifies all ports on the module found in slot 6 of the switch chassis).
slot/port	Enter the slot number and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
link_agg	Enter a link aggregate ID number (0–29). See Chapter 13, "Link Aggregation Commands."
vid	VLAN ID number (1–4094).

Defaults

By default information is displayed for all static multicast MAC addresses contained in the MAC address table.

Platforms Supported

OmniSwitch 6600

Usage Guidelines

- Note that if a static multicast MAC address is configured on a port link that is down or disabled, the configured multicast address does not appear in the **show mac-address-table static-multicast** command display.
- The **show mac-address-table** command display, however, includes all static multicast addresses regardless of whether or not the port assigned to the address is up or down. See the second example below.
- When the **show mac-address-table** command is used to display MAC addresses known to the switch, an asterisk appears to the left of all static MAC addresses that are configured on a port link that is down or disabled. The asterisk indicates that this is an invalid MAC address. When the port link comes up, however, the MAC address is then considered valid and the asterisk no longer appears next to the address in the display.

Examples

```
-> show mac-address-table static-multicast
Legend: Mac Address: * = address not valid

   Vlan      Mac Address          Type       Protocol    Operation    Interface
  ------+-----------------+---------------+-----------+------------+-----------
     1   01:00:00:00:02:02  static multicast        0     bridging      4/16
     1   01:00:00:00:02:02  static multicast        0     bridging      0/1
Total number of Valid MAC addresses above = 3

-> show mac-address-table
Legend: Mac Address: * = address not valid

   Vlan      Mac Address          Type       Protocol    Operation    Interface
  ------+-----------------+---------------+-----------+------------+-----------
     1   00:00:00:00:01:01   permanent               0     bridging      4/1
   * 1   01:00:00:00:00:01   static multicast        0     bridging      4/8
     1   01:00:00:00:02:02   static multicast        0     bridging      4/16
     1   01:00:00:00:02:02   static multicast        0     bridging      0/1
Total number of Valid MAC addresses above = 4
```

output definitions

VLAN	Vlan ID number associated with the static multicast address.
Mac Address	The multicast MAC address that is statically assigned to the VLAN and slot/port.
Type	Indicates the MAC address is a **static multicast** address. This type of address is configured through the **mac-address-table static-multicast** command.
Protocol	Protocol type for the MAC address entry.
Operation	The disposition of the MAC address: **bridging** (default) or **filtering**. Note that this value is always set to **bridging** for static multicast addresses.
Interface	The slot number for the module and the physical port number on that module that is associated with the static multicast MAC address. If the interface is a link aggregate ID, zero is displayed as the slot number (e.g., 0/29).

Release History

Release 5.4.1; command was introduced.

Related Commands

show mac-address-table count	Displays Source Learning MAC Address Table statistics.
show mac-address-table	Displays Source Learning MAC Address Table information.

MIB Objects

```
slMacAddressTable
   slMacAddress
   slMacAddressManagement
   slMacAddressDisposition
   slMacAddressProtocol
```

show mac-address-table count

Displays Source Learning MAC Address Table statistics.

show mac-address-table count [*mac_address***] [slot** *slot* | *slot/port***] [linkagg** *link_agg***] [***vid***]**

Syntax Definitions

mac_address	MAC Address (e.g., 00:00:39:59:f1:0c).
slot | *slot/port*	Slot number for the module or the slot number and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
link_agg	Enter a link aggregate ID number (0–31). See Chapter 13, "Link Aggregation Commands."
vid	VLAN ID number (1–4094).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If no parameters are specified, then statistics are displayed for all MAC addresses contained in the table.
- To display statistics for all ports on one slot, specify only the slot number for the **slot** parameter value.
- Note that if a static multicast MAC address is configured on a port link that is down or disabled, the multicast address is not counted.

Examples

```
-> show mac-address-table count
Mac Address Table count:
Permanent Address Count             = 1
DeleteOnReset Address Count         = 0
DeleteOnTimeout Address Count       = 0
Static Multicast Address Count      = 1
Dynamic Learned Address Count       = 6
Total MAC Address In Use            = 7
```

output definitions

Permanent Address Count	The number of static MAC addresses configured on the switch with a **permanent** management status (MAC address is never aged out).
DeleteOnReset Address Count	The number of static MAC addresses configured on the switch with a **reset** management status (MAC address is deleted on the next switch reboot).

output definitions (continued)

DeleteOnTimeout Address Count	The number of static MAC addresses configured on the switch with a **timeout** management status (MAC address ages out according to the MAC address table aging timer value).
Static Multicast Address Count	The number of static multicast MAC addresses configured on the switch. Note that static multicast addresses assigned to ports that are down or disabled are not counted.
Dynamic Learned Address Count	The number of MAC addresses learned by the switch. These are MAC addresses that are not statically configured addresses.
Total MAC Address In Use	The total number of MAC addresses (learned and static) that are known to the switch.

Release History

Release 5.1; command was introduced.
Release 5.4.1; **Static Multicast Address Count** field added.

Related Commands

show mac-address-table	Displays Source Learning MAC Address Table information.
show mac-address-table static-multicast	Displays the static multicast MAC address configuration for the switch.
show mac-address-table aging-time	Displays the current aging time value for the Source Learning MAC Address Table.

show mac-address-table aging-time

Displays the current aging time value for the specified VLAN.

show mac-address-table aging-time [vlan *vid***]**

Syntax Definitions

vid	VLAN ID number (1–4094).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If a *vid* is not specified, then the aging time value for all VLANs is displayed.
- The MAC Address Table aging time applies to static MAC addresses that were defined using the **time-out** parameter (see page 17-2) and to dynamically learned MAC addresses.

Examples

```
-> show mac-address-table aging-time

Mac Address Aging Time (seconds) for Vlan 1 = 300
Mac Address Aging Time (seconds) for Vlan 2 = 120
Mac Address Aging Time (seconds) for Vlan 50 = 900
Mac Address Aging Time (seconds) for Vlan 1000 = 300

-> show mac-address-table aging-time vlan 50

Mac Address Aging Time (seconds) for Vlan 50 = 900
```

Release History

Release 5.1; command was introduced.

Related Commands

show mac-address-table	Displays Source Learning MAC Address Table information.
show mac-address-table count	Displays Source Learning MAC Address Table statistics.

MIB Objects

```
slMacAddressAgingTable
   slMacAgingValue
```

18 Learned Port Security Commands

Learned Port Security (LPS) provides a mechanism for controlling network device communication on one or more switch ports. Configurable LPS parameters allow the user to restrict source learning on a port to:

- A maximum number of learned source MAC addresses.
- A specific amount of time in which source MAC addresses are learned.
- An individual learned source MAC address.
- A range of learned source MAC addresses.

This chapter includes descriptions of the CLI commands used to define LPS parameters and display information about the current LPS configuration.

MIB information for Learned Port Security commands is as follows:

Filename: AlcatelInd1LearnedPortSecurity.mib
Module: ALCATEL-IND1-LPS-MIB

A summary of the available commands is listed here:

port-security
port-security shutdown
port security maximum
port-security mac
port-security mac-range
port-security violation
port-security release
show port-security
show port-security shutdown

port-security

Enables or disables Learned Port Security (LPS) on a switch port. When LPS is enabled, only devices that have a source MAC address that complies with LPS restrictions are learned on the port.

port-security *slot/port* **[enable | disable]**

no port security *slot/port*

Syntax Definitions

slot/port	Enter the slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3). Use a hyphen to specify a range of ports on the same module (e.g. 3/1-16).
enable	Enables LPS on the specified port(s).
disable	Disables LPS on the specified port(s).

Defaults

By default, LPS is disabled on all switch ports.

parameter	default
enable | disable	enable

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- When LPS is disabled on a port, configured and learned MAC address entries for that port are retained in the LPS database table. Use the **no** form of this command to disable LPS *and* clear all entries from the table.
- LPS is supported on 10/100 and Gigabit Ethernet fixed, mobile, authenticated or 802.1Q tagged ports.
- LPS is not supported on link aggregate or 802.1Q tagged link aggregate (trunked) ports.
- Note that when LPS is enabled on an active port, all MAC addresses learned on that port prior to the time LPS was enabled are cleared from the source learning MAC address table.
- Configurable MAC learning restrictions consist of setting a source learning time limit window, specifying a maximum number of MACs allowed on a specific port, configuring a list of MAC addresses (individual or range of addresses) allowed on the port, and determining how a port handles traffic that is unauthorized.

Examples

```
-> port-security 4/8 enable
-> port-security 2/1-10 enable
-> port-security 2/11-15 disable
-> no port-security 1/1-12
```

Release History

Release 5.1; command was introduced.

Related Commands

port-security mac	Configures a single authorized source MAC address for a port. Enables LPS on the specified port, if it is not already active.
port-security mac-range	Configures a list of authorized source MAC addresses by defining a range of addresses allowed on the port. Enables LPS on the specified port, if it is not already active.
port security maximum	Defines the maximum number of MAC addresses that are allowed on the specified port.
port-security shutdown	Specifies the amount of time in minutes to allow source learning on all LPS ports.
port-security violation	Selects the method for handling traffic that does not comply with LPS restrictions for the specified port.

MIB Objects

```
learnedPortSecurityTable
   lpsAdminStatus
```

port-security shutdown

Configures the amount of time in minutes to allow source learning on all LPS ports. This LPS parameter applies to the entire switch, so when the time limit expires, source learning of *new* MAC addresses is stopped on all LPS ports. Only configured authorized MAC addresses are still allowed on LPS ports after this timer expires.

port-security shutdown *minutes*

Syntax Definitions

minutes	The number of minutes that defines the amount of time in which LPS allows source learning across all LPS ports.

Defaults

By default, the LPS source learning time limit is not set for the switch.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The LPS source learning time window is started and/or reset each time the **port-security shutdown** command is issued.
- To automatically start the timer on switch reboot, save this command to the **boot.cfg** file for the switch. Each time the switch reboots, the timer is restarted. It is still possible at any time, however, to reset the timer by issuing the command again.
- Note that source learning of configured authorized MAC addresses is still allowed after the LPS time limit has expired; however, all learning is stopped if the number of MAC addresses learned meets or exceeds the maximum number of addresses allowed, even if the LPS time limit has not expired.

Examples

```
-> port-security shutdown 25
-> port-security shutdown 60
```

Release History

Release 5.1; command was introduced.

Related Commands

port-security	Enables or disables LPS on the specified port.
port-security mac	Configures a single authorized source MAC address for a port. Enables LPS on the specified port, if it is not already active.
port-security mac-range	Configures a list of authorized source MAC addresses by defining a range of addresses allowed on the port. Enables LPS on the specified port, if it is not already active.
port security maximum	Defines the maximum number of MAC addresses that are allowed on a port.
port-security violation	Selects the method for handling traffic that does not comply with LPS restrictions for the specified port.

MIB Objects

```
learnedPortSecurityGlobalGroup
   lpsLearningWindowTime
```

port security maximum

Specifies the maximum number of source MAC addresses that an LPS port is allowed to learn.

port-security *slot/port* **maximum** *number*

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3). Use a hyphen to specify a range of ports on the same module (e.g. 3/1-16).
number	The number of source MAC addresses (1–100) that are allowed on this port.

Defaults

By default, the number of MAC addresses allowed is set to one.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If the port attempts to learn a MAC address that will exceed the maximum number allowed, the port will block the unauthorized address or will shutdown. Use the **port-security violation** command to specify how an LPS port will handle violating traffic.
- Note that source learning of configured authorized MAC addresses is still allowed after the LPS time limit has expired; however, all learning is stopped if the number of MAC addresses learned meets or exceeds the maximum number of addresses allowed, even if the LPS time limit has not expired.

Examples

```
-> port-security 2/14 maximum 25
-> port-security 4/10-15 maximum 100
```

Release History

Release 5.1; command was introduced.

Related Commands

port-security	Enables or disables LPS on the specified port.
port-security mac	Configures a single authorized source MAC address for a port. Enables LPS on the specified port, if it is not already active.
port-security mac-range	Configures a list of authorized source MAC addresses by defining a range of addresses allowed on the port. Enables LPS on the specified port, if it is not already active.
port-security shutdown	Specifies the amount of time in minutes to allow source learning on all LPS ports.
port-security violation	Selects the method for handling traffic that does not comply with LPS restrictions for the specified port.

MIB Objects

```
learnedPortSecurityTable
   lpsMaxMacNum
```

port-security mac

Configures a single authorized source MAC address for a port and enables LPS on the specified port, if it is not already active.

port-security *slot/port* **mac** *mac_address*

port-security *slot/port* **no mac** *mac_address*

Syntax Definitions

slot/port	Enter the slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3). Use a hyphen to specify a range of ports on the same module (e.g. 3/1-16).
mac_address	Source MAC address (e.g., 00:da:39:59:f1:0c).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of this command to remove statically configured or dynamically learned source MAC address entries from the LPS table. When a MAC address is removed from the LPS table, it is automatically cleared from the source learning table at the same time.
- Any additional source MAC addresses received that do not match configured authorized addresses are allowed on the port based on the LPS time limit (if active) and maximum number of MAC addresses allowed.
- Each configured authorized MAC address counts towards the number of addresses allowed on the port even if the port has not learned the configured address. For example, if a port has 3 configured authorized MAC addresses and the maximum number of addresses allowed is set to 10, then only 7 additional MAC addresses are allowed on that port.
- Note that source learning of configured authorized MAC addresses is still allowed after the LPS time limit has expired; however, all learning is stopped if the number of MAC addresses learned meets or exceeds the maximum number of addresses allowed, even if the LPS time limit has not expired.

Examples

```
-> port-security 4/20 mac 00:20:95:00:fa:5c
-> port-security 2/11-15 no mac 00:20:95:00:fa:5c
```

Release History

Release 5.1; command was introduced.

Related Commands

port-security	Enables or disables LPS on the specified port.
port-security mac-range	Configures a list of authorized source MAC addresses by defining a range of addresses allowed on the port. Enables LPS on the specified port, if it is not already active.
port-security shutdown	Specifies the amount of time in minutes to allow source learning on all LPS ports.
port security maximum	Defines the maximum number of MAC addresses that are allowed on the specified port.
port-security violation	Selects the method for handling traffic that does not comply with LPS restrictions for the specified port.

MIB Objects

```
learnedPortSecurityMacAddressTable
   lpsMacAddress
```

port-security mac-range

Configures a list of authorized MAC addresses by defining a range of addresses allowed on the port. This command also enables LPS on the specified port, if LPS is not already active on the port.

port-security *slot/port* **mac-range [low** *mac_address* | **high** *mac_address* | **low** *mac_address* **high** *mac_address***]**

Syntax Definitions

slot/port	Enter the slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3). Use a hyphen to specify a range of ports on the same module (e.g. 3/1-16).
low *mac_address*	MAC address that defines the low end of a range of MACs (e.g., 00:20:95:00:10:2A).
high *mac_address*	MAC address that defines the high end of a range of MACs (e.g., 00:20:95:00:10:2F).

Defaults

parameter	default
high *mac_address*	ff:ff:ff:ff:ff:ff
low *mac_address*	00:00:00:00:00:00

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If **low** and **high** end MAC addresses are not specified with this command, then the range is set back to the default range value (00:00:00:00:00:00– ff:ff:ff:ff:ff:ff).
- Source MAC addresses received on an LPS port that fall within the authorized range are allowed on the port. An additional entry is made in the LPS table for each of these learned addresses.
- Any additional source MAC addresses received that do not match configured authorized addresses are allowed on the port based on the LPS time limit (if active) and the maximum number of MAC addresses allowed.
- Each configured authorized MAC address counts towards the number of addresses allowed on the port even if the port has not learned the configured address. For example, if a port has 3 configured authorized MAC addresses and the maximum number of addresses allowed is set to 10, then only 7 additional MAC addresses are allowed on that port.
- Note that source learning of configured authorized MAC addresses is still allowed after the LPS time limit has expired; however, all learning is stopped if the number of MAC addresses learned meets or exceeds the maximum number of addresses allowed, even if the LPS time limit has not expired.

Examples

```
-> port-security 4/20 mac-range low 00:20:95:00:fa:5c
-> port-security 5/11-15 mac-range low 00:da:95:00:00:10 high 00:da:95:00:00:1f
-> port-security 5/16-20 mac-range high 00:da:95:00:00:1f
-> port-security 5/11-15 mac-range
```

Release History

Release 5.1; command was introduced.

Related Commands

port-security	Enables or disables LPS on the specified port.
port-security mac	Configures a single authorized source MAC address for a port. Enables LPS on the specified port, if it is not already active.
port-security shutdown	Specifies the amount of time in minutes to allow source learning on all LPS ports.
port security maximum	Defines the maximum number of MAC addresses that are allowed on the specified port.
port-security violation	Selects the method for handling traffic that does not comply with LPS restrictions for the specified port.

MIB Objects

```
learnedPortSecurityTable
   lpsLoMacRange
   lpsHiMacRange
```

port-security violation

Selects the method for handling traffic that does not comply with LPS restrictions for the specified port.

port-security *slot/port* **violation {restrict | shutdown}**

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3). Use a hyphen to specify a range of ports on the same module (e.g. 3/1-16).
restrict	Filters (blocks) unauthorized traffic but allows traffic that complies with LPS restrictions to forward on the port.
shutdown	The port is disabled when the port receives unauthorized traffic; no traffic is allowed on the port.

Defaults

By default, the security violation mode is set to **restrict** when LPS is enabled on the port.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- When a traffic violation occurs on an LPS port, notice is sent to the Switch Logging task.
- If the violation mode is set to **restrict**, unauthorized source MAC addresses are not learned in the LPS table but are still recorded in the source learning MAC address table with a filtered operational status. This allows the user to view MAC addresses that were attempting unauthorized access to the LPS port.
- When an LPS port is disabled (**shutdown**) or unauthorized traffic received on the port is filtered (**restrict**) due to a security violation, use the **port-security release** command to restore the port to normal operation.

Examples

```
-> port-security 2/14 violation restrict
-> port-security 4/10-15 violation shutdown
```

Release History

Release 5.1; command was introduced.

Related Commands

port-security	Enables or disables LPS on the specified port.
port-security release	Releases a port that was shut down due to an LPS violation
port security maximum	Defines the maximum number of MAC addresses that are allowed on the specified port.
port-security mac	Configures a single authorized source MAC address for a port. Enables LPS on the specified port, if it is not already active.
port-security mac-range	Configures a list of authorized source MAC addresses by defining a range of addresses allowed on the port. Enables LPS on the specified port, if it is not already active.
port-security shutdown	Specifies the amount of time in minutes to allow source learning on all LPS ports.

MIB Objects

```
learnedPortSecurityTable
   lpsViolationOption
```

port-security release

Releases a port that was shut down due to a Learned Port Security (LPS) violation. The specified port resumes normal operation without having to manually reset the port and/or the entire module.

port-security *slot/port* **release**

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3). Use a hyphen to specify a range of ports on the same module (e.g. 3/1-16).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command restores the port to the same operational state it was in before the shutdown. This includes the activation of any existing LPS configuration for the port.
- Note that when this command is used, all MAC addresses known to the specified port are flushed from the switch MAC address table.

Examples

```
-> port-security 2/14 release
-> port-security 4/10-15 release
```

Release History

Release 5.1.6; command was introduced.

Related Commands

port-security	Enables or disables LPS on the specified port.
port-security mac	Configures a single authorized source MAC address for a port. Enables LPS on the specified port, if it is not already active.
port-security mac-range	Configures a list of authorized source MAC addresses by defining a range of addresses allowed on the port. Enables LPS on the specified port, if it is not already active.
port-security shutdown	Specifies the amount of time in minutes to allow source learning on all LPS ports.
port security maximum	Defines the maximum number of MAC addresses that are allowed on the specified port.

MIB Objects

```
learnedPortSecurityTable
   lpsRelease
```

show port-security

Displays Learned Port Security (LPS) configuration and table entries.

show port-security [*slot/port* | *slot* **| config-mac-range]**

Syntax Definitions

slot/port	Slot number for the module or the slot number and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3). Use a hyphen to specify a range of ports on the same module (e.g. 3/1-16).
slot	Enter the slot number for a module to specify that the command should include all ports on that module (e.g., 6 specifies all ports on the module found in slot 6 of the switch chassis).
config-mac-range	Displays all LPS ports that are configured with an authorized range of MAC addresses**.**

Defaults

By default, all ports with an LPS configuration are displayed. MAC address range information is not included in the default display.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Displays ports that have an LPS configuration, even if LPS is disabled on the port.
- Specifying a *slot/port* designation or the **config-mac-range** option are mutually exclusive. Using the two options together is not allowed at this time.
- An entry is made in the LPS table for each source MAC address that is learned. If the MAC was allowed on the port but did not match a configured MAC address, it is classified as a **dynamic** MAC type. If the switch configuration is saved and the switch rebooted, this same MAC address is changed to a **configured** MAC type.
- In addition, MAC addresses that were learned on the LPS port because they fell within the specified MAC address range, appear as a separate entry in the LPS table with a dynamic MAC type.
- Dynamic MAC addresses become configured MAC addresses in the LPS table when the switch configuration is saved and the switch is rebooted. If the configuration is not saved before the next reboot, all dynamic MAC addresses are cleared from the LPS table.
- The MAC Type field is blank if an authorized MAC address range is configured for the LPS port.

Examples

```
-> show port-security
  Port   Security    MaxMacs   Violation     IndividualMac     MacType
-------+-----------+---------+-----------+-----------------+-----------
   1/12   enabled    100       restrict   00:01:96:1c:f1:c0  dynamic
                                          00:06:5b:a3:19:3f  dynamic
                                          00:0c:f1:89:f6:03  dynamic
   1/22   enabled      1       restrict
   1/23   enabled      2       restrict   00:95:2a:0f:ce:19  configured
                                          00:95:2a:5e:cf:2a  configured
   1/24   enabled    100       shutdown

-> show port-security config-mac-range
   Port         LowMac           HighMac
---------+------------------+-----------------
  1/12     00:00:00:00:00:00  ff:ff:ff:ff:ff:ff
  1/22     00:00:00:00:00:00  ff:ff:ff:ff:ff:ff
  1/23     00:00:00:00:00:00  ff:ff:ff:ff:ff:ff
  1/24     00:95:2a:00:00:5a  00:95:2a:00:00:6f
```

output definitions

Port	The module slot number and the physical port number on that module.
Security	The Learned Port Security status for the port (**enabled** or **disabled**). Configured through the **port-security** command.
MaxMacs	The maximum number of MAC addresses that are allowed on this port. Configured through the **port security maximum** command.
Violation	The security violation mode for the port (**restrict** or **shutdown**). Configured through the **port-security violation** command.
IndividualMac	An individual authorized MAC address. Configured through the **port-security mac** command.
MacType	Indicates if the MAC address was dynamically learned or statically configured as an authorized MAC address for the port. Dynamic MAC addresses become configured MAC address entries after a configuration save and switch reboot.
LowMac	MAC address that defines the low end of a MAC address range. Configured through the **port-security mac-range** command.
HighMac	MAC address that defines the high end of a MAC address range. Configured through the **port-security mac-range** command.

Release History

Release 5.1; command was introduced.

Related Commands

show port-security shutdown	Displays the amount of time in which source learning is allowed on all switch ports.

show port-security shutdown

Displays the amount of time during which source learning can occur on all LPS ports.

show port-security shutdown

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The source learning time limit is a switch-wide parameter that applies to all ports that have LPS enabled.
- If the shutdown time is set to zero, then a source learning time limit is not active on LPS ports.
- Note that source learning of configured authorized MAC addresses is still allowed after the LPS time limit has expired; however, all learning is stopped if the number of MAC addresses learned meets or exceeds the maximum number of addresses allowed, even if the LPS time limit has not expired.

Examples

```
-> show port-security shutdown
LPS Shutdown = 60 mins
->
```

Release History

Release 5.1; command was introduced.

Related Commands

show port-security	Displays Learned Port Security configuration values as well as MAC addresses learned on the port.

19 Ethernet Port Commands

The Ethernet port software is responsible for configuring and monitoring Ethernet ports (10 Mbps, 100 Mbps, 1 Gbps, and 10 Gbps). This includes:

- Performing hardware diagnostics, loading software, and initializing hardware.
- Notifying other software modules in the system when Ethernet links become active or inactive.
- Configuring basic line parameters for Ethernet ports.
- Gathering basic line statistics for Ethernet ports and passing this information to the user interface and configuration manager.

MIB information for the Ethernet Port commands is as follows:

Filename: AlcatelIND1Port.mib
Module: alcatelIND1PortMIB

Filename: IETF_ETHERLIKE.mib
Module: EtherLike-MIB

A summary of the available commands is listed here.

Trap port commands	**trap port link**
Flow commands	**flow** **flow wait time**
Interfaces commands	**interfaces speed** **interfaces autoneg** **interfaces crossover** **interfaces flow** **interfaces duplex** **interfaces admin** **interfaces alias** **interfaces ifg** **interfaces no l2 statistics** **interfaces long** **interfaces max frame** **interfaces runt** **interfaces runtsize** **interfaces flood** **interfaces flood multicast** **interfaces flood rate** **show interfaces** **show interfaces capability** **show interfaces flow control** **show interfaces accounting** **show interfaces counters** **show interfaces counters errors** **show interfaces collisions** **show interfaces status** **show interfaces port** **show interfaces ifg** **show interfaces flood rate** **show interfaces traffic**
OmniSwitch 8800 10 Gigabit module commands	**10gig slot** **show 10gig**
Debug interfaces commands	**debug interfaces set backpressure** **debug interfaces backpressure**

trap port link

Enables trap link messages. If enabled, a message is displayed on the Network Management Station (NMS) whenever the port changes state.

trap *slot***[/***port***[-***port2***]] port link {enable | disable | on | off}**

Syntax Definitions

slot	Slot number you want to configure.
port	Port number of the interface you want to configure.
port2	Last port number in a range of ports you want to configure.
enable	Port link up/down traps are displayed on the NMS.
disable	Port link up/down traps are not displayed on the NMS.
on	Same as **enable**.
off	Same as **disable**.

Defaults

parameter	default
enable | disable | on | off	**disable**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> trap 3/1 port link enable
-> trap 3 port link enable
-> trap 3/1-6 port link enable
```

Release History

Release 5.1; command was introduced.

Related Commands

show interfaces status	Displays interface line settings.

MIB Objects

```
esmConfigTable
   esmPortSlot
   esmPortIF
```

flow

Enables flow control on interfaces. Flow control enables a receiving device to continue receiving data even after its buffers become full.

flow [ethernet | fastethernet | gigaethernet] *slot***[**/*port***[-***port2***]]**

no flow [ethernet | fastethernet | gigaethernet] *slot***[**/*port***[-***port2***]]**

Syntax Definitions

ethernet	Optional syntax. Documents the interface type as 10 Mbps Ethernet.
fastethernet	Optional syntax. Documents the interface type as 100 Mbps Ethernet.
gigaethernet	Optional syntax. Documents the interface type as 1 Gbps Ethernet.
slot	Slot number you want to configure.
port	Port number of the interface you want to configure.
port2	Last port number in a range of ports you want to configure.

Defaults

On OmniSwitch 6600, 7700, 7800, 8800 switches flow control is disabled by default.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

If auto-negotiation is implemented and enabled for this interface, the “pause” mode for this interface is determined by auto-negotiation.

Examples

```
-> flow 3/1
-> flow 3
-> flow 3/1-4
```

Release History

Release 5.1; command was introduced.

Related Commands

flow wait time	Configures the flow control wait time.
show interfaces flow control	Displays flow control wait time settings.

MIB Objects

```
dot3PauseTable
   dot3PauseAdminMode
```

flow wait time

Configures or disables flow control wait time.

flow [ethernet | fastethernet | gigaethernet] *slot***[**/*port***[**-*port2***]] wait [time]** *microseconds*

flow [ethernet | fastethernet | gigaethernet] *slot***[**/*port***[**-*port2***]] no wait [time]**

Syntax Definitions

ethernet	Optional syntax. Documents the interface type as 10 Mbps Ethernet.
fastethernet	Optional syntax. Documents the interface type as 100 Mbps Ethernet.
gigaethernet	Optional syntax. Documents the interface type as 1 Gbps Ethernet.
time	Optional syntax.
slot	Slot number you want to configure.
port	Port number of the interface you want to configure.
port2	Last port number in a range of ports you want to configure.
microseconds	Wait time, in microseconds, which can be 0 to 30000.
no wait	Disables flow control wait time.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Defaults

parameter	default
microseconds	0

Usage Guidelines

- You can only configure one slot at a time. Repeat the command to configure additional slots.
- The **flow no wait** command is the same as setting the wait time to zero (0).
- The wait time is not configurable at 10 Mbps.
- If auto-negotiation is implemented and enabled for this interface, the “Pause” mode for this interface is determined by Auto-negotiation and Full duplex.

Examples

```
-> flow 3/1 wait 96
-> flow 3/1 no wait
-> flow 3 wait 96
-> flow 3 no wait
-> flow 3/1-6 wait 96
-> flow 3/1-6 no wait
```

Release History

Release 5.1; command was introduced.

Related Commands

flow	Enables/disables flow control (go/pause) on an interface.
show interfaces flow control	Displays interface flow control wait settings.

MIB Objects

```
esmConfigTable
   esmPortPauseSlotTime
```

interfaces speed

Configures interface line speed.

interfaces [ethernet | fastethernet | gigaethernet] *slot*[/*port*[-*port2*]] **speed {auto | 10 | 100 | 1000 | 10000 | max {100 | 1000}}**

Syntax Definitions

ethernet	Optional syntax. Documents the interface type as 10 Mbps Ethernet.
fastethernet	Optional syntax. Documents the interface type as 100 Mbps Ethernet.
gigaethernet	Optional syntax. Documents the interface type as 1 Gbps Ethernet.
slot	Slot number you want to configure.
port	Port number of the interface you want to configure.
port2	Last port number in a range of ports you want to configure.
auto	The switch will automatically set the line speed to match the attached device (auto-sensing).
10	Sets the interface to 10 Mbps.
100	Sets the interface to 100 Mbps.
1000	Sets the interface to 1 Gigabit.
10000	Sets the interface to 10 Gigabit.
max 100	Sets the maximum speed to 100 megabits.
max 1000	Sets the maximum speed to 1000 megabits (1 Gigabit)

Defaults

parameter	default
auto | 10 | 100 | 1000 | 10000 | max 100 | max 1000} (OmniSwitch 7700, 7800, and 8800)	Auto except for the OS7-ENI-FM12, OS7-GNI-U12, OS8-GNI-U8, OS8-GNI-C8, OS8-GNI-U24; 100 for the OS7-ENI-FM12; 1000 for the OS7-GNI-U12, OS8-GNI-U8, OS8-GNI-C8, OS8-GNI-U24.
auto | 10 | 100 | 1000 | 10000 | max 100 | max 1000 (OmniSwitch 6600 Family)	Auto for copper 10/100 and copper Gigabit ports; 100 for ports 1–24 on the OmniSwitch 6600-U24 only; 1000 for fiber Gigabit ports.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- You can only configure one slot at a time. Repeat the command to configure additional slots.
- The **auto** option sets the speed to auto-sensing.
- You cannot configure the speed of the OS7-ENI-FM12; it is fixed at 100 Mbps.
- You cannot configure the speed of the GBIC-C for the OS7-GNI-U2; it is fixed at 1 Gbps.
- On the OmniSwitch 6624, 6600-U24, and OmniSwitch 6600-P24, the **auto** option is not available on fiber Gigabit ports (ports 25 through 28). However, copper Gigabit ports are set by default to **auto**.
- On the OmniSwitch 6602-24, the **auto** option is not available on fiber Gigabit ports (ports 25 and 26). However, copper Gigabit ports are set by default to **auto**.
- On the OmniSwitch 6648, the **auto** option is not available on fiber Gigabit ports (ports 49 through 52). However, copper Gigabit ports are set by default to **auto**.
- On the OmniSwitch 6602-48, the **auto** option is not available on fiber Gigabit ports (ports 49 and 50). However, copper Gigabit ports are set by default to **auto**.
- The auto option is not available on ports 1–24 on the OmniSwitch 6600-U24.
- Copper SFPs used on OmniSwitch 6600 Family switches only support 1000 Mbps.

Examples

```
-> interfaces 3/1 speed auto
-> interfaces 3 speed 100
-> interfaces 3/1-8 speed auto
```

Release History

Release 5.1; command was introduced.

Related Commands

interfaces duplex	Configures duplex mode.
interfaces autoneg	Enables and disables auto negotiation.
show interfaces status	Displays interface line settings.

MIB Objects

```
esmConfTable
   esmPortCfgSpeed
```

interfaces autoneg

Enables or disables auto negotiation on a single port, a range of ports, or an entire Network Interface (NI).

interfaces [ethernet | fastethernet | gigaethernet] *slot***[**/*port***[-***port2***]]**
autoneg {enable | disable | on | off}

Syntax Definitions

ethernet	Optional syntax. Documents the interface type as 10 Mbps Ethernet.
fastethernet	Optional syntax. Documents the interface type as 100 Mbps Ethernet.
gigaethernet	Optional syntax. Documents the interface type as 1 Gbps Ethernet.
slot	Slot number you want to configure.
port	Port number of the interface you want to configure.
port2	Last port number in a range of ports you want to configure.
enable	Enables auto negotiation.
disable	Disables auto negotiation.
on	Same as enable.
off	Same as disable.

Defaults

parameter	default
enable | disable | on | off (all modules except for the OS7-ENI-FM12)	enable
enable | disable | on | off (OS7-ENI-FM12)	disable

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- You can only configure one slot at a time. Repeat the command to configure additional slots.
- If auto negotiation is disabled, auto MDIX, flow control, auto speed, and auto duplex are not accepted. See the **interfaces crossover** command on page 19-14 and **interfaces flow** command on page 19-16 for more information.
- Copper Gigabit ports on OmniSwitch 6600 Family switches do not support disabling of auto negotiation.

Examples

```
-> interfaces 3 autoneg disable
-> interfaces 3/1 autoneg disable
-> interfaces 3/1-4 autoneg disable
```

Release History

Release 5.1; command was introduced.

Related Commands

interfaces speed	Configures interface speed.
interfaces crossover	Configures crossover port settings.
interfaces flow	Enables or disables flow (pause).
show interfaces status	Displays interface line settings.
show interfaces capability	Displays auto negotiation, speed, duplex, and crossover settings.

MIB Objects

```
esmConfTable
   esmPortCfgAutoNegotiation
```

interfaces crossover

Configures port crossover settings on a single port, a range of ports, or an entire Network Interface (NI).

interfaces [ethernet | fastethernet | gigaethernet] *slot***[**/*port***[-***port2***]]**
crossover {auto | mdix | mdi | disable}

Syntax Definitions

ethernet	Optional syntax. Documents the interface type as 10 Mbps Ethernet.
fastethernet	Optional syntax. Documents the interface type as 100 Mbps Ethernet.
gigaethernet	Optional syntax. Documents the interface type as 1 Gbps Ethernet.
slot	Slot number you want to configure.
port	Port number of the interface you want to configure.
port2	Last port number in a range of ports you want to configure.
auto	The interface will automatically detect crossover settings.
mdix	Sets the crossover configuration to Media Dependent Interface with Crossover (MDIX), which is the standard for hubs and switches.
mdi	Sets the crossover configuration to Media Dependent Interface (MDI), which is the standard for end stations.
disable	Disables automatic crossover detection.

Defaults

parameter	default
auto | **mdix** | **mdi** | **disable** (all copper ports except for the GBIC-C for the OS7-GNI-U2)	auto
auto | **mdix** | **mdi** | **disable** (all fiber ports and the GBIC-C for the OS7-GNI-U2)	disable

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- You can only configure one slot at a time. Repeat the command to configure additional slots.
- If auto negotiation is disabled then automatic crossover will also be disabled. See the **interfaces autoneg** command on page 19-12 for more information.
- You cannot configure crossover settings on fiber ports.
- You cannot configure crossover settings on the GBIC-C for the OS7-GNI-U2.
- You cannot change crossover configuration copper SFP ports on OmniSwitch 6600 Family switches.

Examples

```
-> interfaces 3 crossover disable
-> interfaces 3/1 crossover mdix
-> interfaces 3/1-4 crossover auto
```

Release History

Release 5.1; command was introduced.

Related Commands

interfaces speed	Configures interface speed.
interfaces autoneg	Enables and disables auto negotiation.
interfaces flow	Enables or disables flow (pause).
show interfaces status	Displays interface line settings.
show interfaces capability	Displays auto negotiation, speed, duplex, and crossover settings.

MIB Objects

```
esmConfTable
   esmPortCfgCrossover
```

interfaces flow

Enables and disables flow (pause) settings on a single port, a range of ports, or an entire Network Interface (NI).

interfaces [ethernet | fastethernet | gigaethernet] *slot***[**/*port***[**-*port2***]] flow {enable | disable | on | off}**

Syntax Definitions

ethernet	Optional syntax. Documents the interface type as 10 Mbps Ethernet.
fastethernet	Optional syntax. Documents the interface type as 100 Mbps Ethernet.
gigaethernet	Optional syntax. Documents the interface type as 1 Gbps Ethernet.
slot	Slot number you want to configure.
port	Port number of the interface you want to configure.
port2	Last port number in a range of ports you want to configure.
enable	Enables flow.
disable	Disables flow.
on	Same as enable.
off	Same as disable.

Defaults

parameter	default
enable | **disable** | **on** | **off** (all modules except for the OS7-ENI-FM12)	enable
enable | **disable** | **on** | **off** (OS7-ENI-FM12)	disable

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- You can only configure one slot at a time. Repeat the command to configure additional slots.
- If auto negotiation is disabled then flow will also be disabled. See the **interfaces autoneg** command on page 19-12 for more information.
- If auto negotiation is disabled and then later enabled on an interface, the original flow setting will then be restored.

Examples

```
-> interfaces 3 flow disable
-> interfaces 3/1 flow disable
-> interfaces 3/1-4 flow disable
```

Release History

Release 5.1; command was introduced.

Related Commands

interfaces speed	Configures interface speed.
interfaces autoneg	Enables and disables auto negotiation.
interfaces crossover	Configures crossover port settings.
show interfaces status	Displays interface line settings.
show interfaces capability	Displays auto negotiation, speed, duplex, and crossover settings.

MIB Objects

```
dot3ControlTable
   dot3PauseAdminMode
```

interfaces duplex

Configures duplex mode. In full duplex mode, the interface transmits and receives data simultaneously. In half duplex mode, the interface can transmit *or* receive data at a given time. Auto duplex setting causes the switch to advertise all available duplex modes (half/full/both) for the port during autonegotiation.

interfaces [ethernet | fastethernet | gigaethernet] *slot***[**/*port***[-**_port2_**]] duplex {full | half | auto}**

Syntax Definitions

ethernet	Optional syntax. Documents the interface type as 10 Mbps Ethernet.
fastethernet	Optional syntax. Documents the interface type as 100 Mbps Ethernet.
gigaethernet	Optional syntax. Documents the interface type as 1 Gbps Ethernet.
slot	Slot number you want to configure.
port	Port number of the interface you want to configure.
port2	Last port number in a range of ports you want to configure.
full	Sets interface to full duplex mode.
half	Sets interface to half duplex mode.
auto	Switch will automatically set both the duplex mode settings to auto-negotiation.

Defaults

parameter	default
full | **half** | **auto** (OmniSwitch 7700, 7800, 8800)	auto (all except for the OS7-ENI-FM12, OS7-GNI-U12, OS8-GNI-U24); full (OS7-ENI-FM12, OS7-GNI-U12, OS8-GNI-U24)
full | **half** | **auto** (OmniSwitch 6600 Family)	auto (copper ports); full (fiber ports)

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- You can only configure one slot at a time. Repeat the command to configure additional slots.
- Half duplex mode is not supported on Gigabit modules if a port is detected as Gigabit (1000 Mbps).
- OS7-GNI-C12 and OS8-GNI-C24 modules can be configured for full and half duplex. All other Gigabit Ethernet modules on the OmniSwitch 7700/7800/8800 only support full duplex mode.

- On OS7-GNI-C12 and the OS8-GNI-C24 modules if a link is down and auto negotiation is enabled, then half duplex is not accepted since these modules are Gigabit modules by default.
- Copper Gigabit ports on OmniSwitch 6600 Family switches only support full duplex.

Examples

```
-> interfaces 3/1 duplex auto
-> interfaces 3 duplex half
-> interfaces 3/1-4 auto
```

Release History

Release 5.1; command was introduced.

Related Commands

interfaces speed	Configures interface line speed. Set to **auto** to set speed and duplex mode to auto-sensing.
show interfaces status	Displays interface line settings (e.g., speed, mode).

MIB Objects

```
esmConfTable
   esmPortAutoDuplexMode
```

interfaces admin

Administratively enables or disables interfaces.

interfaces [ethernet | fastethernet | gigaethernet] *slot***[**/*port***[-***port2***]] admin {up | down}**

Syntax Definitions

ethernet	Optional syntax. Documents the interface type as 10 Mbps Ethernet.
fastethernet	Optional syntax. Documents the interface type as 100 Mbps Ethernet.
gigaethernet	Optional syntax. Documents the interface type as 1 Gbps Ethernet.
slot	Slot number you want to configure.
port	Port number of the interface you want to configure.
port2	Last port number in a range of ports you want to configure.
up	Enables the interface.
down	Disables the interface.

Defaults

parameter	default
up | **down**	up

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> interfaces 3/1 admin up
-> interfaces 3 admin down
-> interfaces 3/1-4 admin up
```

Release History

Release 5.1; command was introduced.

Related Commands

show interfaces	Displays general interface information (e.g., hardware, MAC address, input errors, output errors).
show interfaces port	Displays port status (up or down).

MIB Objects

```
ifTable
   ifAdminStatus
```

interfaces alias

Configures a description (alias) for a single port.

interfaces [ethernet | fastethernet | gigaethernet] *slot/port* **alias** *description*

Syntax Definitions

ethernet	Optional syntax. Documents the interface type as 10 Mbps Ethernet.
fastethernet	Optional syntax. Documents the interface type as 100 Mbps Ethernet.
gigaethernet	Optional syntax. Documents the interface type as 1 Gbps Ethernet.
slot	Slot number you want to configure.
port	Port number of the interface you want to configure.
description	A description for the port, which can be up to 40 characters long. Spaces must be contained within quotes (e.g., “IP Phone”).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- You can only configure one port at a time. You cannot configure an alias for multiple ports.
- To remove an alias use a description consisting of two quotes without any spaces (e.g., "").

Examples

```
-> interfaces 3/1 alias switch_port
-> interfaces 2/2 alias "IP Phone"
-> interfaces 3/1 alias ""
```

Release History

Release 5.1; command was introduced.

Related Commands

show interfaces	Displays general interface information (e.g., hardware, MAC address, input errors, output errors).
show interfaces port	Displays port status (up or down) and any aliases for a port.

MIB Objects

```
ifXTable
   ifAlias
```

interfaces ifg

Configures the inter-frame gap on Gigabit Ethernet interfaces.

interfaces [ethernet | fastethernet | gigaethernet] *slot***[**/*port***[-***port2***]] ifg** *bytes*

Syntax Definitions

ethernet	Optional syntax. Documents the interface type as 10 Mbps Ethernet.
fastethernet	Optional syntax. Documents the interface type as 100 Mbps Ethernet.
gigaethernet	Optional syntax. Documents the interface type as 1 Gbps Ethernet.
slot	Slot number you want to configure.
port	Port number of the interface you want to configure.
port2	Last port number in a range of ports you want to configure.
bytes	Inter-frame gap value, in bytes. Valid range is 9–12.

Defaults

parameter	default
bytes	12

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- You can only configure one slot at a time. Repeat the command to configure additional slots.
- On the OmniSwitch 6624, 6600-U24, and OmniSwitch 6600-P24, this command is valid only on ports 25 though 28 when Gigabit Ethernet expansion modules are installed.
- On the OmniSwitch 6648, this command is valid only on ports 49 through 52 when Gigabit Ethernet expansion modules are installed.

Examples

```
-> interfaces 3/1 ifg 10
-> interfaces 3 ifg 10
-> interfaces 3/1-4 ifg 10
```

Release History

Release 5.1; command was introduced.

Related Commands

show interfaces ifg	Displays the inter-frame gap value for one or more ports.

MIB Objects

```
esmConfTable
   esmPortCfgIfg
```

interfaces no l2 statistics

Resets all statistics counters.

interfaces [ethernet | fastethernet | gigaethernet] *slot***[**/*port***[-***port2***]] no l2 statistics**

Syntax Definitions

ethernet	Optional syntax. Documents the interface type as 10 Mbps Ethernet.
fastethernet	Optional syntax. Documents the interface type as 100 Mbps Ethernet.
gigaethernet	Optional syntax. Documents the interface type as 1 Gbps Ethernet.
slot	Slot number you want to configure.
port	Port number of the interface you want to configure.
port2	Last port number in a range of ports you want to configure.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- You can only configure one slot at a time. Repeat the command to configure additional slots.
- This command calls for an upper or lower case “L” character in front of the “2” character. Entering the digit “1” (one) will result in an error message.

Examples

```
-> interfaces 3/1 no l2 statistics
-> interfaces 3 no l2 statistics
-> interfaces 3/1-6 no l2 statistics
```

Release History

Release 5.1; command was introduced.

Related Commands

show interfaces	Displays general interface information, including when statistics were last cleared.
show interfaces accounting	Displays interface accounting information (e.g., packets received/ transmitted, deferred frames received).
show interfaces counters	Displays interface counters information (e.g., unicast, broadcast, multi-cast packets received/transmitted).
show interfaces counters errors	Displays interface error frame information (e.g., CRC errors, transit errors, receive errors).
show interfaces collisions	Displays interface collision information (e.g., number of collisions, number of retries).

MIB Objects

```
alcetherStatsTable
   alcetherClearStats
```

interfaces long

Enables and disables maximum frame size configuration for Gigabit interfaces.

interfaces [ethernet | fastethernet | gigaethernet] *slot***[**/*port***[-***port2***]] long {enable | disable}**

Syntax Definitions

ethernet	Optional syntax. Documents the interface type as 10 Mbps Ethernet.
fastethernet	Optional syntax. Documents the interface type as 100 Mbps Ethernet.
gigaethernet	Optional syntax. Documents the interface type as 1 Gbps Ethernet.
slot	Slot number you want to configure.
port	Port number of the interface you want to configure.
port2	Last port number in a range of ports you want to configure.
enable	Enables maximum frame size configuration for Gigabit interfaces.
disable	Disables maximum frame size configuration for Gigabit interfaces.
on	Same as enable.
off	Same as disable.

Defaults

parameter	default
enable | disable	enable

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> interfaces 3/1 long enable
-> interfaces 3 long enable
-> interfaces 3/1-2 long enable
```

Release History

Release 5.1; command was introduced.

Related Commands

show interfaces	Displays general interface information (e.g., hardware, MAC address, input errors, output errors).

MIB Objects

```
esmConfTable
   esmPortCfgLongEnable
```

interfaces max frame

Configures the maximum frame size for Gigabit Ethernet interfaces.

interfaces [gigaethernet] *slot***[**/*port***[**-*port2***]] max frame** *bytes*

Syntax Definitions

gigaethernet	Optional syntax. Documents the interface type as 1 Gbps Ethernet.
slot	Slot number you want to configure.
port	Port number of the interface you want to configure.
port2	Last port number in a range of ports you want to configure.
max frame	Maximum frame size, in bytes. Valid range is 1518–9216.

Defaults

parameter	default
bytes (Gigabit Ethernet Packets)	9216
bytes (Ethernet Packets)	1553

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> interfaces 3/1 max frame 1518
-> interfaces 3 max frame 1518
-> interfaces 3/1-3 max frame 1518
```

Release History

Release 5.1; command was introduced.

Related Commands

show interfaces	Displays general interface information (e.g., hardware, MAC address, input errors, output errors).

MIB Objects

```
esmConfTable
   esmPortCfgMaxFrameSize
```

interfaces runt

Enables and disables minimum frame size configuration for Ethernet, Fast Ethernet, or Gigabit Ethernet interfaces.

interfaces [ethernet | fastethernet | gigaethernet] *slot***[**/*port***[**-*port2***]] runt {enable | disable}**

Syntax Definitions

ethernet	Optional syntax. Documents the interface type as 10 Mbps Ethernet.
fastethernet	Optional syntax. Documents the interface type as 100 Mbps Ethernet.
gigaethernet	Optional syntax. Documents the interface type as 1 Gbps Ethernet.
slot	Slot number you want to configure.
port	Port number of the interface you want to configure.
port2	Last port number in a range of ports you want to configure.
runt	Specifies the minimum frame size.
enable	Enables the minimum frame size for the specified port.
disable	Disables minimum frame size for the specified port.
on	Same as enable.
off	Same as disable.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> interfaces 3/1 runt enable
-> interfaces 3 runt enable
-> interfaces 3/1-4 runt enable
```

Release History

Release 5.1; command was introduced.

Related Commands

show interfaces	Displays general interface information (e.g., hardware, MAC address, input errors, output errors).

MIB Objects

```
esmConfTable
   esmPortCfgRuntEnable
```

interfaces runtsize

Configures the minimum frame size on Ethernet, Fast Ethernet or Gigabit Ethernet interfaces from 0 to 64 bytes.

interfaces [ethernet | fastethernet | gigaethernet] *slot***[**/*port***[**-*port2***]] runtsize** *framesize*

Syntax Definitions

ethernet	Optional syntax. Documents the interface type as 10 Mbps Ethernet.
fastethernet	Optional syntax. Documents the interface type as 100 Mbps Ethernet.
gigaethernet	Optional syntax. Documents the interface type as 1 Gbps Ethernet.
slot	Slot number you want to configure.
port	Port number of the interface you want to configure.
port2	Last port number in a range of ports you want to configure.
framesize	Specifies the minimum framesize from 0 to 64 bytes *(default)*.

Defaults

parameter	default
framesize	64 bytes

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> interfaces 3/1 runtsize 32
-> interfaces 3 runtsize 32
-> interfaces 3/1-8 runtsize 32
```

Release History

Release 5.1; command was introduced.

Related Commands

show interfaces	Displays general interface information (e.g., hardware, MAC address, input errors, output errors).

MIB Objects

```
esmConfTable
   esmPortCfgRuntSize
```

interfaces flood

Enables the maximum flood rate.

interfaces [ethernet | fastethernet | gigaethernet] *slot* **flood**

Syntax Definitions

ethernet	Optional syntax. Documents the interface type as 10 Mbps Ethernet.
fastethernet	Optional syntax. Documents the interface type as 100 Mbps Ethernet.
gigaethernet	Optional syntax. Documents the interface type as 1 Gbps Ethernet.
slot	Slot number you want to configure.

Defaults

Flood broadcasting is enabled by default.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- You cannot configure individual ports or ranges of ports. You can only configure entire slots.

Examples

```
-> interfaces 3 flood
-> interfaces 1/47 flood
-> interfaces 1/45-48 flood
```

Release History

Release 5.1; command was introduced.

Related Commands

show interfaces flood rate	Displays interface peak flood rate settings.
interfaces flood multicast	Enables/disables flood multicasting on an interface.
interfaces flood rate	Configures the peak flood rate for an interface.

MIB Objects

```
esmConfTable
   esmPortFloodMcastEnable
```

interfaces flood multicast

Enables the multicast traffic maximum flood rate.

interfaces [ethernet | fastethernet | gigaethernet] *slot* **flood multicast**

Syntax Definitions

ethernet	Optional syntax. Documents the interface type as 10 Mbps Ethernet.
fastethernet	Optional syntax. Documents the interface type as 100 Mbps Ethernet.
gigaethernet	Optional syntax. Documents the interface type as 1 Gbps Ethernet.
slot	Slot you want to configure (e.g., 3).

Defaults

Flood multicasting is enabled by default.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- You can only configure one slot at a time. Repeat the command to configure additional slots.
- Enabling the maximum multicast flood rate with the **interfaces flood multicast** command will limit IP Multicast Switching (IPMS) and non-IPMS multicast traffic.
- You cannot configure individual ports or ranges of ports. You can only configure entire slots.
- To remove the effects of the interfaces flood multicast command use the **interfaces flood** command.

Examples

```
-> interfaces 3 flood multicast
-> interfaces 1/47 flood multicast
-> interfaces 1/45-48 flood multicast
```

Release History

Release 5.1; command was introduced.

Related Commands

show interfaces flood rate	Displays interface peak flood rate settings.
interfaces flood	Enables maximum flood rate on an interface.
interfaces flood rate	Configures the peak flood rate for an interface.

MIB Objects

```
esmConfTable
   esmPortFloodMcastEnable
```

interfaces flood rate

Configures the peak flood rate for interfaces.

interfaces [ethernet | fastethernet | gigaethernet] *slot***[**/*port***[-***port2***]] flood rate** *Mbps*

Syntax Definitions

ethernet	Optional syntax. Documents the interface type as 10 Mbps Ethernet.
fastethernet	Optional syntax. Documents the interface type as 100 Mbps Ethernet.
gigaethernet	Optional syntax. Documents the interface type as 1 Gbps Ethernet.
slot	Slot number you want to configure.
port	Port number of the interface you want to configure.
port2	Last port number in a range of ports you want to configure.
Mbps	Peak flood rate, in megabits per second (Mbps). Valid ranges: 0–8 for 10 Mbps or Ethernet (OmniSwitch 7700/7800/8800) 0–9 for 10 Mbps or Ethernet (OmniSwitch 6600 Family) 0–98 for 100 Mbps or Fast Ethernet (OmniSwitch 7700/7800/8800) 0–99 for 100 Mbps or Fast Ethernet (OmniSwitch 6600 Family) 0–996 for Gigabit Ethernet (OmniSwitch 7700/7800/8800) 0–999 for Gigabit Ethernet (OmniSwitch 6600 Family) 0–9999 for 10 Gigabit Ethernet (OmniSwitch 8800)

Defaults

parameter	default
Mbps (10/100 ports on OmniSwitch 7700/7800/8800)	47
Mbps (10/100 ports on OmniSwitch 6600 Family)	42
Mbps (100 Mbps ports on OmniSwitch 6600-U24)	42
Mbps (Gigabit Ethernet)	496
Mbps (10 Gigabit Ethernet)	997

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- On OmniSwitch 6600, 7700, and 8800 switches the flood rate configured must be less than the line speed.

- You can only configure one slot at a time. Repeat the command to configure additional slots.
- The interfaces flood rate command sets the maximum *egress* flood rate on OmniSwitch 6600, 7700, 7800, and 8800. The maximum *ingress* flood rate is 5 Mbps per Network Interface (NI).
- The flood rate cannot be accurately set for smaller or larger sized packets. The accuracy/resolution is limited because the switch makes an internal assumption of packet size when it converts bits/seconds to packets/seconds for the hardware.

Examples

```
-> interfaces 3/1 flood rate 400
-> interfaces 3 flood rate 400
-> interfaces 3/1-4 flood rate 400
```

Release History

Release 5.1; command was introduced.

Related Commands

show interfaces flood rate	Displays interface peak flood rate settings.
interfaces flood	Enables maximum flood rate on an interface.
interfaces flood multicast	Enables/disables flood multicasting on an interface.

MIB Objects

```
esmConfTable
   esmPortMaxFloodRate
```

10gig slot

Configures which port will be primary (active) on a 10 Gigabit module.

10gig slot *slot* **{phy-a | phy-b}**

Syntax Definitions

slot	Slot number you want to configure.
phy-a	Sets Port 1 (phy-A) as the active port.
phy-b	Sets Port 12 (phy-B) as the active port.

Defaults

parameter	default
phy-a | phy-b	**phy-a**

Platforms Supported

OmniSwitch 8800

Usage Guidelines

- This command is only supported on the OS8-10GNI-UR1 module in the current release.
- No confirmation message will be displayed when you execute this command. Use the **show 10gig** command to confirm your configuration.

Examples

```
-> 10gig slot 3 phy-a
```

Release History

Release 5.1; command was introduced.

Related Commands

show 10gig	Displays the status of 10 Gigabit modules on an OmniSwitch 8800.

MIB Objects

```
alcether10GigTable
   alcether10GigPrimary
```

show interfaces flow control

Displays interface flow control wait time settings.

show interfaces [ethernet | fastethernet | gigaethernet] [*slot***[/***port***[-***port2***]]] flow [control]**

Syntax Definitions

ethernet	Optional syntax. Documents the interface type as 10 Mbps Ethernet.
fastethernet	Optional syntax. Documents the interface type as 100 Mbps Ethernet.
gigaethernet	Optional syntax. Documents the interface type as 1 Gbps Ethernet.
slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.
control	Optional command syntax. It displays the same information as **show interfaces flow**.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If no slot/port numbers are entered, flow control wait time settings for all slots/ports on the switch are displayed.
- You can display a specific interface by entering the slot and port number, a range of ports by entering slot and a range of ports, display all interfaces in a slot by entering the slot number, or display all interfaces as described above.

Examples

```
-> show interfaces 3/20-24 flow
Slot/Port   Active   Wait time(usec)   Cfg-Flow     Cfg-Cross
----------+--------+----------------+--------+-----------
 13/20         -              0           Pause      MDIX
 13/21         -              0           Pause      MDIX
 13/22         -              0           Pause      MDIX
 13/23         -              0              Go      MDIX
 13/24         -              0              Go      MDIX
```

output definitions

`Slot/Port`	Interface slot and port number
`Active`	Interface status.
`Wait time`	Flow control wait time, in microseconds.
`Cfg-Flow`	Flow control status, which can be **Pause** or **Go**.
`Cfg-Cross`	The user-configured cross-over setting, which can be **Auto**, **MDI**, or **MDIX**.

Release History

Release 5.1; command was introduced.

Related Commands

interfaces flow	Enables/disables flow control.
interfaces crossover	Configures crossover settings.
flow wait time	Configures flow control wait time.

MIB Objects

```
esmConfTable
   esmPortSlot
   esmPortIF
   esmPortPauseSlotTime
   esmPortCfgCrossover
dot3PauseTable
   dot3PauseSlotTime
```

show interfaces

Displays general interface information (e.g., hardware, MAC address, input errors, output errors).

show interfaces [ethernet | fastethernet | gigaethernet] [*slot***[/***port***[-***port2***]]]**

Syntax Definitions

ethernet	Optional syntax. Documents the interface type as 10 Mbps Ethernet.
fastethernet	Optional syntax. Documents the interface type as 100 Mbps Ethernet.
gigaethernet	Optional syntax. Documents the interface type as 1 Gbps Ethernet.
slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If no slot/port numbers are entered, information for all slots/ports on the switch is displayed.
- You can display a specific interface by entering the slot and port number (e.g., 3/1).
- You can display a range of port numbers (e.g., 3/1-4).
- You can display all interfaces in a slot by entering the slot number (e.g., 3).

Examples

```
-> show interfaces 1/2
Slot/Port  1/2  :
  Operational Status     : up,
  Last Time Link Changed : FRI DEC 27 15:10:40 ,
  Number of Status Change: 1,
  Type                   : Ethernet,
  MAC address            : 00:d0:95:b2:39:85,
  BandWidth (Megabits)   : 1000,                Duplex           : Full,
  Autonegotiation        :   1  [ 1000-F 100-F 100-H 10-F 10-H ],
  Long Accept            : Enable,              Runt Accept      : Disable,
  Long Frame Size(Bytes) : 9216,                Runt Size(Bytes) : 64,
  Rx             :
  Bytes Received  :              7967624, Unicast Frames :                   0,
  Broadcast Frames:               124186, M-cast Frames  :                 290,
  UnderSize Frames:                    0, OverSize Frames:                   0,
  Lost Frames     :                    0, Error Frames   :                   0,
  CRC Error Frames:                    0, Alignments Err :                   0,
  Tx             :
  Bytes Xmitted   :            255804426, Unicast Frames :               24992,
  Broadcast Frames:              3178399, M-cast Frames  :              465789,
  UnderSize Frames:                    0, OverSize Frames:                   0,
  Lost Frames     :                    0, Collided Frames:                   0,
```

output definitions

Slot/Port	Interface slot and port.
Operational Status	Interface status (up/down).
Last Time Link Changed	The last time the configuration for this interface was changed.
Number of Status Change	The total number of times that the configuration of this interface has changed.
Type	Interface type (Ethernet/Fast Ethernet/Gigabit Ethernet).
MAC address	Interface MAC address.
Bandwidth	Bandwidth (in megabits).
Duplex	Duplex mode (Half/Full/Auto).
Autonegotiation	The auto negotiation settings for this interface.
Long Accept	Long Frames status (enable/disable).
Runt Accept	Runt Frames status (enable/disable).
Long Frame Size	Long Frame Size (in Bytes).
Runt Size	Runt Frame Size (in Bytes).
Bytes Received	Number of Bytes received.
Rx Unicast Frames	Number of unicast frames received.
Rx Broadcast Frames	Number of broadcast frames received.
Rx M-cast Frames	Number of multicast frames received.
Rx Undersize Frames	Number of undersized frames received.
Rx Oversize Frames	Number of oversized frames received.
Rx Lost Frames	Number of Lost Frames received.

output definitions (continued)

`Rx Error Frames`	Number of error frames received.
`Rx CRC Error Frames`	Number of CRC error frames received.
`Rx Alignments Err`	Number of Alignments Error frames received.
`Bytes Xmitted`	Number of Bytes transmitted.
`Tx Unicast Frames`	Number of unicast frames transmitted.
`Tx Broadcast Frames`	Number of broadcast frames transmitted.
`Tx M-cast Frames`	Number of multicast frames r transmitted.
`Tx Undersize Frames`	Number of undersized frames transmitted.
`Tx Oversize Frames`	Number of oversized frames transmitted.
`Tx Lost Frames`	Number of Lost Frames transmitted.
`Tx Collided Frames`	Number of collision frames received or transmitted.
`Tx Error Frames`	Number of error frames transmitted.

Release History

Release 5.1; command was introduced.

Related Commands

show interfaces accounting	Displays interface accounting information (e.g., packets received/ transmitted).
show interfaces counters	Displays interface counter information (e.g., unicast packets received/transmitted).
show interfaces counters errors	Displays interface error frame information (e.g., CRC errors, transit errors, receive errors).
show interfaces collisions	Displays interface collision information (e.g., number of collisions, number of retries).
show interfaces status	Displays the interface line settings (e.g., speed, mode).
show interfaces traffic	Displays interface traffic statistics (input/output bytes and packets).

MIB Objects

```
ifTable
   ifOperStatus
   ifType
   ifPhysAddress
   ifSpeed
   ifInDiscards
   IfOutDiscards
esmConfTable
   esmPortSlot
   esmPortIF
   esmPortCfgLongEnable
   esmPortCfgRuntEnable
   esmPortCfgMaxFrameSize
   esmPortCfgRuntSize
ifXTable
   ifHCInOctets
   ifHCInUcastPkts
   ifHCInBroadcastPkts
   ifHCInMulticastPkts
   IfHCOutOctets
   IfHCOutUcastPkts
   IfHCOutBroadcastPkts
   IfHCOutMulticastPkts
alcetherStatsTable
   alcetherStatsRxUndersizePkts
   alcetherStatsCRCAlignErrors
   alcetherStatsTxUndersizePkts
   alcetherStatsTxOversizePkts
   alcetherStatsTxCollisions
dot3StatsTable
   dot3StatsFrameTooLong
   dot3StatsFCSErrors
   dot3StatsLateCollisions
```

show interfaces capability

Displays default auto negotiation, speed, duplex, flow, and cross-over settings for a single port, a range of ports, or all ports on a Network Interface (NI) module.

show interfaces [ethernet | fastethernet | gigaethernet] [*slot***[/***port***[-***port2***]]] capability**

Syntax Definitions

ethernet	Optional syntax. Documents the interface type as 10 Mbps Ethernet.
fastethernet	Optional syntax. Documents the interface type as 100 Mbps Ethernet.
gigaethernet	Optional syntax. Documents the interface type as 1 Gbps Ethernet.
slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The **show interfaces capability** command displays defaults settings in two rows of data for each port. The first row of data, identified by the label **CAP**, displays the valid user-defined configuration settings available for the port. The second row, identified by the label **DEF**, displays the default settings for the port.

Examples

```
-> show interfaces 5/1 capability
Slot/Port   AutoNeg     Flow   Crossover      Speed    Duplex
----------+---------+--------+-----------+----------+----------
  5/1  CAP     EN/DIS   EN/DIS  MDI/X/Auto  10/100/1G Full/Half
  5/1  DEF         EN       EN        Auto       Auto     Auto
```

output definitions

slot	The slot number.
port	The port number
AutoNeg	In the row labeled **CAP** this field displays the valid auto negotiation configurations for the port. In the row label **DEF** this field displays the default auto negotiation settings for the port. The possible values are **EN** (enabled) or **DIS** (disabled).

output definitions (continued)

`Flow`	In the row labeled **CAP** this field displays the valid flow configurations for the port. In the row label **DEF** this field displays the default flow settings for the port. The possible values are **EN** (enabled) or **DIS** (disabled).
`Crossover`	In the row labeled **CAP** this field displays the valid cross over configurations for the port. In the row label **DEF** this field displays the default cross over settings for the port. The possible values are **Auto**, **MDI/X/Auto** (MDI/MDIX/Auto), or **--** (not configurable and/or not applicable).
`Speed`	In the row labeled **CAP** this field displays the valid line speed configurations for the port. In the row label **DEF** this field displays the default line speed settings for the port. The possible values are **10/100**, **100**, **1G**, **10/100/1G**, **10G**, or **Auto**.
`Duplex`	In the row labeled **CAP** this field displays the valid duplex configurations for the port. In the row label **DEF** this field displays the default duplex settings for the port. The possible values are **Full**, **Full/Half**, or **Auto**.

Release History

Release 5.1; command was introduced.

Related Commands

interfaces autoneg	Enables and disables auto negotiation.
interfaces flow	Enables or disables flow (pause).
interfaces crossover	Configures crossover port settings.
interfaces speed	Configures interface speed.
interfaces duplex	Configures duplex settings.
show interfaces status	Displays interface line settings.

MIB Objects

```
esmConfTable
   esmPortCfgAutoNegotiation
   esmPortCfgFlow
   esmPortCfgCrossover
   esmPortCfgSpeed
   esmPortAutoDuplexMode
```

show interfaces accounting

Displays interface accounting information (e.g., packets received/transmitted, deferred frames received).

show interfaces [ethernet | fastethernet | gigaethernet] [*slot***[/***port***[-***port2***]]] accounting**

Syntax Definitions

ethernet	Optional syntax. Documents the interface type as 10 Mbps Ethernet.
fastethernet	Optional syntax. Documents the interface type as 100 Mbps Ethernet.
gigaethernet	Optional syntax. Documents the interface type as 1 Gbps Ethernet.
slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If no slot/port numbers are entered, accounting information for all slots/ports on the switch is displayed.
- You can display a specific interface by entering the slot and port number (e.g., 3/1).
- You can display a range of port numbers (e.g., 3/1-4).
- You can display all interfaces in a slot by entering the slot number (e.g., 3).

Examples

```
-> show interfaces 1/2 accounting
1/2 ,
     Rx undersize packets         =                    0,
     Tx undersize packets         =                    0,
     Rx oversize packets          =                    0,
     Tx oversize packets          =                    0,
     Rx packets 64 Octets         =              3073753,
     Rx packets 65To127 Octets    =               678698,
     Rx packets 128To255 Octets   =                21616,
     Rx packets 256To511 Octets   =                21062,
     Rx packets 512To1023 Octets  =                    2,
     Rx packets 1024To1518 Octets =                   84,
     Rx packets 1519to4095 Octets =                    0,
     Rx packets 4096ToMax Octets  =                    0,
     Rx Jabber frames             =                    0
```

output definitions

`Rx undersize packets`	Number of undersized packets received.
`Tx undersize packets`	Number of undersized packets transmitted.
`Rx oversize packets`	Number of oversized packets received.
`Tx oversize packets`	Number of oversized packets transmitted.
`Rx packets Octets`	Number of packets received in each listed octet range.
`Rx Jabber frames`	Number of jabber packets received (longer than 1518 octets).
`Tx deferred frames`	Number of packets for which transmission was delayed (Ethernet only).

Release History

Release 5.1; command was introduced.

Related Commands

show interfaces	Displays general interface information (e.g., hardware, MAC address, input/output errors).
show interfaces counters	Displays interface counter information (e.g., unicast packets received/transmitted).

MIB Objects

```
esmConfTable
   esmPortSlot
   esmPortIF
dot3StatsTable
   dot3StatsFrameTooLong
   dot3StatsDeferredTransmissions
alcetherStatsTable
   alcetherStatRxsUndersizePkts
   alcetherStatTxsUndersizePkts
   alcetherStatsTxOversizePkts
   alcetherStatsPkts64Octets
   alcetherStatsPkts65to127Octets
   alcetherStatsPkts128to255Octets
   alcetherStatsPkts256to511Octets
   alcetherStatsPkts512to1023Octets
   alcetherStatsPkts1024to1518Octets
   gigaEtherStatsPkts1519to4095Octets
   gigaEtherStatsPkts4096to9215Octets
   alcetherStatsRxJabber
```

show interfaces counters

Displays interface counters information (e.g., unicast, broadcast, multi-cast packets received/transmitted).

show interfaces [ethernet | fastethernet | gigaethernet] [*slot***[/***port***[-***port2***]]] counters**

Syntax Definitions

ethernet	Optional syntax. Documents the interface type as 10 Mbps Ethernet.
fastethernet	Optional syntax. Documents the interface type as 100 Mbps Ethernet.
gigaethernet	Optional syntax. Documents the interface type as 1 Gbps Ethernet.
slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If no slot/port numbers are entered, counter information for all slots/ports on the switch is displayed.
- You can display a specific interface by entering the slot and port number (e.g., 3/1).
- You can display a range of port numbers (e.g., 3/1-4).
- You can display all interfaces in a slot by entering the slot number (e.g., 3).
- These counters do not apply to Gigabit Ethernet traffic.

Examples

```
-> show interfaces 3/1 counters

InOctets      = 54367578586897979,  OutOctets     = 5.78E19,
InUcastPkts   = 55654265276,        OutUcastPkts  = 5.78E20,
InMcastPkts   = 58767867868768777,  OutMcastPkts  = 5465758756856,
InBcastPkts   = 576567567567567576, OutBcastPkts  = 786876,
InPauseFrames = 567798768768767,    OutPauseFrames= 786876,
```

output definitions

InOctets	Number of octets received.
OutOctets	Number of octets transmitted.
InUcastPkts	Number of unicast packets received.
OutUcastPkts	Number of unicast packets transmitted.
InMcastPkts	Number of multicast packets received.
OutMcastPkts	Number of unicast packets transmitted.
InBcastPkts	Number of broadcast packets received.
OutBcastPkts	Number of unicast packets transmitted.
InPauseFrames	Number of MAC control frames received.
OutPauseFrames	Number of MAC control frames transmitted.

Release History

Release 5.1; command was introduced.

Related Commands

show interfaces counters errors	Displays interface error frame information (e.g., CRC errors, transit errors, receive errors).

MIB Objects

```
esmConfTable
   esmPortSlot
   esmPortIF
ifXTable
   IfHCInOctets
   IfHCOutOctets
   IfHCInUcastPkts
   IfHCOutUcastPkts
   IfHCInMulticastPkts
   IfHCOutMulticastPkts
   IfHCInBroadcastPkts
   IfHCOutBroadcastPkts
dot3PauseTable
   dot3InPauseFrame
   dot3OutPauseFrame
```

show interfaces counters errors

Displays interface error frame information (e.g., CRC errors, transit errors, receive errors).

show interfaces [ethernet | fastethernet | gigaethernet] [*slot***[/***port***[-***port2***]]] counters errors**

Syntax Definitions

ethernet	Optional syntax. Documents the interface type as 10 Mbps Ethernet.
fastethernet	Optional syntax. Documents the interface type as 100 Mbps Ethernet.
gigaethernet	Optional syntax. Documents the interface type as 1 Gbps Ethernet.
slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If no slot/port numbers are entered, counter error information for all slots/ports on the switch is displayed.
- You can display a specific interface by entering the slot and port number (e.g., 3/1).
- You can display a range of port numbers (e.g., 3/1-4).
- You can display all interfaces in a slot by entering the slot number (e.g., 3).
- These counters do not apply to Gigabit Ethernet traffic.

Examples

```
-> show interfaces 2/1 counters errors

02/01,
  Alignments Errors = 6.45E13,  FCS Errors = 7.65E12
  IfInErrors        = 6435346,  IfOutErrors= 5543,
  Undersize pkts    = 867568, Oversize pkts= 5.98E8
```

output definitions

`Slot/Port`	Interface slot and port number.
`Alignments Errors`	Number of Alignments errors.
`FCS Errors`	Number of Frame Check Sequence errors.
`IfInErrors`	Number of transmitted error frames.
`IfOutErrors`	Number of received error frames.
`Undersize pkts`	Number of undersized packets.
`Oversize pkts`	Number of oversized packets (more than 1518 octets).

Release History

Release 5.1; command was introduced.

Related Commands

show interfaces counters	Displays interface counters information (e.g., unicast, broadcast, multi-cast packets received/transmitted).

MIB Objects

```
esmConfTable
   esmPortSlot
   esmPortIF
ifTable
   ifInErrors
   ifOutErrors
alcetherStatsTable
   alcetherStatsRxUndersizePkts
dot3StatsTable
   dot3StatsAlignmentErrors
   dot3StatsFCSErrors
   dot3StatsFrameTooLong
```

show interfaces collisions

Displays interface collision information (e.g., number of collisions, number of retries).

show interfaces [ethernet | fastethernet | gigaethernet] [*slot***[/***port***[-***port2***]]] collisions**

Syntax Definitions

ethernet	Optional syntax. Documents the interface type as 10 Mbps Ethernet.
fastethernet	Optional syntax. Documents the interface type as 100 Mbps Ethernet.
gigaethernet	Optional syntax. Documents the interface type as 1 Gbps Ethernet.
slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If no slot/port numbers are entered, collision information for all slots/ports on the switch is displayed.
- You can display a specific interface by entering the slot and port number (e.g., 3/1).
- You can display a range of port numbers (e.g., 3/1-4).
- You can display all interfaces in a slot by entering the slot number (e.g., 3).
- These counters do not apply to Gigabit Ethernet traffic.

Examples

```
-> show interfaces 2/1 collisions

02/01,
  Rx Collisions = 6.56E18,  Rx Single Collision = 345464364,
  Rx Multiple Collisions = 6325235326,  Rx Excessive Collisions = 5.65E19
```

output definitions

`Slot/Port`	Interface slot and port number.
`Tx Collisions`	Number of transmit collisions.
`Tx Single Collision`	Number of successfully transmitted frames for which transmission was inhibited by one collision.

output definitions (continued)

`Tx Multiple Collisions`	Number of successfully transmitted frames for which transmission was inhibited by multiple collisions.
`Tx Excessive Retries`	Number of frames for which transmission fails due to excessive collisions.
`Rx Collisions`	Number of received collisions.
`Rx Single Collision`	Number of successfully received frames for which reception was inhibited by one collision.
`Rx Multiple Collisions`	Number of successfully received frames for which reception was inhibited by multiple collisions.
`Rx Excessive Retries`	Number of frames for which reception fails due to excessive collisions.

Release History

Release 5.1; command was introduced.

Related Commands

show interfaces	Displays general interface information (e.g., hardware, MAC address, input errors, output errors).

MIB Objects

```
esmConfTable
   esmPortSlot
   esmPortIF
alcetherStatsTable
   alcetherStatsRxCollisions
dot3StatsTable
   dot3StatsSingleCollisionFrames
   dot3StatsMultipleCollisionFrames
   dot3StatsExcessiveCollisions
```

show interfaces status

Displays interface line settings (e.g., speed, mode).

show interfaces [ethernet | fastethernet | gigaethernet] [*slot***[/***port***[-***port2***]]] status**

Syntax Definitions

ethernet	Optional syntax. Documents the interface type as 10 Mbps Ethernet.
fastethernet	Optional syntax. Documents the interface type as 100 Mbps Ethernet.
gigaethernet	Optional syntax. Documents the interface type as 1 Gbps Ethernet.
slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If no slot/port numbers are entered, line settings for all slots/ports on the switch are displayed.
- You can display a specific interface by entering the slot and port number (e.g., 3/1).
- You can display a range of port numbers (e.g., 3/1-4).
- You can display all interfaces in a slot by entering the slot number (e.g., 3).

Examples

```
-> show interfaces 1/2 status
                        DETECTED            CONFIGURED
Slot/ AutoNego  Speed Duplex Hybrid  Speed   Duplex Hybrid  Trap
Port           (Mbps)         Type   (Mbps)         Mode   LinkUpDown
-----+--------+------+------+------+--------+------+------+------
 1/2   Enable   1000   Full    NA      Auto   Auto    NA      -
```

output definitions

Slot/Port	Interface slot/port number.
AutoNego	Auto negotiation status (Enable/Disable).
Detected Speed	Detected line speed (10/100/Auto/1000/10000 Mbps).
Detected Duplex	Detected line duplex (Half duplex/Full duplex/Auto).
Detected Hybrid Type	This field is not relevant for OmniSwitch 6600/7700/7800/8800 switches.
Configured Speed	Configured line speed (10/100/Auto/1000/10000 Mbps).
Configured Duplex	Configured line duplex (Half duplex/Full duplex/Auto).
Configured Hybrid Type	This field is not relevant for OmniSwitch 6600/7700/7800/8800 switches.
Trap Link Up/Down	Trap Link status (up/down).

Release History

Release 5.1; command was introduced.

Related Commands

trap port link	Enables/disables Trap LinkUpDown.
interfaces speed	Configures interface line speed, sets speed and duplex mode to auto-sensing.
interfaces duplex	Configures interface duplex mode.

MIB Objects

```
ifTable
   ifLinkUpDownTrapEnable
esmConfTable
   esmPortSlot
   esmPortIF
   esmPortAutoSpeed
   esmPortAutoDuplexMode
   esmPortCfgSpeed
   esmPortCfgDuplexMode
esmHybridConfTable
   esmPortCfgHybridMode
   esmPortCfgHybridType
```

show interfaces port

Displays interface port status (up or down).

show interfaces [ethernet | fastethernet | gigaethernet] [*slot***[/***port***[-***port2***]]] port**

Syntax Definitions

ethernet	Optional syntax. Documents the interface type as 10 Mbps Ethernet.
fastethernet	Optional syntax. Documents the interface type as 100 Mbps Ethernet.
gigaethernet	Optional syntax. Documents the interface type as 1 Gbps Ethernet.
slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If no slot/port numbers are entered, the status for all slots/ports on the switch is displayed.
- You can display a specific interface by entering the slot and port number.
- You can display a range of port numbers (e.g., 3/1-4).
- You can display all interfaces in a slot by entering the slot number (e.g., 3).

Examples

```
-> show interfaces 1/1 port
Slot/Port   Admin Status   Link Status                   Alias
----------+--------------+------------+----------------------------------------
  1/1         enable          down     ""
```

output definitions

`Slot/Port`	Interface slot and port number.
`Admin Status`	Port status (enable/disable).
`Link Status`	Operational status (enable/disable).
`Alias`	Interface alias.

Release History

Release 5.1; command was introduced.

Related Commands

interfaces admin	Enables/disables an interface.
interfaces alias	Configures an alias for a port.

MIB Objects

```
esmConfTable
   esmPortSlot
   esmPortIF
ifXTable
   ifAlias
ifTable
   ifAdminStatus
   ifOperStatus
```

show interfaces ifg

Displays interface inter-frame gap values.

show interfaces [ethernet | fastethernet | gigaethernet] [*slot***[/***port***[-***port2***]]] ifg**

Syntax Definitions

ethernet	Optional syntax. Documents the interface type as 10 Mbps Ethernet.
fastethernet	Optional syntax. Documents the interface type as 100 Mbps Ethernet.
gigaethernet	Optional syntax. Documents the interface type as 1 Gbps Ethernet.
slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If no slot/port numbers are entered, IFG values for all slots/ports on the switch are displayed.
- You can display a specific interface by entering the slot and port number (e.g., 3/1).
- You can display a range of port numbers (e.g., 3/1-4).
- You can display all interfaces in a slot by entering the slot number (e.g., 3).

Examples

```
-> show interfaces ifg
 Slot/Port   ifg(Bytes)
-----------+-------------
 02/01          12
 02/02          12
 02/03          12
 02/04          12
 02/05          12
 02/06          12
 02/07          12
 02/08          12
 02/09          12
 02/10          12
 02/11          12
 02/12          12
 02/13          12
 02/14          12
 02/15          12
 02/16          12
 02/17          12
 02/18          12
```

output definitions

`Slot/Port`	Interface slot and port numbers.
`ifg`	Inter-frame gap value (Gigabit Ethernet interface).

Release History

Release 5.1; command was introduced.

Related Commands

interfaces ifg	Configures the inter-frame gap value.

MIB Objects

```
esmConfTable
   esmPortSlot
   esmPortIF
   esmPortCfgIFG
```

show interfaces flood rate

Displays interface peak flood rate settings.

show interfaces [ethernet | fastethernet | gigaethernet] [*slot***[/***port***[-***port2***]]] flood rate**

Syntax Definitions

ethernet	Optional syntax. Documents the interface type as 10 Mbps Ethernet.
fastethernet	Optional syntax. Documents the interface type as 100 Mbps Ethernet.
gigaethernet	Optional syntax. Documents the interface type as 1 Gbps Ethernet.
slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If no slot/port numbers are entered, peak rate settings for all slots/ports on the switch are displayed.
- You can display a specific interface by entering the slot and port number.
- You can display a range of port numbers (e.g., 3/1-4).
- You can display all interfaces in a slot by entering the slot number only.

Examples

```
-> show interfaces flood rate

 Slot/Port   peak rate(Mb/second)   Enable
-----------+----------------------+---------------
 02/01            12               Flood only
 02/02            47               Flood only
 02/03            16               Flood only
 02/04            47               Flood only
 02/05            47               Flood only
 02/06            47               Flood only
 02/07            47               Flood only
 02/08            47               Flood only
 02/09            47               Flood only
 02/10            47               Flood only
 02/11            47               Flood only
 02/12            47               Flood only
 02/13            47               Flood only
 02/14            47               Flood only
 02/15            47               Flood only
 02/16            47               Flood only
 02/17            47               Flood only
 02/18            47               Flood only
 02/19            47               Flood only
```

output definitions

Slot/Port	Interface slot and port numbers.
Peak Rate (Mbps)	Configures peak flood rate.
Enable	Configuration enabled (Flood only/Flood Multicast/Multicast).

Release History

Release 5.1; command was introduced.

Related Commands

interfaces flood	Enables the maximum flood rate on an interface.
interfaces flood rate	Configures the peak flood rate for an interface.
interfaces flood multicast	Enables/disables flood multicasting on an interface.

MIB Objects

```
esmConfTable
   esmPortSlot
   esmPortIF
   esmPortMaxFloodRate
   esmPortFloodMcastEnable
```

show interfaces traffic

Displays interface traffic statistics.

show interfaces [ethernet | fastethernet | gigaethernet] [*slot***[/***port***[-***port2***]]] traffic**

Syntax Definitions

ethernet	Optional syntax. Documents the interface type as 10 Mbps Ethernet.
fastethernet	Optional syntax. Documents the interface type as 100 Mbps Ethernet.
gigaethernet	Optional syntax. Documents the interface type as 1 Gbps Ethernet.
slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If no slot/port numbers are entered, traffic settings for all slots/ports on the switch are displayed.
- You can display a specific interface by entering the slot and port number (e.g., 3/1).
- You can display all interfaces in a slot by entering the slot number (e.g., 3).

Examples

```
-> show interfaces traffic

Slot/Port   Input packets     Input bytes      Output packets    Output bytes
---------+----------------+----------------+----------------+----------------

02/01                0                0         0                0
02/02                0                0         0                0
02/03                0                0         0                0
03/01                0                0         0                0
03/02                0                0         0                0
```

output definitions

Slot/Port	Interface slot and port numbers.
Input packets	Input packets detected.
Input bytes	Input bytes detected.
Output packets	Output packets detected.
Output bytes	Output bytes detected.

Release History

Release 5.1; command was introduced.

Related Commands

show interfaces	Displays general interface information (e.g., hardware, MAC address, input/output errors).
show interfaces counters	Displays interface counter information (e.g., unicast packets received/transmitted).

MIB Objects

```
esmConfTable
   esmPortSlot
   esmPortIF
ifXTable
   ifHCInOctets
   ifHCInUcastPkts
   ifHCInMulticastPkts
   ifHCInBroadcastPkts
   ifHCOutOctets
   ifHCOutUcastPkts
   ifHCOutMulticastPkts
   ifHCOutBroadcastPkts
```

show 10gig

Displays the status of 10 Gigabit modules in an OmniSwitch 8800 chassis.

show 10gig [slot *slot***]**

Syntax Definitions

slot	Slot number you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 8800

Usage Guidelines

- This command is only supported on the OS8-10GNI-UR1 module in the current release.
- If you do not specify a slot number then the status of all 10 Gigabit modules in a chassis will be displayed.

Examples

```
-> show 10gig
Slot  7: PHY A primary
Slot  9: PHY A primary

-> show 10gig slot  9
Slot  9: PHY A primary

-> show 10gig slot 10
Slot 10 is not a 10 GIG NI

-> show 10gig slot 11
Slot 11 is not powered up yet
```

Release History

Release 5.1; command was introduced.

Related Commands

10gig slot	Configures which port will be active on a 10 Gigabit module.

MIB Objects

```
alcether10GigTable
   alcether10GigPrimary
```

debug interfaces set backpressure

Enables and disables fabric back pressure on a Network Interface (NI) or an entire chassis.

debug interfaces set [*slot*] **backpressure {enable | disable}**

Syntax Definitions

slot	The slot number to enable or disable fabric back pressure. The valid range is 1–8 on an OmniSwitch 7700, 1–16 on an OmniSwitch 7800, and 1–16 on an OmniSwitch 8800.
enable	Enables fabric backpressure.
disable	Disables fabric backpressure.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

If the slot number is not specified then the switch back pressure feature will be enabled or disabled on an entire chassis.

Examples

```
-> debug interfaces set backpressure enable
-> debug interfaces set backpressure disable
-> debug interfaces set 3 backpressure enable
-> debug interfaces set 3 backpressure disable
```

Release History

Release 5.1; command was introduced.

Related Commands

debug interfaces backpressure	Displays if fabric back pressure is enabled or disabled on an NI or on an entire chassis.

MIB Objects

N/A

debug interfaces backpressure

Displays if fabric back pressure is enabled or disabled on a Network Interface (NI) or an entire chassis.

debug interfaces [*slot*] **backpressure**

Syntax Definitions

slot	The slot number to display the fabric back pressure state. The valid range is 1–8 on an OmniSwitch 7700, 1–16 on an OmniSwitch 7800, and 1–16 on an OmniSwitch 8800

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

If the slot number is not specified then the switch back pressure state will be displayed for an entire chassis.

Examples

```
-> debug interfaces backpressure
 Slot   Backpressure
------+--------------
 1      disable
 2      disable
 3      enable
 4      enable
 5      disable
 6      disable
 7      disable
 8      enable
-> debug interfaces 3 backpressure
 Slot   Backpressure
------+--------------
 3      enable
```

output definitions

Slot	The slot number of the NI.
Backpressure	Displays if the switch fabric back pressure feature is enabled or disabled on this NI. (The default is disabled.)

Release History

Release 5.1; command was introduced.

Related Commands

debug interfaces set backpressure	Enables and disables fabric back pressure on an NI or on an entire chassis.

MIB Objects

N/A

20 Port Mobility Commands

Port mobility allows dynamic VLAN port assignment based on VLAN rules that are applied to port traffic. By default, all switch ports are non-mobile ports that are manually assigned to a specific VLAN and can only belong to one VLAN at a time. When a port is defined as a mobile port, switch software compares traffic coming in on the port with configured VLAN rules. If any of the mobile port traffic matches any of the VLAN rules, the port and the matching traffic become a member of that VLAN. It is also possible for mobile ports to belong to more than one VLAN, when the port carries multiple traffic types that match different rules on different VLANs.

VLANs do not have a mobile or non-mobile distinction and there is no overall switch setting to invoke the mobile port feature. Instead, mobility is enabled on individual switch ports and rules are defined for individual VLANs to capture mobile port traffic. This chapter includes descriptions of Command Line Interface (CLI) commands used to define VLAN rules, enable or disable mobile port properties, and display mobile port configuration information.

MIB information for port mobility commands is as follows:

Filename: alcatelIND1GroupMobility.MIB
Module: ALCATEL-IND1-GROUP-MOBILITY-MIB

A summary of the available commands is listed here:

vlan dhcp mac
vlan dhcp mac range
vlan dhcp port
vlan dhcp generic
vlan binding mac-ip-port
vlan binding mac-port-protocol
vlan binding mac-port
vlan binding mac-ip
vlan binding ip-port
vlan binding port-protocol
vlan mac
vlan mac range
vlan ip
vlan ipx
vlan protocol
vlan user
vlan port
vlan port mobile
vlan port default vlan restore
vlan port default vlan
vlan port authenticate
vlan port 802.1x
show vlan rules
show vlan port mobile

vlan dhcp mac

Defines a DHCP MAC address rule for an existing VLAN. If a DHCP frame received on any mobile port contains a source MAC address that matches the MAC address specified in the rule, the frame's mobile port is temporarily assigned to the rule's VLAN.

vlan *vid* **dhcp mac** *mac_address*

vlan *vid* **no dhcp mac** *mac_address*

Syntax Definitions

vid	VLAN ID number (1–4094).
mac_address	Source MAC address (e.g., 00:00:39:59:f1:0C).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of this command to delete a DHCP MAC address rule from the specified VLAN.
- Port mobility software checks for and processes DHCP traffic first on an active mobile port. When a mobile port receives a DHCP frame that matches a DHCP rule, the port is temporarily assigned to the VLAN long enough to forward the DHCP requests within the VLAN broadcast domain. The source MAC address of the DHCP frame, however, is not learned for that VLAN port association.
- Once a DHCP device has obtained an IP address, its non-DHCP traffic must match other VLAN rules within the same VLAN for the device to remain a member of that VLAN. If this match occurs, then the frame source is learned in the matching rule VLAN.
- DHCP rules are most often used in combination with IP network address rules. A DHCP client has an IP address of all zeros (0.0.0.0) until it receives an IP address from a DHCP server, so it would not match any IP network address rules.
- Binding rules, MAC address rules, and protocol rules also capture DHCP client traffic. The exception to this is binding rules that specify an IP address as part of the rule, similar to IP network address rule definitions.
- Rules are only assigned to existing VLANs. Use the **vlan** command to create a new VLAN.

Examples

```
-> vlan 10 dhcp mac 00:00:39:59:0a:0c
-> vlan 20 dhcp mac 00:00:39:4f:f1:22
-> vlan 10 no dhcp mac 00:00:39:59:0a:0c
```

Release History

Release 5.1; command was introduced.

Related Commands

vlan dhcp mac range	Defines a DHCP MAC address range rule for an existing VLAN. Mobile ports that receive DHCP frames with a source MAC address that falls within the range specified by this rule are temporarily assigned to the VLAN.
vlan dhcp port	Defines a DHCP port rule for an existing VLAN. The mobile port specified by this rule is temporarily assigned to the VLAN when it receives DHCP frames.
vlan dhcp generic	Defines a generic DHCP rule for an existing VLAN. Mobile ports that receive DHCP frames that do not match other DHCP rules are temporarily assigned to the VLAN.
show vlan	Displays existing VLANs.
show vlan rules	Displays rules defined for VLANs.

MIB Objects

```
vDhcpMacRuleTable
   vDhcpMacRuleAddr
   vDhcpMacRuleVlanId
   vDhcpMacRuleStatus
```

vlan dhcp mac range

Defines a DHCP MAC range rule for an existing VLAN. If a DHCP frame contains a source MAC address that matches the low or high end MAC or falls within the range defined by the low and high end MAC, the frame's mobile port is temporarily assigned to the rule's VLAN.

vlan *vid* **dhcp mac range** *low_mac_address high_mac_address*

vlan *vid* **no dhcp mac range** *low_mac_address*

Syntax Definitions

vid	VLAN ID number (1–4094).
low_mac_address	MAC address that defines the low end of the range (e.g., 00:00:39:59:f1:00).
high_mac_address	MAC address that defines the high end of the range (e.g., 00:00:39:59:f1:90).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of this command to delete a DHCP MAC range rule from the specified VLAN. It is only necessary to specify the low end MAC to identify which rule to delete; the high end MAC is not required.
- Only valid source MAC addresses are allowed for the low and high end boundary MACs. For example, multicast addresses (e.g., 01:00:00:c5:09:1a) are ignored even if they fall within a specified MAC range. To allow the use of a multicast address as either the low or high end boundary MAC would cause misleading DHCP MAC range rule results.
- Port mobility software checks for and processes DHCP traffic first on an active mobile port. When a mobile port receives a DHCP frame that matches a DHCP rule, the port is temporarily assigned to the VLAN long enough to forward the DHCP requests within the VLAN broadcast domain. The source MAC address of the DHCP frame, however, is not learned for that VLAN port association.
- Once a DHCP device has obtained an IP address, its non-DHCP traffic must match other VLAN rules within the same VLAN for the device to remain a member of that VLAN. If this match occurs, then the frame source is learned in the matching rule VLAN.
- DHCP rules are most often used in combination with IP network address rules. A DHCP client has an IP address of all zeros (0.0.0.0) until it receives an IP address from a DHCP server, so it would not match any IP network address rules.

- Binding rules, MAC address rules, and protocol rules also capture DHCP client traffic. The exception to this is binding rules that specify an IP address as part of the rule, similar to IP network address rule definitions.
- Rules are only assigned to existing VLANs. Use the **vlan** command to create a new VLAN.

Examples

```
-> vlan 10 dhcp mac range 00:00:39:59:0a:0c 00:00:39:59:0a:0f
-> vlan 10 no dhcp mac range 00:00:39:59:0a:0c
```

Release History

Release 5.1; command was introduced.

Related Commands

vlan dhcp mac	Defines a DHCP MAC address rule for an existing VLAN. Mobile ports that receive DHCP frames with a source MAC address that matches the address specified by this rule are temporarily assigned to the VLAN.
vlan dhcp port	Defines a DHCP port rule for an existing VLAN. The mobile port specified by this rule is temporarily assigned to the VLAN when it receives DHCP frames.
vlan dhcp generic	Defines a generic DHCP rule for an existing VLAN. Mobile ports that receive DHCP frames that do not match other DHCP rules are temporarily assigned to the VLAN.
show vlan	Displays existing VLANs.
show vlan rules	Displays rules defined for VLANs.

vlan dhcp port

Defines a DHCP port rule for an existing VLAN. If a DHCP frame is received on a mobile port that matches the port specified in the rule, the mobile port is temporarily assigned to the rule's VLAN.

vlan *vid* **dhcp port** *slot/port*

vlan *vid* **no dhcp port** *slot/port*

Syntax Definitions

vid	VLAN ID number (1–4094).
slot/port	The slot number for the module and the physical mobile port number on that module (e.g., 3/1 specifies port 1 on slot 3). To enter multiple slots and ports in a single command, use a hyphen to specify a range of ports (e.g., 3/1-16) and a space to specify multiple slots (e.g., 3/1-16 5/10-20 8/2-9).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of this command to delete a DHCP port rule from the specified VLAN.
- Port mobility software checks for and processes DHCP traffic first on an active mobile port. When a mobile port receives a DHCP frame that matches a DHCP rule, the port is temporarily assigned to the VLAN long enough to forward the DHCP requests within the VLAN broadcast domain. The source MAC address of the DHCP frame, however, is not learned for that VLAN port association.
- Once a DHCP device has obtained an IP address, its non-DHCP traffic must match other VLAN rules within the same VLAN for the device to remain a member of that VLAN. If this match occurs, then the frame source is learned in the matching rule VLAN.
- DHCP rules are most often used in combination with IP network address rules. A DHCP client has an IP address of all zeros (0.0.0.0) until it receives an IP address from a DHCP server, so it would not match any IP network address rules.
- Binding rules, MAC address rules, and protocol rules also capture DHCP client traffic. The exception to this is binding rules that specify an IP address as part of the rule, similar to IP network address rule definitions.
- Rules are only assigned to existing VLANs. Use the **vlan** command to create a new VLAN.

Examples

```
-> vlan 10 dhcp port 3/1
-> van 20 dhcp port 4/1-16
-> vlan 30 dhcp port 5/1-32 6/5-10 8/7-22
-> vlan 10 no dhcp port 3/1
-> vlan 20 no dhcp port 4/1-16
```

Release History

Release 5.1; command was introduced.

Related Commands

vlan dhcp mac	Defines a DHCP MAC address rule for an existing VLAN. Mobile ports that receive DHCP frames with a source MAC address that matches the address specified by this rule are temporarily assigned to the VLAN.
vlan dhcp mac range	Defines a DHCP MAC address range rule for an existing VLAN. Mobile ports that receive DHCP frames with a source MAC address that falls within the range specified by this rule are temporarily assigned to the VLAN.
vlan dhcp generic	Defines a generic DHCP rule for an existing VLAN. Mobile ports that receive DHCP frames that do not match other DHCP rules are temporarily assigned to the VLAN.
show vlan	Displays existing VLANs.
show vlan rules	Displays rules defined for VLANs.

MIB Objects

```
vDhcpPortRuleTable
   vDhcpPortRuleIfIndex
   vDhcpPortRuleVlanId
   vDhcpPortRuleStatus
```

vlan dhcp generic

Defines a DHCP rule for an existing VLAN. If a DHCP frame does not match any other DHCP rule criteria, the frame's mobile port is temporarily assigned to the DHCP generic rule VLAN.

vlan *vid* **dhcp generic**

vlan *vid* **no dhcp generic**

Syntax Definitions

vid	VLAN ID number (1–4094).

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Defaults

N/A

Usage Guidelines

- Use the **no** form of this command to delete a DHCP generic rule from the specified VLAN.
- Only one DHCP generic rule per switch is allowed.
- Port mobility software checks for and processes DHCP traffic first on an active mobile port. When a mobile port receives a DHCP frame that matches a DHCP rule, the port is temporarily assigned to the VLAN long enough to forward the DHCP requests within the VLAN broadcast domain. The source MAC address of the DHCP frame, however, is not learned for that VLAN port association.
- Once a DHCP device has obtained an IP address, its non-DHCP traffic must match other VLAN rules within the same VLAN for the device to remain a member of that VLAN. If this match occurs, then the frame source is learned in the matching rule VLAN.
- DHCP rules are most often used in combination with IP network address rules. A DHCP client has an IP address of all zeros (0.0.0.0) until it receives an IP address from a DHCP server, so it would not match any IP network address rules.
- Binding rules, MAC address rules, and protocol rules also capture DHCP client traffic. The exception to this is binding rules that specify an IP address as part of the rule, similar to IP network address rule definitions.
- Rules are only assigned to existing VLANs. Use the **vlan** command to create a new VLAN.

Examples

```
-> vlan 10 dhcp generic
-> vlan 10 no dhcp generic
```

Release History

Release 5.1; command was introduced.

Related Commands

vlan dhcp port	Defines a DHCP port rule for an existing VLAN. The mobile port specified by this rule is temporarily assigned to the VLAN when it receives DHCP frames.
vlan dhcp mac	Defines a DHCP MAC address rule for an existing VLAN. Mobile ports that receive DHCP frames with a source MAC address that matches the address specified by this rule are temporarily assigned to the VLAN.
vlan dhcp mac range	Defines a DHCP MAC address range rule for an existing VLAN. Mobile ports that receive DHCP frames with a source MAC address that falls within the range specified by this rule are temporarily assigned to the VLAN.
show vlan	Displays existing VLANs.
show vlan rules	Displays rules defined for VLANs.

MIB Objects

```
vDhcpGenericRuleTable
   vDhcpGenericRuleVlanId
   vDhcpGenericRuleStatus
```

vlan binding mac-ip-port

Defines a binding MAC-IP-port rule for an existing VLAN. This rule restricts VLAN membership to a device that matches all criteria of the rule. Device frames received on the specified mobile port must also contain a source MAC address and source IP address that matches the MAC and IP address specified in the rule.

vlan *vid* **binding mac-ip-port** *mac_address ip_address slot/port*

vlan *vid* **no binding mac-ip-port** *mac_address*

Syntax Definitions

vid	VLAN ID number (1–4094).
mac_address	Source MAC address (e.g., 00:00:39:59:f1:0c).
ip_address	IP address (e.g., 21.0.0.10, 176.23.100.2)
slot/port	The slot number for the module and the physical mobile port number on that module (e.g., 3/1 specifies port 1 on slot 3).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of this command to delete a binding MAC-IP-port rule from the specified VLAN. It is only necessary to specify a MAC address to identify which rule to delete; the IP address and slot/port are not required.
- If only the frame's source MAC address matches the MAC address specified in this rule, a binding rule violation occurs and the device frame is blocked and its port is *not* assigned to the VLAN. There is no further attempt to compare the frame to other VLAN rules.
- If only the frame's source IP address matches the MAC address specified in this rule, a binding rule violation occurs and the device frame is blocked and its port is *not* assigned to the VLAN. There is no further attempt to compare the frame to other VLAN rules.
- If only the frane's port matches the port specified in this rule, the frame is allowed but the port is still not assigned to the VLAN. The frame is then compared to other VLAN rules for possible matches.
- A binding rule applies to traffic from a specific device. Therefore, a separate binding rule is required for each device.
- Binding MAC-IP-port rules have the highest precedence of all the rules.
- Rules are only assigned to existing VLANs. Use the **vlan** command to create a new VLAN.

Examples

```
-> vlan 10 binding mac-ip-port 00:00:39:59:0a:0c 21.0.0.10 5/1
-> van 20 no binding mac-ip-port 00:00:39:4f:f1:22
```

Release History

Release 5.1; command was introduced.

Related Commands

show vlan	Displays existing VLANs.
show vlan rules	Displays rules defined for VLANs.

MIB Objects

```
vMacPortIpBRuleTable
   vMacPortIpBRuleMac
   vMacPortIpBRuleIfIndex
   vMacPortIpBruleIp
   vMacPortIpBRuleVlanId
   vMacPortIPBRuleStatus
```

vlan binding mac-port-protocol

Defines a binding MAC-port-protocol rule for an existing VLAN. This rule restricts VLAN membership to a device that matches all criteria of the rule. Device frames received on the specified mobile port must contain a source MAC address and protocol type that matches the MAC address and protocol type value specified in the rule.

vlan *vid* **binding mac-port-protocol** *mac_address slot/port* **{ip-e2 | ip-snap | ipx-e2 | ipx-novell | ipx-llc | ipx-snap | decnet | appletalk | ethertype** *type* **| dsapssap** *dsap/ssap* **| snap** *snaptype***}**

vlan *vid* **no binding mac-port-protocol** *mac_address* **{ip-e2 | ip-snap | ipx-e2 | ipx-novell | ipx-llc | ipx-snap | decnet | appletalk | ethertype** *type* **| dsapssap** *dsap/ssap* **| snap** *snaptype***}**

Syntax Definitions

vid	VLAN ID number (1–4094).
mac_address	Source MAC address (e.g., 00:00:39:59:f1:0c).
slot/port	The slot number for the module and the physical mobile port number on that module (e.g., 3/1 specifies port 1 on slot 3).
ip-e2	IP Ethernet-II protocol. Also captures Address Resolution Protocol (ARP).
ip-snap	IP SNAP protocol.
ipx-e2	IPX Ethernet-II protocol.
ipx-novell	IPX Novell (802.3) protocol.
ipx-llc	IPX LLC (802.2) protocol.
ipx-snap	IPX SNAP protocol.
decnet	DECNET Phase IV (6003) protocol.
appletalk	AppleTalk protocol. Also captures Datagram Delivery Protocol (DDP) and AppleTalk ARP (AARP).
type	A two-byte hex value between 0x600 and 0xffff that defines an Ethernet type (e.g., 0600, 0806, 6002).
dsap/ssap	A one-byte hex value between 0x00 and 0xff that defines Destination Service Access Protocol (DSAP) and Source Service Access Protocol (SSAP) header values. Specify both a DSAP and an SSAP value for this parameter variable (e.g., F0/F0, 04/04, BC/BC).
snaptype	A two-byte hex value between 0x600 and 0xffff that defines a Subnetwork Access Protocol (SNAP) protocol.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of this command to delete a binding MAC-port-protocol rule from the specified VLAN. It is only necessary to specify a MAC address and protocol type to identify which rule to delete; the slot/port is not required.
- If only the frame's source MAC address matches the MAC address specified in this rule, a binding rule violation occurs and the device frame is blocked and its port is not assigned to the VLAN. There is no further attempt to compare the frame to other VLAN rules.
- If only the frame's port and/or protocol matches the port and/or protocol specified in this rule, the frame is allowed but the port is still not assigned to the VLAN. The frame is then compared to other VLAN rules for possible matches.
- A binding rule applies to a specific device. Therefore, a separate binding rule is required for each device.
- Binding MAC-port-protocol rules take precedence over all other rules, except binding MAC-IP-port rules.
- Rules are only assigned to existing VLANs. Use the **vlan** command to create a new VLAN.

Examples

```
-> vlan 10 binding mac-port-protocol 00:00:39:59:0a:0c 5/1 ipx-e2
-> vlan 20 binding mac-port-protocol 00:00:39:4f:f1:22 9/3 dsapssap f0/f0
-> vlan 20 no binding mac-port-protocol 00:00:39:4f:f1:22
```

Release History

Release 5.1; command was introduced.

Related Commands

show vlan	Displays existing VLANs.
show vlan rules	Displays rules defined for VLANs.

MIB Objects

```
vMacPortProtoBRuleTable
   vMacPortProtoBRuleMacAddr
   vMacPortProtoBRuleIfIndex
   vMacPortProtoBRuleProtoClass
   vMacPortProtoBRuleEthertype
   vMacPortProtoBRuleDsapSsap
   vMacPortProtoBRuleVlanId
   vMacPortProtoBRuleStatus
```

vlan binding mac-port

Defines a binding MAC-port rule for an existing VLAN. This rule restricts VLAN membership to a device that matches all criteria of the rule. Device frames received on the specified mobile port must contain a source MAC address that matches the MAC address specified in the rule.

vlan *vid* **binding mac-port** *mac_address slot/port*

vlan *vid* **no binding mac-port** *mac_address*

Syntax Definitions

vid	VLAN ID number (1–4094).
mac_address	Source MAC address (e.g., 00:00:39:59:f1:0c).
slot/port	The slot number for the module and the physical mobile port number on that module (e.g., 3/1 specifies port 1 on slot 3).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of this command to delete a binding MAC-port rule from the specified VLAN. It is only necessary to enter a MAC address to identify which rule to delete; the slot/port is not required.
- If only the frame's source MAC address matches the MAC address specified in this rule, a binding rule violation occurs and the device frame is blocked and its port is not assigned to the VLAN. There is no further attempt to compare the frame to other VLAN rules.
- If only the frame's port matches the port specified in this rule, the frame is allowed but the port is still not assigned to the VLAN. The frame is then compared to other VLAN rules for possible matches.
- A binding rule applies to a specific device. Therefore, a separate binding rule is required for each device.
- Binding MAC-port rules take precedence over all other rules, except binding MAC-port-protocol and binding MAC-IP-port rules.
- Rules are only assigned to existing VLANs. Use the **vlan** command to create a new VLAN.

Examples

```
-> vlan 10 binding mac-port 00:00:39:59:0a:0c 5/1
-> vlan 20 no binding mac-port 00:00:39:4f:f1:22
```

Release History

Release 5.1; command was introduced.

Related Commands

show vlan	Displays existing VLANs.
show vlan rules	Displays rules defined for VLANs.

MIB Objects

```
vMacPortBRuleTable
   vMacPortBRuleMac
   vMacPortBRuleIfIndex
   vMacPortBRuleVlanId
   vMacPortBRuleStatus
```

vlan binding mac-ip

Defines a binding MAC-IP for a VLAN. This rule restricts VLAN membership to a device that matches all criteria of the rule. Device frames received on any mobile port must contain a source MAC address and source IP address that matches the MAC and IP addresses specified in the rule.

vlan *vid* **binding mac-ip** *mac_address ip_address*

vlan *vid* **no binding mac-ip** *mac_address*

Syntax Definitions

vid	VLAN ID number (1–4094).
mac_address	Source MAC address (e.g., 00:00:39:59:f1:0c).
ip_address	IP address (e.g., 21.0.0.10, 176.23.100.2).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of this command to delete a binding MAC-IP rule from the specified VLAN. It is only necessary to enter a MAC address to identify which rule to delete; the IP address is not required.
- If only the frame's source MAC address matches the MAC address specified in this rule, a binding rule violation occurs and the device frame is blocked and its port is not assigned to the VLAN. There is no further attempt to compare the frame to other VLAN rules.
- If only the frame's source IP address matches the IP address specified in this rule, a binding rule violation occurs and the device frame is blocked and its port is not assigned to the VLAN. There is no further attempt to compare the frame to other VLAN rules.
- A binding rule applies to a specific device. Therefore, a separate binding rule is required for each device.
- Binding MAC-IP rules take precedence over all other rules, except binding MAC-port rules, binding MAC-port-protocol, and binding MAC-IP-port.
- Rules are only assigned to existing VLANs. Use the **vlan** command to create a new VLAN.

Examples

```
-> vlan 10 binding mac-ip 00:00:39:59:0a:0c 21.0.0.10
-> vlan 20 no binding mac-ip 00:00:39:4f:f1:22
```

Release History

Release 5.1; command was introduced.

Related Commands

show vlan	Displays existing VLANs.
show vlan rules	Displays rules defined for VLANs.

MIB Objects

```
vMacIpBRuleTable
   vMacIpBRuleMac
   vMacIpBRuleIp
   vMacIpBRuleVlanId
   vMacIpBRuleStatus
```

vlan binding ip-port

Defines a binding IP-port rule for an existing VLAN. This rule restricts VLAN membership to a device that matches all criteria of the rule. Device frames received on the specified mobile port must contain a source IP address that matches the IP address specified in the rule.

vlan *vid* **binding ip-port** *ip_address slot/port*

vlan *vid* **no binding ip-port** *ip_address*

Syntax Definitions

vid	VLAN ID number (1–4094).
ip_address	IP address (e.g., 21.0.0.10, 176.23.100.2)
slot/port	The slot number for the module and the physical mobile port number on that module (e.g., 3/1 specifies port 1 on slot 3).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of this command to delete a binding IP-port rule from the specified VLAN. It is only necessary to enter an IP address to identify which rule to delete; the slot/port is not required.
- If only the frame's source IP address matches the IP address specified in this rule, a binding rule violation occurs and the device frame is blocked and its port is not assigned to the VLAN. There is no further attempt to compare the frame to other VLAN rules.
- If only the frame's port matches the port specified in this rule, the frame is allowed but the port is still not assigned to the VLAN. The frame is then compared to other VLAN rules for possible matches.
- A binding rule applies to a specific device. Therefore, a separate binding rule is required for each device.
- Binding IP-port rules take precedence over all other rules, except binding MAC-IP, binding MAC-port, binding MAC-port-protocol, and binding MAC-IP-port rules.
- Rules are only assigned to existing VLANs. Use the **vlan** command to create a new VLAN.

Examples

```
-> vlan 10 binding ip-port 21.0.0.10 6/1
-> vlan 20 no binding ip-port 31.0.0.2
```

Release History

Release 5.1; command was introduced.

Related Commands

show vlan	Displays existing VLANs.
show vlan rules	Displays rules defined for VLANs.

MIB Objects

```
vPortIpBRuleTable
   vPortIpBRuleIp
   vPortIpBRuleIfIndex
   vPortIpBRuleVlanId
   vPortIpBRuleStatus
```

vlan binding port-protocol

Defines a binding port-protocol rule for an existing VLAN. This rule restricts VLAN membership to a device that matches all criteria of the rule. Device frames received on the specified mobile port must contain a protocol type that matches the protocol value specified in the rule.

vlan *vid* **binding port-protocol** *slot/port* **{ip-e2 | ip-snap | ipv6 | ipx-e2 | ipx-novell | ipx-llc | ipx-snap | decnet | appletalk | ethertype** *type* **| dsapssap** *dsap/ssap* **| snap** *snaptype***}**

vlan *vid* **no binding port-protocol** *slot/port* **{ip-e2 | ip-snap | ipx-e2 | ipx-novell | ipx-llc | ipx-snap | decnet | appletalk | ethertype** *type* **| dsapssap** *dsap/ssap* **| snap** *snaptype***}**

Syntax Definitions

vid	VLAN ID number (1–4094).
slot/port	The slot number for the module and the physical mobile port number on that module (e.g., 3/1 specifies port 1 on slot 3).
ip-e2	IP Ethernet-II protocol. Also captures Address Resolution Protocol (ARP).
ip-snap	IP SNAP protocol.
ipv6	IPv6 protocol.
ipx-e2	IPX Ethernet-II protocol.
ipx-novell	IPX Novell (802.3) protocol.
ipx-llc	IPX LLC (802.2) protocol.
ipx-snap	IPX SNAP protocol.
decnet	DECNET Phase IV (6003) protocol.
appletalk	AppleTalk protocol. Also captures Datagram Delivery Protocol (DDP) and AppleTalk ARP (AARP).
type	A two-byte hex value between 0x600 and 0xffff that defines an Ethernet type (e.g., 0600, 0806, 6002).
dsap/ssap	A one-byte hex value between 0x00 and 0xff that defines Destination Service Access Protocol (DSAP) and Source Service Access Protocol (SSAP) header values. Specify both a DSAP and an SSAP value for this parameter variable (e.g., F0/F0, 04/04, BC/BC).
snaptype	A two-byte hex value between 0x600 and 0xffff that defines a Subnetwork Access Protocol (SNAP) protocol.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of this command to delete a binding port-protocol rule from the specified VLAN.
- If only the frame's port matches the port specified in this rule, a binding rule violation occurs and the device frame is blocked and its port is not assigned to the VLAN. There is no further attempt to compare the frame to other VLAN rules.
- If only the frame's protocol matches the protocol specified in this rule, the frame is allowed but the port is still not assigned to the VLAN. The frame is then compared to other VLAN rules for possible matches.
- Binding port-protocol rules take precedence behind all other binding rules.
- Rules are only assigned to existing VLANs. Use the **vlan** command to create a new VLAN.

Examples

```
-> vlan 10 binding port-protocol 5/1 ipx-e2
-> vlan 20 binding port-protocol 7/2 dsapssap F0/F0
-> vlan 20 no binding port-protocol 7/2 dsapssap F0/F0
```

Release History

Release 5.1; command was introduced.

Related Commands

show vlan	Displays existing VLANs.
show vlan rules	Displays rules defined for VLANs.

MIB Objects

```
vPortProtoBRuleTable
   vPortProtoBRuleIfIndex
   vPortProtoBRuleProtoClass
   vPortProtoBRuleEthertype
   vPortProtoBRuleDsapSsap
   vPortProtoBRuleVlanId
   vPortProtoBRuleStatus
```

vlan mac

Defines a MAC address rule for an existing VLAN. If the source MAC address of a device matches a MAC address specified in this rule, the device and its mobile port will join the VLAN when the device starts to send traffic.

vlan *vid* **mac** *mac_address*

vlan *vid* **no mac** *mac_address*

Syntax Definitions

vid	VLAN ID number (1–4094).
mac_address	MAC address (e.g., 00:00:39:59:f1:0c).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of this command to delete a MAC address rule from the specified VLAN.
- Once a device joins a MAC address rule VLAN, then it is not eligible to join multiple VLANs even if the device traffic matches other VLAN rules.
- Mac address rules take precedence behind DHCP and binding rules.
- MAC address rules also capture DHCP traffic, if no other DHCP rule exists that would classify the DHCP traffic into another VLAN. Therefore, it is not necessary to combine DHCP rules with MAC address rules for the same VLAN.
- If there are a large number of devices that must join a VLAN, try MAC range rules (see **vlan mac range** command on page 20-24).
- Rules are only assigned to existing VLANs. Use the **vlan** command to create a new VLAN.

Examples

```
-> vlan 10 mac 00:00:39:59:0a:0c
-> vlan 20 mac 00:00:39:4f:f1:22
-> vlan 10 no mac 00:00:39:59:0a:0c
```

Release History

Release 5.1; command was introduced.

Related Commands

vlan mac range	Defines a MAC range rule for an existing VLAN. Mobile ports that receive frames with a source MAC address that falls within the range specified by this rule are temporarily assigned to the VLAN.
show vlan	Displays existing VLANs.
show vlan rules	Displays rules defined for VLANs.

MIB Objects

```
vMacRuleTable
   vMacRuleAddr
   vMacRuleVlanId
   vMacRuleStatus
```

vlan mac range

Defines a MAC range rule for an existing VLAN. If the source MAC address of a device matches the low or high end MAC or falls within the range defined by the low and high end MAC, the device and its mobile port will join the VLAN when the device starts to send traffic.

vlan *vid* **mac range** *low_mac_address high_mac_address*

vlan *vid* **no mac range** *low_mac_address*

Syntax Definitions

vid	VLAN ID number (1–4094).
low_mac_address	MAC address that defines the low end of the range (e.g., 00:00:39:59:f1:00).
high_mac_address	MAC address that defines the high end of the range (e.g., 00:00:39:59:f1:90).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of this command to delete a MAC range rule from the specified VLAN. It is only necessary to enter the low end MAC address to identify which rule to delete; the high end MAC is not required.
- Only valid source MAC addresses are allowed for the low and high end boundary MACs. For example, multicast addresses (e.g., 01:00:00:c5:09:1a) are ignored even if they fall within a specified MAC range. To allow the use of a multicast address as either the low or high end boundary MAC would cause misleading MAC range rule results.
- Once a device joins a MAC range rule VLAN, then it is not eligible to join multiple VLANs even if the device traffic matches other VLAN rules.
- MAC range rules follow the same precedence as MAC address rules.
- MAC range rules also capture DHCP traffic, if no other DHCP rule exists that would classify the DHCP traffic into another VLAN. Therefore, it is not necessary to combine DHCP rules with MAC range rules for the same VLAN.
- Rules are only assigned to existing VLANs. Use the **vlan** command to create a new VLAN.

Examples

```
-> vlan 10 mac range 00:00:39:59:0a:0c 00:00:39:59:0a:0f
-> vlan 10 no mac range 00:00:39:59:0a:0c
```

Release History

Release 5.1; command was introduced.

Related Commands

vlan mac	Defines a MAC address rule for an existing VLAN. Mobile ports that receive frames with a source MAC address that matches the address specified by this rule are temporarily assigned to the VLAN.
show vlan	Displays existing VLANs.
show vlan rules	Displays rules defined for VLANs.

MIB Objects

```
vMacRangeRuleTable
   vMacRangeRuleLoAddr
   vMacRangeRuleHiAddr
   vMacRangeRuleVlanId
   vMacRangeRuleStatus
```

vlan ip

Defines an IP network address rule for an existing VLAN. If a device sends traffic that matches the IP address specified in the rule, the device and its mobile port will join the rule's VLAN.

vlan *vid* **ip** *ip_address* **[***subnet_mask***]**

vlan *vid* **no ip** *ip_address* **[***subnet_mask***]**

Syntax Definitions

vid	VLAN ID number (1–4094).
ip_address	IP network address (e.g., 10.0.0.0, 171.15.0.0, 196.190.254.0)
subnet_mask	Class A, B, or C subnet mask (e.g., 255.0.0.0, 255.255.0.0, or 255.255.255.0).

Defaults

By default, the subnet mask is set to the default subnet mask value for the IP address class.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of this command to delete an IP network address rule from the specified VLAN.
- Network address rules take precedence behind DHCP, binding, and MAC address rules.
- Use DHCP rules in combination with IP network address rules to capture and forward DHCP traffic.
- Rules are only assigned to existing VLANs. Use the **vlan** command to create a new VLAN.

Examples

```
-> vlan 10 ip 51.0.0.0 255.0.0.0
-> vlan 20 ip 21.0.0.0
-> vlan 10 no ip 21.0.0.0 255.0.0.0
-> vlan 10 no ip 51.0.0.0
```

Release History

Release 5.1; command was introduced.

Related Commands

vlan dhcp mac	Defines a DHCP MAC address rule for an existing VLAN. Mobile ports that receive DHCP frames with a source MAC address that matches the address specified by this rule are temporarily assigned to the VLAN.
vlan dhcp mac range	Defines a DHCP MAC address range rule for an existing VLAN. Mobile ports that receive DHCP frames with a source MAC address that falls within the range specified by this rule are temporarily assigned to the VLAN.
vlan dhcp port	Defines a DHCP port rule for an existing VLAN. The mobile port specified by this rule is temporarily assigned to the VLAN when it receives DHCP frames.
vlan dhcp generic	Defines a generic DHCP rule for an existing VLAN. Mobile ports that receive DHCP frames that do not match other DHCP rules are temporarily assigned to the VLAN.
show vlan	Displays existing VLANs.
show vlan rules	Displays rules defined for VLANs.

MIB Objects

```
vIpNetRuleTable
   vIpNetRuleAddr
   vIpNetRuleMask
   vIpNetRuleVlanId
   vIpNetRuleStatus
```

vlan ipx

Defines an IPX network address rule for an existing VLAN. If a device sends traffic that matches the IPX network address and encapsulation specified in the rule, the device and its mobile port will join the rule's VLAN.

vlan *vid* **ipx** *ipx_net* **[e2 | llc | snap | novell]**

vlan *vid* **no ipx** *ipx_net*

Syntax Definitions

vid	VLAN ID number (1–4094).
ipx_net	IPX network address consisting of up to eight hex characters (e.g., A010590C, B030210A). If less than eight hex digits are entered, the entry is prefixed with zeros to equal eight digits.
e2	Enter **e2** or **ethernet2** to specify Ethernet-II encapsulation.
llc	LLC (802.2) encapsulation.
snap	SNAP encapsulation.
novell	Novell Raw (802.3) encapsulation.

Defaults

parameter	default
e2 | llc | snap | raw	**e2**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of this command to delete an IPX network address rule from the specified VLAN. It is only necessary to enter the IPX network address to identify which rule to delete; the encapsulation is not required.
- Specify **e2**, **llc**, **snap**, or **novell-raw** to identify the IPX encapsulation the device is going to use. If there is a mismatch and IPX traffic is routed, connectivity with the IPX server may not occur.
- This rule only applies to those devices that already have an IPX network address configured with an encapsulation that matches the encapsulation specified for the rule.
- Network address rules take precedence behind DHCP, binding, and MAC address rules.
- To remove an IPX network address rule, it is not necessary to specify the IPX encapsulation value.
- Rules are only assigned to existing VLANs. Use the **vlan** command to create a new VLAN.

Examples

```
-> vlan 10 ipx 250A llc
-> vlan 10 no ipx 250A
```

Release History

Release 5.1; command was introduced.

Related Commands

show vlan	Displays existing VLANs.
show vlan rules	Displays rules defined for VLANs.

MIB Objects

```
vIpxNetRuleTable
   vIpxNetRuleAddr
   vIpxNetRuleEncap
   vIpxNetRuleVlanId
   vIpxNetRuleStatus
```

vlan protocol

Defines a protocol rule for an existing VLAN. If a device sends traffic that matches the protocol value specified in the rule, the device and its mobile port will join the rule's VLAN.

vlan *vid* **protocol {ip-e2 | ip-snap | ipv6 | ipx-e2 | ipx-novell | ipx-llc | ipx-snap | decnet | appletalk | ethertype** *type* **| dsapssap** *dsap/ssap* **| snap** *snaptype***}**

vlan *vid* **no protocol {ip-e2 | ip-snap | ipx-e2 | ipx-nov | ipx-llc | ipx-snap | decnet | appletalk | ethertype** *type* **| dsapssap** *dsap/ssap* **| snap** *snaptype***}**

Syntax Definitions

vid	VLAN ID number (1–4094).
ip-e2	IP Ethernet-II protocol. Also captures Address Resolution Protocol (ARP).
ip-snap	IP Sub-network Access Protocol (SNAP) protocol.
ipv6	IPv6 protocol.
ipx-e2	IPX Ethernet-II protocol.
ipx-novell	IPX Novell (802.3) protocol.
ipx-llc	IPX LLC (802.2) protocol.
ipx-snap	IPX SNAP protocol.
decnet	DECNET Phase IV (6003) protocol.
appletalk	AppleTalk protocol. Also captures Datagram Delivery Protocol (DDP) and AppleTalk ARP (AARP).
type	A two-byte hex value between 0x600 and 0xffff that defines an Ethernet type (e.g., 0600, 0806, 6002).
dsap/ssap	A one-byte hex value between 0x00 and 0xff that defines Destination Service Access Protocol (DSAP) and Source Service Access Protocol (SSAP) header values. Specify both a DSAP and an SSAP value for this parameter variable (e.g., F0/F0, 04/04, BC/BC).
snaptype	A two-byte hex value between 0x600 and 0xffff that defines a SNAP protocol.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of this command to delete a protocol rule from the specified VLAN.
- Use the **ethertype, dsapssap,** or **snap** parameters if none of the generic protocol rule parameters (**ip-e2, ip-snap, ipx-e2, ipx-nov, ipx-llc, ipx-snap, decnet, appletalk**) provide the necessary rule definition for a specific traffic protocol.
- If an attempt is made to define an Ethertype rule with a protocol type value that is equal to the value already captured by one of the generic IP or IPX protocol rules, a message displays recommending the use of the IP or IPX generic rule.
- Protocol rules take precedence behind DHCP, binding, MAC address, and network address rules.
- IP protocol rules (ipE2 and ipSnap) also capture DHCP traffic, if no other DHCP rule exists that would classify the DHCP traffic into another VLAN. Therefore, it is not necessary to combine DHCP rules with protocol rules for the same VLAN.
- Rules are only assigned to existing VLANs. Use the **vlan** command to create a new VLAN.

Examples

```
-> vlan 10 protocol ip-e2
-> vlan 20 protocol ipx-nov
-> vlan 30 protocol ethertype 0600
-> vlan 40 protocol dsapssap F0/F0
-> vlan 50 protocol snap 6004
-> vlan 10 no protocol ip-snap
-> vlan 20 no protocol ipx-e2
-> vlan 30 no protocol ethertype 0806
-> vlan 40 no protocol dsapssap 04/04
-> vlan 50 no protocol snap 80FE
```

Release History

Release 5.1; command was introduced.

Related Commands

show vlan	Displays existing VLANs.
show vlan rules	Displays rules defined for VLANs.

MIB Objects

```
vProtocolRuleTable
   vProtoRuleProtoClass
   vProtoRuleEthertype
   vProtoRuleDsapSsap
   vProtoRuleVlanId
   vProtoRuleStatus
```

vlan user

Defines a custom (user) rule for an existing VLAN. If a device sends traffic that matches a custom rule value, the device and its mobile port will join the rule's VLAN.

vlan *vid* **user** *offset value mask*

vlan *vid* **no user** *offset value*

Syntax Definitions

vid	VLAN ID number (1–4094).
offset	Number between 0 and 72. Specifies the number of bytes into the frame to identify where to look for the pattern (*value*).
value	A four-byte hex value that specifies a pattern (e.g., 60020000).
mask	A four-byte hex value that identifies the bytes in the pattern to compare to the frame contents at the offset location. Use any hex character in the *mask* to mark bytes in the pattern to match and '0' to mark bytes in the pattern to ignore (e.g., EEFF0000 is the *mask* for the 60020000 *value* pattern).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of this command to delete a custom rule from the specified VLAN. It is only necessary to enter the offset and pattern values to identify which rule to delete; the mask value is not required.
- Use custom rules if none of the other standard VLAN rules provide the necessary rule definition for a specific type of traffic.
- Custom rules have the lowest precedence of all VLAN rules.
- To remove a custom rule, it is not necessary to specify the *mask* value.
- Rules are only assigned to existing VLANs. Use the **vlan** command to create a new VLAN.

Examples

```
-> vlan 200 user 14 E0000000 FF000000
-> vlan 310 user 14 F0F00000 FFFF0000
-> vlan 1500 user 12 60020000 FFFF0000
-> vlan 2000 user 6 12345678 FFFFFFFF
-> vlan 2210 no user 14 F0F00000
```

Release History

Release 5.1; command was introduced.

Related Commands

show vlan	Displays existing VLANs.
show vlan rules	Displays rules defined for VLANs.

MIB Objects

```
vCustomRuleTable
   vCustomRuleValue
   vCustomRuleOffset
   vCustomRuleMask
   vCustomRuleVlanId
   vCustomRuleStatus
```

vlan port

Defines a port rule for an existing VLAN. An active mobile port that is specified in a port rule, dynamically joins the VLAN even if traffic on that port does not get learned or matches any VLAN rules. The specified port becomes a VLAN member only for the purpose of forwarding broadcast traffic for a VLAN on that port. The advantage to this is that traffic from multiple VLANs can flood out on a single port.

vlan *vid* **port** *slot/port*

vlan *vid* **no port** *slot/port*

Syntax Definitions

vid	VLAN ID number (1–4094).
slot/port	The slot number for the module and the physical mobile port number on that module (e.g., 3/1 specifies port 1 on slot 3). To enter multiple slots and ports in a single command, use a hyphen to specify a range of ports (e.g., 3/1-16) and a space to specify multiple slots (e.g., 3/1-16 5/10-20 8/2-9).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of this command to delete a port rule from the specified VLAN.
- Port rules are for silent devices, such as printers, that require VLAN membership to receive traffic forwarded from the VLAN. These devices usually don't send traffic, so they do not trigger dynamic assignment of their mobile ports to a VLAN.
- Port rules do not classify incoming traffic on the specified mobile port. Incoming traffic is classified for VLAN assignment in the same manner as all other mobile port traffic.
- VLAN assignments that are defined using port rules are exempt from the port's default VLAN restore status.
- An alternative to port rules is to manually assign a port to a VLAN by using the **vlan port default** command. This applies to both mobile and non-mobile ports.
- Rules are only assigned to existing VLANs. Use the **vlan** command to create a new VLAN.

Examples

```
-> vlan 10 port 3/10
-> vlan 20 port 6/1-32
-> vlan 500 port 2/1-12 4/10-16 8/4-17
-> vlan 30 no port 9/11
-> vlan 40 no port 4/1-16
-> vlan 600 no port 2/14-20 7/1-9
```

Release History

Release 5.1; command was introduced.

Related Commands

show vlan	Displays existing VLANs.
show vlan rules	Displays rules defined for VLANs.

MIB Objects

```
vPortRuleTable
   vPortRuleIfIndes
   vPortRuleVlanId
   vPortRuleStatus
```

vlan port mobile

Configures Ethernet ports as mobile ports and enables or disables BPDU ignore. Mobile ports are eligible for dynamic VLAN assignment, which occurs when mobile port traffic matches a VLAN rule on one or more VLANs. Typically, mobility is applied to ports that do not send or receive BPDUs. However, enabling BPDU ignore allows BPDU ports to also participate in dynamic VLAN assignment.

Note. Enabling BPDU ignore is not recommended. In specific cases where it is required, such as connecting legacy networks to port mobility networks, make sure that ignoring BPDUs on a mobile port will not cause network loops to go undetected. Connectivity problems could also result if a mobile BPDU port dynamically moves out of its configured default VLAN where it provides traffic flow to and from another switch.

vlan port mobile *slot/port* **[bpdu ignore {enable | disable}]**

vlan no port mobile *slot/port*

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3). To enter multiple slots and ports in a single command, use a hyphen to specify a range of ports (e.g., 3/1-16) and a space to specify multiple slots (e.g., 3/1-16 5/10-20 8/2-9).
enable	Enables BPDU ignore on a mobile port.
disable	Disables BPDU ignore on a mobile port.

Defaults

By default, all ports are non-mobile (fixed) ports.

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of this command to disable mobility on the specified port.
- Only 10/100 and gigabit Ethernet ports are eligible for mobile port status.
- Mobile ports can join more than one VLAN. For example, if a device connected to a mobile port sends both IP and IPX traffic and VLAN 10 has an IP protocol rule and VLAN 20 has an IPX protocol rule, the mobile port and its device dynamically join both VLANs. However, certain rules, such as MAC address rules, can limit port membership to one VLAN.

- When a VLAN is administratively disabled, manual port and dynamic mobile port assignments are retained but traffic on these ports is not forwarded. However, VLAN rules remain active and continue to classify mobile port traffic for VLAN membership.
- When a BPDU is received on a mobile port and BPDU ignore is disabled, the port is changed to a fixed (non-mobile) port that is associated only with its configured default VLAN. Also, the BPDU port participates in the Spanning Tree algorithm. When BPDU ignore is enabled, a mobile port that receives a BPDU remains mobile and is not included in Spanning Tree topology calculations.
- Enabling mobility on an active port that sends or receives BPDU (e.g. ports that connect two switches and Spanning Tree is enabled on both the ports and their assigned VLANs) is not allowed. If mobility is required on this type of port, enable mobility and the BPDU ignore flag when the port is not active.

Examples

```
-> vlan port mobile 3/1
-> vlan port mobile 3/1-16
-> vlan port mobile 3/1-16 4/17-32 8/4-12
-> vlan port mobile 5/22 authenticate enable
-> vlan port mobile 6/12-16 authenticate disable
-> vlan no port mobile 2/1
-> vlan no port mobile 3/1-16
-> vlan no port mobile 4/17-32 8/4-12
```

Release History

Release 5.1; command was introduced.

Related Commands

vlan port default vlan restore	Enables default VLAN restore on a mobile port.
vlan port default vlan	Enables default VLAN membership for mobile port traffic that does not match any VLAN rules.
vlan port authenticate	Enables or disables authentication on a mobile port.
show vlan port mobile	Displays mobile port properties.

MIB Objects

```
vMobilePortTable
   vMobilePortIIfIndex
   vMobilePortMobility
   vMobilePortIgnoreBPDU
```

vlan port default vlan restore

Enables or disables default VLAN restore for a mobile port. Use this command to specify if a mobile port should retain or drop its dynamic VLAN assignments after all MAC addresses learned on that port have aged out.

vlan port *slot/port* **default vlan restore {enable | disable}**

Syntax Definitions

slot/port	The slot number for the module and the physical mobile port number on that module (e.g., 3/1 specifies port 1 on slot 3). To enter multiple slots and ports in a single command, use a hyphen to specify a range of ports (e.g., 3/1-16) and a space to specify multiple slots (e.g., 3/1-16 5/10-20 8/2-9).
enable	Enable default VLAN restore for the specified mobile port. VLAN assignments are dropped when port traffic ages out.
disable	Disable default VLAN restore for the specified mobile port. VLAN assignments are retained when port traffic ages out.

Defaults

By default, VLAN restore is enabled on mobile ports.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If a hub is connected to a mobile port, enabling default VLAN restore on that port is recommended.
- If a VLAN port rule exists for a mobile port, it will remain a member of the port rule VLAN even if default VLAN restore is enabled for that port.
- When a mobile port link is disabled and then enabled, the port is always returned to its configured default VLAN. Switch ports are disabled when a device is disconnected from the port, a configuration change is made to disable the port, or switch power is turned off.

Examples

```
-> vlan port 3/1 default vlan restore enable
-> vlan port 5/2 default vlan restore disable
-> vlan port 6/1-32 8/10-24 9/3-14 default vlan restore enable
```

Release History

Release 5.1; command was introduced.

Related Commands

vlan port mobile	Configures Ethernet ports as mobile ports.
vlan port default vlan	Enables default VLAN membership for mobile port traffic that does not match any VLAN rules.
vlan port authenticate	Enables or disables authentication on a mobile port.
show vlan port mobile	Displays mobile port properties.

MIB Objects

```
vMobilePortTable
   vMobilePortIIfIndex
   vMobilePortDefVlanRestore
```

vlan port default vlan

Enables or disables the forwarding of mobile port traffic on the configured default VLAN for the mobile port when the traffic does not match any VLAN rules.

vlan port *slot/port* **default vlan {enable | disable}**

Syntax Definitions

slot/port	The slot number for the module and the physical mobile port number on that module (e.g., 3/1 specifies port 1 on slot 3). To enter multiple slots and ports in a single command, use a hyphen to specify a range of ports (e.g., 3/1-16) and a space to specify multiple slots (e.g., 3/1-16 5/10-20 8/2-9).
enable	Enable the configured default VLAN for the specified mobile port.
disable	Disable the configured default VLAN for the specified mobile port.

Defaults

Default VLAN is enabled on mobile ports.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- It is recommended that mobile ports with their default VLAN disabled should not share a VLAN with any other types of ports (e.g., mobile ports with default VLAN enabled or non-mobile, fixed ports).
- If the default VLAN is enabled for a mobile port, traffic that does not match any VLAN rules is forwarded on the default VLAN.
- If the default VLAN is disabled for the mobile port, traffic that does not match any VLAN rules is dropped.
- When a port (mobile or fixed) is manually assigned to a default VLAN or is still a member of default VLAN 1, then that association is referred to as the *configured* default VLAN for the port. If a mobile port is dynamically assigned to additional VLANs, these subsequent associations are referred to as secondary VLANs.

Examples

```
-> vlan port 3/1 default vlan enable
-> vlan port 5/2 default vlan disable
-> vlan port 6/1-32 8/10-24 9/3-14 default vlan enable
```

Release History

Release 5.1; command was introduced.

Related Commands

vlan port mobile	Configures Ethernet ports as mobile ports.
vlan port default vlan restore	Enables default VLAN restore on a mobile port.
vlan port authenticate	Enables or disables authentication on a mobile port.
show vlan port mobile	Displays mobile port properties.

MIB Objects

```
vMobilePortTable
   vMobilePortIIfIndex
   vMobilePortDefVlanEnable
```

vlan port authenticate

Enables or disables authentication on a mobile port.

vlan port *slot/port* **authenticate {enable | disable}**

Syntax Definitions

slot/port	The slot number for the module and the physical mobile port number on that module (e.g., 3/1 specifies port 1 on slot 3). To enter multiple slots and ports in a single command, use a hyphen to specify a range of ports (e.g., 3/1-16) and a space to specify multiple slots (e.g., 3/1-16 5/10-20 8/2-9).
enable	Enable authentication on the specified mobile port.
disable	Disable authentication on the specified mobile port.

Defaults

By default, authentication is disabled on mobile ports.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

At this time, authentication is only supported on mobile ports.

Examples

```
-> vlan port 3/1 authenticate enable
-> vlan port 5/2 authenticate disable
-> vlan port 6/1-32 8/10-24 9/3-14 authenticate enable
```

Release History

Release 5.1; command was introduced.

Related Commands

vlan port mobile	Configures Ethernet ports as mobile ports.
vlan port 802.1x	Enables or disables 802.1X port-based access control on a mobile port.
show vlan port mobile	Displays mobile port properties.

MIB Objects

```
vMobilePortTable
   vMobilePortIIfIndex
   vMobilePortAuthenticate
```

vlan port 802.1x

Enables or disables 802.1X port-based access control on a mobile port.

vlan port *slot/port* **802.1x {enable | disable}**

Syntax Definitions

slot/port	The slot number for the module and the physical mobile port number on that module (e.g., 3/1 specifies port 1 on slot 3). To enter multiple slots and ports in a single command, use a hyphen to specify a range of ports (e.g., 3/1-16) and a space to specify multiple slots (e.g., 3/1-16 5/10-20 8/2-9).
enable	Enable 802.1x on the specified mobile port.
disable	Disable 802.1x on the specified mobile port.

Defaults

By default, 802.1x is disabled on mobile ports.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- At this time, 802.1X is only supported on mobile ports.
- Authentication and 802.1X are mutually exclusive on a given mobile port.

Examples

```
-> vlan port 3/1 802.1x enable
-> vlan port 5/2 802.1x disable
-> vlan port 6/1-32 8/10-24 9/3-14 802.1x enable
```

Release History

Release 5.1; command was introduced.

Related Commands

vlan port mobile	Configures Ethernet ports as mobile ports.
vlan port authenticate	Enables or disables authentication on a mobile port.
show vlan port mobile	Displays mobile port properties.

MIB Objects

```
vMobilePortTable
   vMobilePortIIfIndex
   vMobilePortAuthenticate
```

show vlan rules

Displays VLAN rules for the specified VLAN.

show vlan [*vid*] rules

Syntax Definitions

vid	VLAN ID number (1–4094).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

If a *vid* is not specified, rules defined for all VLANs are displayed.

Examples

```
-> show vlan rules
Legend:  * indicates a binding rule

  type                 vlan    rule
+--------------------+------+-----------------------------------------------------+
  ip-net                  7    143.113.0.0, 255.255.0.0
  ipx-net                 8    0x450c, llc
  mac-addr             4000    00:00:00:00:10:10
  mac-range            4001    00:00:00:10:00:00, 00:00:00:20:00:00
  mac-port-proto*      4094    00:00:0e:00:12:34, 15/4, appletalk

-> show vlan 55 rules
Legend:  * indicates a binding rule

  type                 vlan    rule
+--------------------+------+-----------------------------------------------------+
  ip-net                 55    143.113.0.0, 255.255.0.0
  ipx-net                55    45, llc
  mac-addr               55    00:00:00:00:10:10
  mac-range              55    00:00:00:10:00:00, 00:00:00:20:00:00
  mac-port-proto*        55    00:00:0e:00:12:34, 15/4, appletalk
```

output definitions

Type	The type of rule defined. There are several types of VLAN rules: binding rules, MAC address rules, IP/IPX network address rules, protocol rules, port rules, custom rules, and DHCP rules.
*****	Identifies a binding rule. The asterisk appears next to the rule type.

output definitions (continued)

VLAN	The VLAN ID number for the rule's VLAN.
Rule	The value for the type of rule defined. Switch software uses these rule values to determine mobile port VLAN assignment. If traffic coming in on a mobile port matches the value of a VLAN rule, then the mobile port is dynamically assigned to that VLAN.

Release History

Release 5.1; command was introduced.

Related Commands

show vlan	Displays a list of existing VLANs.
show vlan port	Displays VLAN port assignments for all VLANs, a specific VLAN, or for a specific port (mobile and fixed).

show vlan port mobile

Displays current status of mobile properties for a switch port.

show vlan port mobile [*slot/port***]**

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3). To enter multiple slots and ports in a single command, use a hyphen to specify a range of ports (e.g., 3/1-16) and a space to specify multiple slots (e.g., 3/1-16 5/10-20 8/2-9).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If a *slot/port* is not specified, then mobile properties for all ports are displayed.
- Note that the **show vlan port mobile** command only displays ports that are mobile or are eligible to become mobile ports. For example, ports that are part of a link aggregate or are configured for 802.1Q VLAN tagging are not included in the output of this command.

Examples

```
-> show vlan port mobile
              cfg                              ignore
 port  mobile def  authent  enabled  restore  bpdu
+-----+------+----+--------+--------+--------+-----+
 12/12   on    1     off       on      off    off
 12/13  off
 12/14  off
 12/15   on   10   on-avlan   off       on    off
 12/16   on   10   on-8021x    on      off     on
```

output definitions

port	The slot number for the module and the physical mobile port number on that module.
mobile	The mobile status for the port (**on** or **off**). If set to **on**, the port is mobile and eligible for dynamic VLAN assignment. If set to **off**, the port is non-mobile and remains only a member of its configured default VLAN. Use the **vlan port mobile** to enable or disable mobility on a port.
cfg def	The configured default VLAN for the port, which is assigned using the **vlan port default** command.

output definitions (continued)

authent	The authentication status for the port (**on-avlan**, **on-8021x**, or **off**). Use the **vlan port authenticate** and **vlan port 802.1x** commands to change this status.
enabled	The default VLAN status for the port: **on** enables the forwarding of traffic that doesn't match any rules on the port's configured default VLAN; **off** disables the forwarding of such traffic and packets are discarded. Use the **vlan port default vlan** to change this status.
restore	The default VLAN restore status for the port: **on** indicates that the mobile port will not retain its VLAN assignments when qualifying traffic ages out on that port; **off** indicates that the mobile port will retain its dynamic VLAN assignments after qualifying traffic has aged out. Use the **vlan port default vlan restore** command to change this status.
ignore BPDU	The ignore BPDU status for the port: **on** indicates that if the mobile port receives BPDUs, they're ignored and the port remains eligible for dynamic VLAN assignment; **off** indicates that if a BPDU is seen on the port, mobility is disabled and the port is not eligible for dynamic assignment. The status of ignore BPDU is set when the **vlan port mobile** command is used to enable or disable mobility on a port.

Release History

Release 5.1; command was introduced.

Related Commands

show vlan port	Displays VLAN port assignments for all VLANs, a specific VLAN, or for a specific port.

21 VLAN Management Commands

VLAN management software handles VLAN configuration and the reporting of VLAN configuration changes to other switch tasks. A VLAN defines a broadcast domain that contains physical ports and can span across multiple switches. All switches contain a default VLAN 1. Physical switch ports are initially assigned to VLAN 1 until they are statically or dynamically assigned to other VLANs.

This chapter includes descriptions of VLAN management commands used to create, modify or remove VLANs. These commands allow you to enable or disable Spanning Tree Protocol (STP) and Authentication on a VLAN, add or remove virtual router ports, statically assign physical switch ports to a default VLAN, and display VLAN configuration information.

The VLAN management commands comply with RFC 2674.

MIB information is as follows:

Filename: AlcatelIND1VlanManager.mib
Module: ALCATEL-IND1-VLAN-MGR-MIB

A summary of the available commands is listed here:

vlan
vlan stp
vlan mobile-tag
vlan authentication
vlan router ipx
vlan router mac multiple
vlan port default
show vlan
show vlan port
show vlan router mac status

vlan

Creates a new VLAN with the specified VLAN ID (VID) and an optional description.

vlan *vid* **[enable | disable] [name** *description***]**

no vlan *vid*

Syntax Definitions

vid	A numeric value (2–4094) that uniquely identifies an individual VLAN. This value becomes the VLAN ID for the new VLAN.
description	Text string up to 32 characters. Use quotes around string if description contains multiple words with spaces between them (e.g. “Alcatel Marketing VLAN”).
enable	Enable VLAN administrative status.
disable	Disable VLAN administrative status.

Defaults

parameter	default
enable | disable	**enable**
description	VLAN ID

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of this command to delete a VLAN from the configuration. All VLAN ports and routers are detached before the VLAN is removed. Ports return to their default VLANs or VLAN 1, if the VLAN deleted is the port’s configured default VLAN.
- A VLAN is not operationally active until at least one active port is assigned to the VLAN.
- When a VLAN is administratively disabled, static port and dynamic mobile port assignments are retained but traffic on these ports is not forwarded. However, VLAN rules remain active and continue to classify mobile port traffic for VLAN membership.
- Ports are manually configured or dynamically assigned to VLANs.

Examples

```
-> vlan 850 “Marketing Admin”
-> vlan 720 disable
-> no vlan 1020
```

Release History

Release 5.1; command was introduced.

Related Commands

vlan port default	Statically assigns ports to a VLAN.
show vlan	Displays a list of existing VLANs.
show vlan port	Displays VLAN port assignments.

MIB Objects

```
vlanTable
   vlanNumber
   vlanDescription
   vlanAdmStatus
   vlanOperStatus
   vlanStatus
```

vlan stp

Enables or disables the Spanning Tree status for a VLAN.

vlan *vid* **[1x1 | flat] stp {enable | disable}**

Syntax Definitions

vid	A VLAN ID number (1–4094).
1x1	Specifies that the Spanning Tree status for the VLAN applies when the switch is running in the 1x1 Spanning Tree mode.
flat	Specifies that the Spanning Tree status for the VLAN applies when the switch is running in the flat Spanning Tree mode.
enable	Enables Spanning Tree for the specified VLAN.
disable	Disables Spanning Tree for the specified VLAN.

Defaults

By default, STP is enabled when a VLAN is created.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- STP is not active until at least one active port is assigned to the VLAN.
- Use the optional **1x1** or **flat** parameter with this command to configure the Spanning Tree status only for the Spanning Tree mode specified by the parameter. For example, if the **flat** parameter is specified when disabling STP for VLAN 10, then the Spanning Tree status for VLAN 10 is disabled when the switch is running in the flat mode. However, the current Spanning Tree status for VLAN 10 in the 1x1 mode remains unchanged.
- If this command is used without specifying the **1x1** or **flat** parameter, then the Spanning Tree status for the specified VLAN is changed for both operating modes.
- Up to 253 Spanning Tree instances per switch are supported in the 1x1 Spanning Tree mode. Since each VLAN with Spanning Tree enabled uses one of these instances, only 253 VLANs can have an active Spanning Tree instance at any given time.
- When STP is disabled on a VLAN, it remains disabled even if the switch STP operating mode is set to **1x1** (one STP instance per VLAN). In addition, all active ports for the disabled VLAN remain in a forwarding state in both the 1x1 and flat Spanning Tree modes.
- If a switch is running in the flat Spanning Tree mode, disabling Spanning Tree on VLAN 1 disables the instance across all VLANs. Disabling STP on any other VLAN disables the instance only for that VLAN.

Examples

```
-> vlan 850 stp enable
-> vlan 720 stp disable
-> vlan 500 1x1 stp enable
-> vlan 500 flat stp disable
-> vlan 1020 stp disable
```

Release History

Release 5.1; command was introduced.
Release 5.3.1 and 5.1.6; **1x1** and **flat** parameters added.

Related Commands

vlan	Creates a VLAN.
bridge mode	Selects a flat Spanning Tree or 1x1 Spanning Tree operating mode for a switch.
show vlan	Displays a list of existing VLANs.
show vlan port	Displays VLAN port assignments.

MIB Objects

```
vlanTable
   vlanNumber
   vlanStpStatus
   vlan1x1StpStatus
   vlanflatStpStatus
```

vlan mobile-tag

Enables or disables classification of tagged packets received on mobile ports. If a mobile port receives a tagged packet with a VLAN ID that matches the specified VLAN ID, the port and packet are dynamically assigned to that VLAN. If vlan mobile-tag is disabled, the packets tagged with a VLAN ID that does not match the mobile port's default VLAN or a rule VLAN that the traffic qualifies for, the packet is dropped.

vlan *vid* **mobile-tag {enable | disable}**

Syntax Definitions

vid	An existing VLAN ID number (1–4094).
enable	Enables dynamic assignment of tagged mobile port packets to the specified VLAN.
disable	Disables dynamic assignment of tagged mobile port packets to the specified VLAN.

Defaults

By default, mobile port tagging is disabled when a VLAN is created.

Platforms Supported

OmniSwitch 6600

Usage Guidelines

- This command is VLAN based but only applies to tagged packets received on mobile ports.
- Packets received on mobile ports tagged with the VLAN ID are discarded.

Examples

```
-> vlan 850 mobile-tag enable
-> vlan 720 mobile-tag enable
-> vlan 1020 mobile-tag disable
```

Release History

Release 5.1; command was introduced.

Related Commands

vlan	Creates a VLAN.
show vlan	Displays a list of existing VLANs.
show vlan port	Displays VLAN port assignments.

MIB Objects

```
vlanTable
   vlanNumber
   vlanTagMobilePortStatus
```

vlan authentication

Enables or disables authentication for a VLAN.

vlan *vid* **authentication {enable | disable}**

Syntax Definitions

vid	An existing VLAN ID number (1–4094).
enable	Enables authentication for the specified VLAN.
disable	Disables authentication for the specified VLAN.

Defaults

By default, authentication is disabled when a VLAN is created.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

A maximum of 128 authenticated VLANs per switch is supported. See Chapter 43, "AAA Commands," for more information about configuring Layer 2 Authentication.

Examples

```
-> vlan 850 authentication enable
-> vlan 720 authentication enable
-> vlan 1020 authentication disable
```

Release History

Release 5.1; command was introduced.

Related Commands

vlan	Creates a VLAN.
show vlan	Displays list of existing VLANs.
show vlan port	Displays VLAN port assignments.

MIB Objects

```
vlanTable
   vlanNumber
   vlanAuthentStatus
```

vlan router ipx

Defines a virtual router port to enable IPX routing on a VLAN. Defining an IPX virtual router port allows VLAN traffic to communicate with traffic from other IPX router port VLANs. Without a virtual router port, traffic is bridged within the VLAN or across connections to the same VLAN on other switches.

vlan *vid* **router ipx** *ipx_net* **[rip | active | inactive | triggered] [e2 | llc | snap | novell] [timeticks** *ticks***]**

vlan *vid* **no router ipx**

Syntax Definitions

vid	An existing VLAN ID number (1–4094).
ipx_net	IPX network address consisting of eight hex characters (e.g. 0000590c, 0000210a). If less than eight hex digits are entered, the entry is prefixed with zeros to equal eight digits.
rip	RIP updates are processed.
active	RIP and SAP updates are processed.
inactive	RIP and SAP updates are not processed, but router port remains active.
triggered	RIP and SAP information is broadcast only when there are updates.
e2	Enter **e2** or **ethernet2** to specify Ethernet-II encapsulation.
novell	Novell Raw (802.3) encapsulation.
llc	LLC (802.2) encapsulation.
snap	SNAP encapsulation.
ticks	A 16-bit value (0–65535) that specifies the number of ticks for IPX delay time. A tick is approximately 1/18th of a second.

Defaults

parameter	default
rip | active | inactive | triggered	**active**
e2 | llc | snap | raw	**e2**
ticks	0

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of this command to remove an IPX virtual router port from the VLAN.
- Configuring both an IP and IPX virtual router port on the same VLAN is allowed. VLAN router ports, however, are not active until at least one active port is assigned to the VLAN.
- If the switch is running in multiple MAC router mode, then a maximum of 64 VLANs can have IP, IPX, or a combination of both router ports defined. If the switch is running in single MAC router mode, then a maximum of 4094 VLANs can have IP and 256 VLANs can have IPX router ports defined.

Examples

```
-> vlan 10 router ipx 1000590c
-> vlan 200 router ipx 250a active raw timeticks 10
-> vlan 420 router ipx 350a triggered snap timeticks 5
-> vlan 1020 router ipx 2110650d inactive
-> vlan 1020 no router ipx
```

Release History

Release 5.1; command was introduced.

Related Commands

vlan	Creates a VLAN.
show vlan	Displays list of existing VLANs.
show vlan port	Displays VLAN port assignments.
show vlan router mac status	Displays router MAC operating mode and VLAN router port statistics.

MIB Objects

```
vlanTable
   vlanNumber
   vlanIpxNet
   vlanIpxEncap
   vlanIpxRipSapMode
   vlanIpxDelayTicks
   vlanIpxStatus
```

vlan router mac multiple

Enables or disables multiple MAC router mode on a switch. Enabling this mode specifies that a unique MAC address is assigned to every router port VLAN. If a VLAN has both an IP and IPX router port defined, then both router ports share the MAC address assigned to that VLAN.

Note. Using this command to enable or disable multiple MAC router mode is supported only when the switch is rebooted. To configure a mode change to occur at boot time, add **vlan router mac multiple enable** or **vlan router mac multiple disable** command to the **boot.cfg** file.

vlan router mac multiple {enable | disable}

Syntax Definitions

enable	Enables multiple MAC router mode. A unique MAC address is assigned to each router port.
disable	Disables multiple MAC router mode. Switch is returned to single mac router mode, where one MAC address is used for all router ports.

Defaults

By default, the switch operates in multiple MAC router mode.

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- If this mode is disabled, then the switch is running in single MAC router mode, which uses the chassis base MAC address for every IP or IPX router port defined (note that IPX routing is not supported on the OmniSwitch 6600).
- The total number of supported router ports per switch depends on the switch MAC router mode. If the switch is running in multiple MAC router mode, then a maximum of 64 VLANs can have IP, IPX, or a combination of both router ports defined. If the switch is running in single MAC router mode, then a maximum of 4094 VLANs can have IP and 256 VLANs can have IPX router ports defined.
- Each switch is equipped with 32 MAC addresses. If operating in the multiple MAC router mode and configuring more than 32 router port VLANs, then additional MAC addresses are required. Contact your Alcatel representative for information about how to increase the number of MAC addresses allocated for the switch.
- Enabling multiple MAC router mode on a switch that has more than 64 router port VLANs defined is not allowed. If an attempt is made to do so, an error message is displayed and the switch remains operating in the single MAC router mode.

Examples

```
-> vlan router mac multiple enable
-> vlan router mac multiple disable
```

Release History

Release 5.1; command was introduced.

Related Commands

ip interface	Defines a virtual router port to enable IP routing on a VLAN.
vlan router ipx	Defines a virtual router port to enable IPX routing on a VLAN.
show vlan router mac status	Displays router MAC operating mode and VLAN router port statistics.

MIB Objects

```
vlanMgrVlanSet
   vlanSetMultiRtrMacStatus
```

vlan port default

Configures a new default VLAN for a single port or an aggregate of ports. The VLAN specified with this command is referred to as the *configured default VLAN* for the port.

vlan *vid* **port default {***slot/port* | *link_agg***}**

vlan *vid* **no port default {***slot/port* | *link_agg***}**

Syntax Definitions

vid	An existing VLAN ID number (1–4094) of the VLAN to assign as the port's configured default VLAN.
slot/port	The slot number for the module and the physical port number on that module (e.g. 3/1 specifies port 1 on slot 3). To enter multiple slots and ports in a single command, use a hyphen to specify a range of ports (e.g. 3/1-16) and a space to specify multiple slots (e.g. 3/1-16 5/10-20 8/2-9).
link_agg	The link aggregate ID number (0–31) to assign to the specified VLAN. See Chapter 13, "Link Aggregation Commands."

Defaults

VLAN 1 is the default VLAN for all ports.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of this command to remove a port or link aggregate from its configured default VLAN and restore VLAN 1 as the default VLAN.
- The *link_agg* value range for link aggregate ID numbers is 0–29 on the OmniSwitch 6600 and 0–15 on the OmniSwitch 8800.
- Every switch port or link aggregate has only one configured default VLAN. Mobile and 802.1Q tagged ports, however, may have additional VLAN assignments, which are often referred to as *secondary* VLANs.
- Mobile ports that are assigned to a default VLAN other than VLAN 1 are still eligible for dynamic assignment to other VLANs.

Examples

```
-> vlan 10 port default 3/1
-> vlan 20 port default 4/1-24
-> vlan 30 port default 5/1-8 6/12-24
-> vlan 200 port default 29
-> vlan 10 no port default 3/1
-> vlan 20 no port default 4/1-24
-> vlan 30 no port default 5/1-8 6/12-24
-> vlan 200 no port default 29
```

Release History

Release 5.1; command was introduced.

Related Commands

vlan	Creates a VLAN.
show vlan	Displays list of existing VLANs.
show vlan port	Displays VLAN port assignments.

MIB Objects

```
vpaTable
   vpaVlanNumber
   vpaIfIndex
   vpaType
   vpaState
   vpaStatus
```

show vlan

Displays a list of VLANs configured on the switch.

show vlan [*vid***]**

Syntax Definitions

vid	VLAN ID number (1–4094).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

If a *vid* is not specified, all VLANs are displayed.

Examples

```
-> show vlan
                          stree                          mble
 vlan     admin   oper   1x1  flat   auth   ip   ipx   tag   name
+------+--------+-------+----------+------+----+-----+-----+---------+
    1       on      off   on    on   off   off    off  off   VLAN 1
    2       on      off   on   off   off   off    off  off   VLAN 2
    3       on      off   off  off   off   off    off  off   VLAN 3
    4       on      off   off   on   off   off    off  off   VLAN 4
    5       on      off   on    on   off   off    off  off   VLAN 5

-> show vlan 2
    Name                : VLAN 200,
    Administrative State: enabled
    Operational State   : enabled
    1x1 Spanning Tree State  : enabled,
    Flat Spanning Tree State : enabled,
    Authentication      : disabled
    IP Router Port      : 143.113.1.1  255.255.0.0  ethernet-II
    IPX Router Port     : 455ff  novell  active  ticks:100
    Mobile Tag          : off
```

output definitions

vlan	The numerical VLAN ID. Use the **vlan** command to create or remove VLANs.
admin	VLAN administrative status: **on** enables VLAN functions to operate; **off** disables VLAN functions without deleting the VLAN. Use the **vlan** command to change the VLAN administrative status.

output definitions (continued)

oper	VLAN operational status: **on** (enabled) or **off** (disabled). The operational status remains disabled until an active port is assigned to the VLAN. When the operational status is enabled, then VLAN properties (e.g. virtual router ports, Spanning Tree) are applied to ports and traffic flow. A VLAN must have an enabled administrative status before it can become operationally enabled.
stree 1x1	VLAN Spanning Tree status for the VLAN in the 1x1 mode: **on** (enabled) allows the Spanning Tree algorithm to determine the state of VLAN ports (forwarding or blocking); **off** (disabled) prevents Spanning Tree algorithm from controlling VLAN ports, leaving active ports in a forwarding state. Configured through the **vlan stp** command.
stree flat	VLAN Spanning Tree status for the VLAN in the flat mode: **on** (enabled) allows the Spanning Tree algorithm to determine the state of VLAN ports (forwarding or blocking); **off** (disabled) prevents Spanning Tree algorithm from controlling VLAN ports, leaving active ports in a forwarding state. Configured through the **vlan stp** command.
auth	VLAN Authentication status: **on** (enabled) or **off** (disabled). Use the **vlan authentication** command to change the VLAN Authentication status.
ip	IP virtual router port information. Displays the IP address, subnet mask, and encapsulation for the VLAN's IP router port, if one is defined. Use the **ip interface** command to define an IP router for a VLAN.
ipx	IPX virtual router port. Shows the IPX address, RIP mode, and encapsulation for the VLAN's IPX router port, if one is defined. Use the **vlan router ipx** command to configure IPX router ports.
mble tag	Mobile tagging status: **on** (enabled); **off** (disabled). Configured through the **vlan mobile-tag** command. Note that this field only displays on an OmniSwitch 6600.
name	The user-defined text description for the VLAN. By default, the VLAN ID is specified for the VLAN description.

Release History

Release 5.1; command was introduced.
Release 5.3.1 and 5.1.6; **stree** field divided into two new fields: **1x1** and **flat**.

Related Commands

show vlan port	Displays VLAN port assignments.
show vlan router mac status	Displays the current MAC router operating mode (single or multiple) and VLAN router port statistics.
show ip interface	Displays VLAN IP router port information.

MIB Objects

```
vlanMgrVlan
vlanTable
   vlanNumber
   vlanDescription
   vlanAdmStatus
   vlanOperStatus
   vlanStatus
   vlanStpStatus
   vlanAuthentStatus
   vlanIpAddress
   vlanIpMask
   vlanIpEnacp
   vlanIpForward
   vlanIpStatus
   vlanIpxNet
   vlanIpxEncap
   vlanIpxRipSapMode
   vlanIpxDelayTicks
   vlanIpxStatus
   vlanTagMobilePortStatus
```

show vlan port

Displays VLAN port associations (VPAs) for all VLANs, a specific VLAN, or for a specific port. Information is also included that shows the VPA type (configured default VLAN, 802.1Q tagged VLAN, dynamically assigned secondary VLAN, or mirrored port VLAN assignment) and the status of that association (inactive, blocking, forwarding, or filtering).

show vlan [*vid***] port {***slot/port* | *link_agg***}**

Syntax Definitions

vid	VLAN ID number (1–4094).
slot/port	Enter the slot number for the module and the physical port number on that module (e.g. 3/1 specifies port 1 on slot 3).
ling_agg	Enter the link aggregate ID number (0–31) to assign to the specified VLAN.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If the *vid* and *slot/port* or *link_agg* are not specified, then a list of all VLANs and their assigned ports is displayed.
- If the *vid* is specified without a *slot/port* or *link_agg*, then all port assignments for that VLAN are displayed.
- If the *slot/port* or *link_agg* is specified without a *vid*, then all VLAN assignments for that port are displayed.
- If both the *vid* and *slot/port* or *link_agg* are specified, then information only for that VLAN and slot/port or link aggregate ID is displayed.
- The *link_agg* value range for link aggregate ID numbers is 0–29 on the OmniSwitch 6600 and 0–15 on the OmniSwitch 8800.

Examples

```
-> show vlan port
 vlan   port     type      status
+-----+-------+---------+------------+
  1      1/1    default   inactive
  2      1/2    default   blocking
         1/3    mobile    forwarding
        11/4    qtagged   forwarding
  3      1/2    qtagged   blocking
        11/4    default  forwarding
```

```
-> show vlan 10 port
  port   type      status
+------+--------+------------+
  1/1   default   forwarding
  1/2   qtagged   forwarding
  1/3   mobile    forwarding
-> show vlan port 3/2
 vlan     type      status
+------+---------+------------+
   1     default   forwarding
   2     qtagged   forwarding
   3     qtagged   blocking

-> show vlan 500 port 8/16
type       :default
status     :blocking
vlan admin :on
vlan oper  :off
port admin :on
port oper  :off
```

output definitions

vlan	Numerical VLAN ID. Identifies the port's VLAN assignment.
port	The slot number for the module and the physical port number on that module (e.g. 3/1 specifies port 1 on slot 3).
type	The type of VPA: **default** (configured default VLAN assignment for the port), **qtagged** (802.1Q tagged secondary VLAN assignment for the port), **mobile** (dynamic secondary VLAN assignment for the port), or **mirror** (port is mirroring the VLAN assignment of another port).
status	The VPA status: **inactive** (port is not active), **forwarding** (traffic is forwarding on this VPA), **blocking** (traffic is not forwarding on this VPA), or **filtering** (a mobile port's VLAN is administratively off or the port's default VLAN status is disabled; does not apply to fixed ports).
vlan admin	VLAN administrative status: **on** enables VLAN functions to operate; **off** disables VLAN functions without deleting the VLAN. Use the **vlan** command to change the VLAN administrative status.
vlan oper	VLAN operational status: **on** (enabled) or **off** (disabled). The operational status remains disabled until an active port is assigned to the VLAN. When the operational status is enabled, then VLAN properties (e.g. virtual router ports, Spanning Tree) are applied to ports and traffic flow. A VLAN must have an enabled administrative status before it can become operationally enabled.
port admin	Port administrative status: **on** (enabled) allows the port to send and receive data when it is active; **off** (disabled) prevents the port from sending and receiving traffic even if it has an active connection.
port oper	Port operational status: **on** (enabled) or **off** (disabled). If a port is currently in use, then the operational status is enabled. A port must have an enabled administrative status before it can become operationally enabled.

Release History

Release 5.1; command was introduced.

Related Commands

show vlan	Displays list of VLANs configured on the switch.
show vlan router mac status	Displays the current MAC router operating mode (single or multiple) and VLAN router port statistics.
show ip interface	Displays VLAN IP router port information.

MIB Objects

```
vlanMgrVpa
vpaTable
   vpaVlanNumber
   vpaIfIndex
   vpaType
   vpaState
   vpaStatus
vlanMgrVlan
vlanTable
   vlanAdmStatus
   vlanOperStatus
```

show vlan router mac status

Displays current status of multiple MAC router mode, the number of VLANs configured on the switch, the number of VLANs with router ports and the number of IP and IPX router ports configured.

show vlan router mac status

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If this mode is enabled, then a unique router port MAC address is assigned for each configured router port VLAN. Multiple MAC router mode supports the configuration 64 IP, IPX, or a combination of both router ports per switch.
- If this mode is disabled, then the switch is running in single MAC router mode, which uses the chassis base MAC address for every IP or IPX router port defined. Single MAC router mode supports the configuration of 4094 IP and 256 IPX router ports per switch.

Examples

```
-> show vlan router mac status
  router-mac-multiple   total vlans   router vlans   ip vlans   ipx vlans
----------------------+-------------+--------------+----------+------------
       disabled               7              6           4           2
```

output definitions

router-mac-multiple	Multiple MAC router mode status: **enabled** or **disabled**. If this mode is disabled, the switch is running in single MAC router mode. Use the **vlan router mac multiple** command to change this status.
total vlans	The total number of VLANs configured on the switch. Use the **vlan** command to create or remove VLANs.
router vlans	The total number of VLANs configured on the switch that have at least one router port defined (either IP or IPX). On an OmniSwitch 6600, 7700/7800, and 8800 use the **ip interface** command to define an IP router for a VLAN. On all platforms use the **vlan router ipx** commands to define an IPX router for a VLAN.

output definitions

ip vlans	The total number of VLANs configured on the switch that have an IP router port defined. On an OmniSwitch 6600, 7700/7800, and 8800 use the **ip interface** command to define an IP router for a VLAN.
ipx vlans	The total number of VLANs configured on the switch that have an IPX router port defined. Use the **vlan router ipx** command to define an IPX router port for a VLAN. This field will contain an **NA** when the **show vlan router mac status** command is used on an OmniSwitch 6600.

Release History

Release 5.1; command was introduced.

Related Commands

show vlan	Displays list of VLANs configured on the switch.
show vlan port	Displays VLAN port assignments.
show ip interface	Displays VLAN IP router port information.

MIB Objects

```
vlanMgrVlanSet
   vlanSetMultiRtrMacStatus
   vlanSetVlanCount
   vlanSetVlanRouterCount
   vlanSetIpRouterCount
   vlanSetIpxRouterCount
```

22 Port Mapping Commands

Port Mapping is a security feature, which controls the peer users from communicating with each other. Each session comprises a session ID and a set of user ports and/or a set of network ports. The user ports within a session cannot communicate with each other and can only communicate via network ports. In a Port Mapping session with user port set A and network port set B, ports in set A can communicate with ports in set B only. If set B is empty, the ports in set A can communicate with the rest of the ports in the system.

A port mapping session can be configured in a unidirectional or bidirectional mode. In the unidirectional mode, the network ports can communicate with each other within the same session. In the bidirectional mode, the network ports cannot communicate with each other. Network ports of a unidirectional port mapping session can be shared with other unidirectional sessions, but cannot be shared with any session configured in bidirectional mode. Network ports of different sessions can communicate with each other.

MIB information for the Port Mapping commands is as follows:

Filename: AlcatelIND1PortMapping.mib
Module: ALCATEL-IND1-PORT-MAPPING

A summary of the available commands is listed here:

port mapping user-port network-port
port mapping (configures port mapping status)
port mapping (configures port mapping direction)
show port mapping status
show port mapping

port mapping user-port network-port

Creates a port mapping session either with or without the user ports, network ports, or both. Use the **no** form of the command to delete ports or an aggregate from a session.

port mapping *port_mapping_sessionid* **[no] [user-port {slot** *slot* **|** *slot/port***[-***port2***] | linkagg** *agg_num***}] [network-port {slot** *slot* **|** *slot/port***[-***port2***] | linkagg** *agg_num***}]**

Syntax Definitions

port_mapping_sessionid	The port mapping session ID. Valid range is 1 to 8.
user-port	Specifies a user port of the mapping session.
network-port	Specifies a network port of the mapping session.
slot	Specifies a slot to be assigned to the mapping session.
slot	Slot number you want to configure.
port	Port number you want to configure.
port2	Last port number in a range of ports you want to configure.
linkagg	Specifies a link aggregation group to be assigned to the mapping session.
agg_num	Link aggregation number.

Defaults

N/A

Platforms Supported

OmniSwitch 6600

Usage Guidelines

- User ports that are part of one session cannot communicate with each other and can communicate only via network ports of the session to the rest of the system.
- User ports can be part of one Port Mapping session only.
- An aggregable port of a link aggregation group cannot be a mapped port and a mapped port cannot be an aggregable port of a link aggregation group.
- A mirrored port cannot be a mapped port and a mapped port cannot be a mirrored port.
- A mobile port cannot be configured as a network port of a mapping session.

Examples

```
-> port mapping 3 user-port 2/3 network-port 6/4
-> port mapping 4 user-port 2/5-8
-> port mapping 5 user-port 2/3 network-port slot 3
-> port mapping 5 no user-port 2/3
-> port mapping 6 no network-port linkagg 7
```

Release History

Release 5.4.1; command was introduced.

Related Commands

port mapping	Enables, disables, or deletes a port mapping session.
port mapping	Configures the direction of a port mapping session.
show port mapping	Displays the configuration of one or more port mapping sessions.

MIB Objects

```
PortMappingSessionTable
   pmapSessionNumber
portMappingTable
   pmapPortIfindex
   pmapPortType
```

port mapping

Enables, disables, or deletes a port mapping session.

port mapping *port_mapping_sessionid* **{enable | disable}**

no port mapping *port_mapping_sessionid*

Syntax Definitions

port_mapping_sessionid	The port mapping session ID. Valid range is 1 to 8.
enable	Enables a port mapping session.
disable	Disables a port mapping session.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6600

Usage Guidelines

To be enabled, a session should have a minimum of two ports.

Examples

```
-> port mapping 3 enable
-> port mapping 4 disable
-> no port mapping 5
```

Release History

Release 5.4.1; command was introduced.

Related Commands

port mapping user-port network-port	Creates a port mapping session with or without the user ports, network ports, or both.
port mapping	Configures the direction of a port mapping session.
show port mapping status	Displays the status of one or more port mapping sessions.
show port mapping	Displays the configuration of one or more port mapping sessions.

MIB Objects

```
PortMappingSessionTable
   pmapSessionNumber
   pmapSessionStatus
```

port mapping

Configures the direction of a port mapping session.

port mapping *port_mapping_sessionid* **{unidirectional | bidirectional}**

Syntax Definitions

port_mapping_sessionid	The port mapping session ID. Valid range is 1 to 8.
unidirectional	Specifies unidirectional port mapping.
bidirectional	Specifies bidirectional port mapping.

Defaults

parameter	default
unidirectional | bidirectional	**bidirectional**

Platform Supported

OmniSwitch 6600

Usage Guidelines

- In the bidirectional mode, the network ports of a session cannot communicate with each other. Also, the network ports of that session cannot be a part of a network port set of another session.
- In the unidirectional mode, the network ports of a session can communicate with each other. Also, the network ports of that session can be part of a network port set of another session, which is also in the unidirectional mode.
- To change the direction of an active session with network ports, delete the network ports of the session, change the direction, and recreate the network ports.

Examples

```
-> port mapping 5 unidirectional
-> port mapping 6 bidirectional
```

Release History

Release 5.4.1; command was introduced.

Related Commands

port mapping user-port network-port	Creates a port mapping session with or without the user ports, network ports or both.
port mapping	Enables, disables, or deletes a port mapping session.
show port mapping	Displays the configuration of one or more port mapping sessions.

MIB Objects

```
PortMappingSessionTable
   PmapSessionNumber
   PmapSessionDirection
```

show port mapping status

Displays the status of one or more port mapping sessions.

show port mapping [*port_mapping_sessionid*] **status**

Syntax definitions

port_mapping_sessionid	The port mapping session ID. Valid range is 1 to 8.

Defaults

N/A

Platforms Supported

OmniSwitch 6600

Usage Guidelines

If you do not specify the port mapping session ID, then the status of all the port mapping sessions will be displayed.

Examples

```
-> show port mapping status

SessionID       Direction        Status
------------+----------------+---------------
    8            bi               disable
```

output definitions

SessionID	Displays the port mapping session ID.
Direction	Displays the direction of a port mapping session.
Status	Displays status of a port mapping session.

Release History

Release 5.4.1; command was introduced.

Related Commands

port mapping user-port network-port	Creates a port mapping session with or without the user ports, network ports, or both.
port mapping	Enables, disables, or deletes a port mapping session.

MIB Objects

```
PortMappingSessionTable
   PmapSessionNumber
   PmapSessionDirection
   pmapSessionStatus
```

show port mapping

Displays the configuration of one or more port mapping sessions.

show port mapping [*port_mapping_sessionid***]**

Syntax Definitions

port_mapping_sessionid	The port mapping session ID. Valid range is 1 to 8.

Defaults

N/A

Platforms Supported

OmniSwitch 6600

Usage Guidelines

If you do not specify the port mapping session ID, then the configuration for all the port mapping sessions will be displayed.

Examples

```
-> show port mapping 3

SessionID       USR-PORT        NETWORK-PORT
----------+---------------+-----------------
     8          1/2               1/3
     8          1/6
     8          1/7
```

output definitions

SessionID	Displays the port mapping session ID.
USR-PORT	Displays the set of user ports of a port mapping session.
NETWORK-PORT	Displays the set of network ports of a port mapping session.

Release History

Release 5.4.1; command was introduced.

Related Commands

port mapping user-port network-port	Creates a port mapping session with or without the user ports, network ports, or both.
port mapping	Enables, disables, or deletes a port mapping session.

MIB Objects

```
PortMappingSessionTable
   PmapSessionNumber
   portMappingTable
   pmapPortIfindex
   pmapPortType
```

23 IP Commands

This chapter details Internet Protocol (IP) commands for the switch. IP is a network-layer (Layer 3) protocol that contains addressing information and some control information that enables packets to be forwarded. IP is documented in RFC 791 and is the primary network-layer protocol in the Internet protocol suite. Along with the Transmission Control Protocol (TCP), IP represents the heart of the Internet protocols.

IP is enabled on the switch by default and there are few options that can, or need to be, configured. This chapter provides instructions for basic IP configuration commands. It also includes commands for several Layer 3 and Layer 4 protocols that are associated with IP:

- Address Resolution Protocol (ARP)—Used to match the IP address of a device with its physical (MAC) address and to create a static ARP entry that associates a firewall IP address with a multicast MAC address.
- Internet Control Message Protocol (ICMP)—Specifies the generation of error messages, test packets, and informational messages related to IP. ICMP supports the **ping** command used to determine whether hosts are online.
- Transmission Control Protocol (TCP)—A major data transport mechanism that provides reliable, connection-oriented, full-duplex data streams. While the role of TCP is to add reliability to IP, TCP relies upon IP to do the actual delivering of datagrams.
- User Datagram Protocol (UDP)—A secondary transport-layer protocol that uses IP for delivery. UDP is not connection-oriented and does not provide reliable end-to-end delivery of datagrams. But some applications can safely use UDP to send datagrams that do not require the extra overhead added by TCP.

The IP commands also include protection from Denial of Service (DoS) attacks. The goal of this feature is to protect a switch from well-known DoS attacks and to notify the administrator or manager when an attack is underway. Also, notifications can be sent when port scans are being performed.

Note. Packets can be forwarded using IP if all devices are on the same VLAN, or if IP interfaces are created on multiple VLANs to enable routing of packets. However, IP routing requires one of the IP routing protocols: Routing Information Protocol (RIP) or Open Shortest Path First (OSPF). See the following chapters for the appropriate CLI commands: Chapter 27, “RIP Commands,” Chapter 30, “OSPF Commands.” For more information on VLANs and RIP see the applicable chapter(s) in the Configuration Guide. For more information on OSPF, see the “Configuring OSPF” chapter in the *OmniSwitch 7700/7800/8800 Advanced Routing Configuration Guide*.

MIB information for the IP commands is as follows:

Filename: IpForward.mib
Module: IpForward

Filename: Ip.mib
Module: Ip

Filename: AlcatelIND1Ip.mib
Module: alcatelIND1IPMIB

Filename: AlcatelIND1Iprm.mib
Module: alcatelIND1IPRMMIB

A summary of the available commands is listed here:

IP	**ip interface** **ip router primary-address** **ip router router-id** **ip static-route** **ip route-pref** **ip default-ttl** **ping** **traceroute** **ip directed-broadcast** **ip service** **debug ip packet** (configures debug parameters) **debug ip level** **debug ip packet default** **debug ip packet** (displays debug configuration parameters) **debug ip packet** **show ip traffic** **show ip interface** **show ip route** **show ip route-pref** **show ip emp-route** **show ip config** **show ip protocols** **show ip service**
ARP	**arp** **clear arp-cache** **arp filter** **clear arp filter** **show arp** **show arp filter**
ICMP	**icmp type** **icmp unreachable** **icmp echo** **icmp timestamp** **icmp addr-mask** **icmp messages** **show icmp control** **show icmp statistics**
TCP	**show tcp statistics** **show tcp ports**

UDP	**show udp statistics** **show udp ports**
Denial of Service (DoS)	**ip dos scan close-port-penalty** **ip dos scan tcp open-port-penalty** **ip dos scan udp open-port-penalty** **ip dos scan threshold** **ip dos trap** **ip dos scan decay** **show ip dos config** **show ip dos statistics**

ip interface

Configures an IP interface to enable IP routing on a VLAN. Without an IP interface, traffic is bridged within the VLAN or across connections to the same VLAN on other switches.

ip interface *name* **[address** *ip_address***] [mask** *subnet_mask***] [admin [enable | disable]] [vlan** *vid***] [forward | no forward] [local-proxy-arp | no local-proxy-arp] [e2 | snap] [mtu** *size***] [primary | no primary][firewall-vlan** *vid***]**

no ip interface *name*

Syntax Definitions

name	Text string of up to 20 characters. Use quotes around string if description contains multiple words with spaces between them (e.g., “Alcatel Marketing”). Note that this value is case sensitive.
ip_address	An IP host address (e.g., 10.0.0.1, 171.15.0.20) to specify the IP router network.
subnet_mask	A valid IP address mask (e.g., 255.0.0.0, 255.255.0.0) to identify the IP subnet for the interface.
enable	Enables the administrative status for the IP interface.
disable	Disables the administrative status for the IP interface.
vid	An existing VLAN ID number (1–4094).
forward	Enables forwarding of IP frames to other subnets.
no forward	Disables forwarding of IP frames. The router interface still receives frames from other hosts on the same subnet.
local-proxy-arp	Enables Local Proxy ARP on the specified interface. This parameter is not supported on the OmniSwitch 6600 Family
no local-proxy-arp	Disables Local Proxy ARP on the specified interface. This parameter is not supported on the OmniSwitch 6600 Family.
e2	Enter **e2** or **ethernet2** to specify Ethernet-II encapsulation.
snap	SNAP encapsulation.
size	The Maximum Transmission Unit (MTU) packet size for the specified interface (512–10222 bytes).
primary	Designates the specified IP interface as the primary interface for the VLAN.
no primary	Removes the configured primary IP interface designation for the VLAN. The first interface bound to the VLAN becomes the primary by default.
firewall-vlan	Designates a VLAN to be a firewall VLAN.

Defaults

parameter	default
ip_address	0.0.0.0
subnet_mask	IP address class
enable | disable	**enable**
vid	none (unbound)
forward | no forward	**forward**
local-proxy-arp | no local-proxy-arp	**no local-proxy-arp**
e2 | snap	**e2**
size	1500 bytes
primary | no primary	First interface bound to a VLAN.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of this command to remove an IP interface.
- Up to eight IP interfaces per VLAN are allowed on an OmniSwitch 6600, 7700/7800, and 8800.
- The total number of IP interfaces per switch depends on which MAC router mode is active. If the switch is running in multiple MAC router modes, then a maximum of 64 VLANs can have IP, IPX, or a combination of both interfaces. If the switch is running in a single MAC router mode, then a maximum of 4094 VLANs can have IP and 256 VLANs can have IPX interfaces.
- Note that when Local Proxy ARP is enabled for any one IP router interface associated with a VLAN, the feature is applied to the entire VLAN. It is not necessary to enable it for each interface. However, if the IP interface that has this feature enabled is moved to another VLAN, Local Proxy ARP is enabled for the new VLAN and must be enabled on another interface for the old VLAN.
- When Local Proxy ARP is enabled, all traffic is routed instead of bridged within the VLAN. ARP requests return the MAC address of the IP router interface. Note that the same MAC address is assigned to each interface configured for a VLAN.
- Local Proxy ARP takes precedence over any switch-wide ARP or Proxy ARP function. It is not necessary to have Proxy ARP configured in order to use Local Proxy ARP. The two features are independent of each other.
- Assign only ports to the VLAN that are capable of handling the MTU size restrictions configured for the IP interface(s) associated with the VLAN. For example, if an interface MTU size is greater than 1500, do not assign 10/100 Ethernet ports to the VLAN if traffic for the interface will originate or forward on these ports.
- The MTU range supported on the OmniSwitch 6600 Family is 512–1500 (data only).
- By default, the first interface bound to a VLAN becomes the primary interface for that VLAN. Use the **primary** keyword with this command to configure a different IP interface as the primary.

- To create an IP interface for network management purposes, specify **Loopback0** (case sensitive) as the name of the interface. The Loopback0 interface is not bound to any VLAN, hence it will always remain operationally active.
- To create an IP interface for firewall VLAN, use the **firewall-vlan** keyword, followed by the VLAN ID.

Examples

```
-> ip interface Marketing
-> ip interface Payroll address 18.12.6.3 vlan 255
-> ip interface “Human Resources” 10.200.12.101 vlan 500 no forward snap
-> ip interface “Distribution” 11.255.14.102 vlan 500 local-proxy-arp primary
-> ip interface firewall address 11.1.1.1 firewall-vlan 173
```

Release History

Release 5.1.6; command was introduced.
Release 5.4.1; command modified for OmniSwitch 6600 Family, 7700/7800, and 8800.

Related Commands

show ip interface	Displays the status and configuration of IP interfaces.

MIB Objects

```
alaIpInterfaceTable
   alaIpInterfaceName
   alaIpInterfaceAddress
   alaIpInterfaceMask
   alaIpInterfaceAdminState
   alaIpInterfaceDeviceType
   alaIpInterfaceVlanID
   alaIpInterfaceIpForward
   alaIpInterfaceEncap
   alaIpInterfaceMtu
   alaIpInterfaceLocalProxyArp
   alaIpInterfacePrimCfg
   alaIpInterfaceOperState
   alaIpInterfaceOperReason
   alaIpInterfaceRouterMac
   alaIpInterfaceBcastAddr
   alaIpInterfacePrimAct
   alaIpInterfaceFirewallVlanID
```

ip router primary-address

Configures the router primary IP address. The router primary IP address is used by advanced routing protocols to identify the switch on the network. It is also the address that is used to access the switch for management purposes.

ip router primary-address *ip_address*

Syntax Definitions

ip_address	32-bit IP address.

Defaults

parameter	default
ip_address	0.0.0.0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

If a particular protocol has not assigned a source address to outgoing packets, it will use the router primary address as the source address.

Examples

```
-> ip router primary-address 172.22.2.115
```

Release History

Release 5.1; command was introduced.

Related Commands

ip router router-id	Configures the router ID for the router.

MIB Objects

```
alaDcrTmConfig
   alaDrcTmIpRouterPrimaryAddress
```

ip router router-id

Configures the router ID for the router. By default, the router primary address of the router is used as the router ID. However, if a primary address has not been configured, the router ID is used by OSPF to identify the switch on the network.

ip router router-id *ip_address*

Syntax Definitions

ip_address	32-bit IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

The router ID can be any 32-bit number. It is not recommended to change the router ID when the OSPF and other protocols like BGP, RIP are enabled.

Examples

```
-> ip router router-id 172.22.2.115
```

Release History

Release 5.1; command was introduced.

Related Commands

ip router primary-address	Configures the router primary IP address.

MIB Objects

```
alaDcrTmConfig
   alaDrcTmIpRouterId
```

ip static-route

Creates/deletes an IP static route. Static routes are user-defined, they carry a higher priority than routes created by dynamic routing protocols. That is, static routes always have priority over dynamic routes, regardless of the metric value.

ip static-route *ip_address* **[mask** *mask***] gateway** *gateway* **[metric** *metric***]**

no ip static-route *ip_address* **[mask** *mask***] gateway** *ip_address* **[metric** *metric***]**

Syntax Definitions

ip_address	Destination IP address of the static route.
mask	Subnet mask corresponding to the destination IP address.
gateway	IP address of the next used to reach the destination IP address.
metric	RIP metric or cost (hop-count) for the static route. You can set a priority for the static route by assigning a metric value. The lower the metric value, the higher the priority. Valid range is 1–15.

Defaults

parameter	default
metric	1

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- A static route is not active unless the gateway it is using is active.
- The subnet mask is not required if you want to use the natural subnet mask. By default, the switch imposes a natural mask on the IP address.
- Static routes do not age out of the routing tables; however, they can be deleted. Use the **no** form of the command to delete a static route.
- Use the **ip static-route** command to configure default route. For example, to create a default route through gateway 171.11.2.1, you would enter: **ip static-route** 0.0.0.0 **mask** 0.0.0.0 **gateway** 171.11.2.1.
- You cannot create a default route using the EMP port as a gateway (on the OmniSwitch 7700, 7800, 8800).

Examples

```
-> ip static-route 171.11.1.1 gateway 171.11.2.1
-> ip static-route 0.0.0.0 mask 0.0.0.0 gateway 171.11.2.1
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip route	Displays the IP Forwarding table.

MIB Objects

```
alaIprmStaticRoute
   alaIprmStaticRouteDest
   alaIprmStaticRouteMask
   alaIprmStaticRouteNextHop
   alaIprmStaticRouteMetric
   alaIprmStaticRouteStatus
```

ip route-pref

Configures the route preference of a router.

ip route-pref {static | ospf | rip | bgp} *value*

Syntax definition

static	Configures the route preference of static routes.
ospf	Configures the route preference of OSPF routes.
rip	Configures the route preference of RIP routes.
bgp	Configures the route preference of BGP routes.
value	Route preference value.

Defaults

parameter	default
value	2 (**static**) 10 (**ospf**) 100 (**rip**) 20 (**bgp**)

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- BGP is not supported on OmniSwitch 6600 Family switches.
- Route preference of local routes cannot be changed.

Examples

```
-> ip route-pref bgp 20
-> ip route-pref rip 60
```

Release History

Release 5.4.1; command was introduced.

Related Commands

show ip route-pref	Displays the configured route-preference of a router.

MIB Objects

```
alaIprmRtPrefTable
   alaIprmRtPrefLocal
   alaIprmRtPrefStatic
   alaIprmRtPrefOspf
   alaIprmRtPrefRip
   alaIprmRtPrefBgp
```

ip default-ttl

Configures the Time To Live value (TTL) for IP packets. The TTL value is the maximum number of hops an IP packet will travel before being discarded.

ip *default*-ttl *hops*

Syntax Definitions

hops	TTL value, in hops. Valid range is 1–255.

Defaults

parameter	default
hops	64

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This value represents the default value inserted in the TTL field of the IP header for datagrams originating from this switch whenever a TTL value is not supplied by the transport layer protocol.

Examples

```
-> ip default-ttl 30
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip config	Displays IP configuration parameters.

MIB Objects

```
IpDefaultTTL
```

ping

Used to test whether an IP destination can be reached from the local switch. This command sends an ICMP echo request to a destination and then waits for a reply. To ping a destination, enter the **ping** command and enter either the destination's IP address or hostname. The switch will ping the destination using the default frame count, packet size, interval, and timeout parameters (6 frames, 64 bytes, 1 second, and 5 seconds, respectively). You can also customize any or all of these parameters as described below.

ping {*ip_address* | *hostname***} [count** *count***] [size** *packet_size***] [interval** *seconds***] [timeout** *seconds***]**

Syntax Definitions

ip_address	IP address of the system to ping.
hostname	DNS name of the system to ping.
count	Number of frames to be transmitted.
packet_size	Size of the data portion of the packet sent for this ping, in bytes. Valid range is 1–60000.
interval *seconds*	Polling interval. The switch will poll the host at time intervals specified in seconds.
timeout *seconds*	Number of seconds the program will wait for a response before timing out.

Defaults

parameter	default
count	6
packet_size	64
interval *seconds*	1
timeout *seconds*	5

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

If you change the default values they will only apply to the current ping. The next time you use the ping command, the default values will be used unless you again enter different values.

Examples

```
-> ping 10.255.11.242

PING 10.255.11.242: 56 data bytes
64 bytes from 10.255.11.242: icmp_seq=0. time=0. ms
64 bytes from 10.255.11.242: icmp_seq=1. time=0. ms
64 bytes from 10.255.11.242: icmp_seq=2. time=0. ms
64 bytes from 10.255.11.242: icmp_seq=3. time=0. ms
64 bytes from 10.255.11.242: icmp_seq=4. time=0. ms
64 bytes from 10.255.11.242: icmp_seq=5. time=0. ms
----10.255.11.242 PING Statistics----
6 packets transmitted, 6 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 0/0/0
```

Release History

Release 5.1; command was introduced.

Related Commands

traceroute	Used to find the path taken by an IP packet from the local switch to a specified destination.

traceroute

Used to find the path taken by an IP packet from the local switch to a specified destination. This command displays the individual hops to the destination as well as some timing information.

traceroute {*ip_address* | *hostname***} [max-hop** *max_hop_count***]**

Syntax Definitions

ip_address	IP address of the host whose route you want to trace.
hostname	DNS name of the host whose route you want to trace.
max_hop_count	Maximum hop-count for the trace.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- When using this command, you must enter the name of the destination as part of the command line (either the IP address or host name).
- Use the optional **max-hop** parameter to set a maximum hop-count to the destination. If the trace reaches this maximum hop-count without reaching the destination, the trace stops.

Examples

```
-> traceroute 128.251.17.224

traceroute to 128.251.17.224, 30 hops max, 40 byte packets
 1  10.255.11.254 0 ms  0 ms  0 ms
 2  172.23.0.251 0 ms  16.6667 ms  0 ms
 3  128.251.14.253 0 ms  0 ms  0 ms
 4  128.251.17.224 0 ms  0 ms  0 ms

-> traceroute 128.251.17.224 max-hop 3
traceroute to 128.251.17.224, 3 hops max, 40 byte packets
 1  10.255.11.254 0 ms  0 ms  0 ms
 2  172.23.0.251 16.6667 ms  0 ms  0 ms
 3  128.251.14.253 0 ms  0 ms  0 ms
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip route	Displays the IP Forwarding table.

ip directed-broadcast

Enables or disables IP directed broadcasts routed through the switch. An IP directed broadcast is an IP datagram that has all zeros or all 1's in the host portion of the destination address. The packet is sent to the broadcast address of a subnet to which the sender is not directly attached.

ip directed-broadcast {on | off}

Syntax Definitions

N/A

Defaults

The default value is **off**.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Directed broadcasts are used in denial-of-service "smurf" attacks. In a smurf attack, a continuous stream of ping requests are sent from a falsified source address to a directed broadcast address, resulting in a large stream of replies, which can overload the host of the source address. By default, the switch drops directed broadcasts. Typically, directed broadcasts should not be enabled.

Examples

```
-> ip directed-broadcast off
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip interface	Displays the status and configuration of IP interfaces.
show ip route	Displays the IP Forwarding table.
show ip config	Displays IP configuration parameters.

MIB Objects

```
alaIpDirectedBroadcast
```

ip service

Enables (opens) or disables (closes) well-known TCP/UDP service ports (i.e., SSH, telnet, FTP, etc.). Selectively enabling or disabling these types of ports provides an additional method for protecting against denial of service (DoS) attacks.

ip service { all | ftp | ssh | telnet | http | secure-http | avlan-http | avlan-secure-http | avlan-telnet | udp-relay | network-time | snmp | port *service_port* **}**

no ip service { all | ftp | ssh | telnet | http | secure-http | avlan-http | avlan-secure-http | avlan-telnet | udp-relay | network-time | snmp | port *service_port***}**

Syntax Definitions

all	Configures access to all TCP/UDP ports.
ftp	Configures access to FTP port 21.
ssh	Configures access to Secure Shell port 22.
telnet	Configures access to Telnet port 23.
http	Configures access to HTTP port 80.
secure-http	Configures access to secure HTTP port 443.
avlan-http	Configures access to Authenticated VLAN HTTP port 260.
avlan-secure-http	Configures access to Authenticated VLAN secure HTTP port 261.
avlan-telnet	Configures access to Authenticated VLAN Telnet port 259.
udp-relay	Configures access to UDP Relay port 67.
network-time	Configures access to Network Time Protocol (NTP) port 123.
snmp	Configures access to SNMP port 161.
port	Configures access to specific TCP/UDP port.
service_port	A TCP/UDP service port number. Configures access by port number rather than by service name.

Defaults

All TCP/UDP ports are open by default.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **all** option with this command to configure access to all well-known TCP/UDP service ports.
- To configure access to one or more service ports, specify the service name(s). See the examples below.
- This command only applies to TCP/UDP service ports opened by default. It does not affect ports that are opened by applications, such as RIP, BGP, etc.

Examples

```
-> ip service all
-> ip service ftp telnet snmp
-> ip service port 1024
-> no ip service ftp snmp
-> no ip service all
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip service	Displays a list of all well-known TCP/UDP ports and their current status (enabled or disabled).

MIB Objects

```
alaIpServiceTable
   alaIpServiceType
   alaIpServicePort
   alaIpServiceStatus
alaIpPortServiceTable
   alaIpPortServicePort
   alaIpPortServiceStatus
```

arp

Adds a permanent entry to the ARP table. To forward packets, the switch dynamically builds an ARP table to match the IP address of a device with its physical (MAC) address. These entries age out of the table when the timeout value is exceeded. This command is used to add a permanent entry to the table. Permanent entries do not age out of the table. It also creates a static ARP entry that associates a multicast mac address configured for firewall IP address only.

arp *ip_address mac_address* **[alias]**

no arp *ip_address* **[alias]**

Syntax Definitions

ip_address	IP address of the device you are adding to the ARP table.
mac_address	MAC address of the device in hexadecimal format (e.g., 00.00.39.59.f1.0c).
alias	Specifies that the switch will act as an alias (or proxy) for this IP address. When the alias option is used, the switch responds to all ARP requests for the specified IP address with its own MAC address. You can also enable the proxy feature for an IP interface using the **ip interface** command. When enabled, ARP requests return the MAC address of the IP router interface and all traffic within the VLAN is routed.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to delete a permanent ARP entry.
- Note that using the **arp alias** command is not related to proxy ARP as defined in RFC 925. Instead, **arp alias** is similar to the Local Proxy ARP feature, except that it is used to configure the switch as a proxy for only *one* IP address.
- Because most hosts support the use of address resolution protocols to determine cache address information (called dynamic address resolution), you generally do not need to specify permanent ARP cache entries.
- Only the IP address is required when deleting an ARP entry from the table.

Examples

```
-> arp 171.11.1.1 00:05:02:c0:7f:11
-> arp 11.1.1.5 01:00:5e:01:01:01
```

Release History

Release 5.1; command was introduced.

Related Commands

clear arp-cache	Deletes all dynamic entries from the ARP table.
ip interface	Enables or disables the Local Proxy ARP feature for an IP interface. When enabled, all traffic within the VLAN is routed. ARP requests return the MAC address of the IP router interface.
show arp	Displays the ARP table.

MIB Objects

```
ipNetToMediaTable
   ipNetToMediaIfIndex
   ipNetToMediaNetAddress
   ipNetToMediaPhyAddress
   ipNetToMediaType
alaIpNetToMediaTable
   alaIpNetToMediaPhyAddress
   alaIpNetToMediaProxy
```

clear arp-cache

Deletes all dynamic entries from the ARP table.

clear arp-cache

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This commands only clears dynamic entries. If permanent entries have been added to the table, they must be removed using the **no** form of the **ip service** command.
- Dynamic entries remain in the ARP table until they time out. The switch uses the MAC address table timeout value as the ARP timeout value. Use the **mac-address-table aging-time** command to set the timeout value.

Examples

```
-> clear arp-cache
```

Release History

Release 5.1; command was introduced.

Related Commands

ip service	Adds a permanent entry to the ARP table.
show arp	Displays the ARP table.

MIB Objects

```
alaIpClearArpCache
```

arp filter

Configures an ARP filter that will determine if ARP Request packets containing a specific IP address are processed by the switch or discarded.

arp filter *ip_address* **[mask** *ip_mask***] [***vid***] [sender | target] [allow | block]**

no arp filter *ip_address*

Syntax Definitions

ip_address	The IP address to use for filtering ARP packet IP addresses.
ip_mask	An IP mask that identifies which part of the ARP packet the IP address is examined for filtering (e.g., mask 255.0.0.0 filters on the first octet of the ARP packet IP address).
vid	A VLAN ID that specifies that only ARP packets for a specific VLAN are filtered.
sender	The sender IP address in the ARP packet is used for ARP filtering.
target	The target IP address in the ARP packet is used for ARP filtering.
allow	ARP packets that meet filter criteria are processed.
block	ARP packets that meet filter criteria are discarded.

Defaults

parameter	default
vid	0 (no VLAN)
ip_mask	255.255.255.255
sender | target	**target**
allow | **block**	**block**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to delete an ARP filter.
- If there are no filters configured for the switch, all ARP Request packets received are processed.
- Up to 200 filters are allowed on each switch.
- If sender or target IP address in an ARP Request packet does not match any filter criteria, the packet is processed by the switch.
- ARP filtering is generally used in conjunction with the Local Proxy ARP application; however, ARP filtering is available for use on its own and/or with other applications.

Examples

```
-> arp filter 171.11.1.1
-> arp filter 172.0.0.0 mask 255.0.0.0
-> arp filter 198.0.0.0 mask 255.0.0.0 sender
-> arp filter 198.172.16.1 vlan 200 allow
-> no arp filter 171.11.1.1
```

Release History

Release 5.1.6; command was introduced.

Related Commands

clear arp filter	Clears all ARP filters from the filter database.
ip interface	Enables or disables the Local Proxy ARP feature on an IP interface. When enabled, all traffic within the VLAN is routed. ARP requests return the MAC address of the IP router interface.
show arp filter	Displays the ARP filter configuration.

MIB Objects

```
alaIpArpFilterTable
   alaIpArpFilterIpAddr
   alaIpArpFilterIpMask
   alaIpArpFilterVlan
   alaIpArpFilterMode
   alaIpArpFilterType
```

clear arp filter

Clears the ARP filter database of all entries.

clear arp-cache

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This commands clears all ARP filters configured on the switch. To remove an individual filter entry, use the **no** form of the **arp filter** command.

Examples

```
-> clear arp filter
```

Release History

Release 5.1.6; command was introduced.

Related Commands

arp filter	Configures an ARP filter to allow or block the processing of specified ARP Request packets.
show arp filter	Displays the ARP filter configuration.

MIB Objects

```
alaIpClearArpFilter
```

icmp type

Enables or disables a specific type of ICMP message, and sets the minimum packet gap. The minimum packet gap is the number of microseconds that must pass between ICMP messages of the same type.

icmp type *type* **code** *code* **{{enable | disable} | min-pkt-gap** *gap***}**

Syntax Definitions

type	The ICMP packet type. This is in conjunction with the ICMP code, which determines the type of ICMP message being specified.
code	The ICMP code type. This is in conjunction with the ICMP type, which determines the type of ICMP message being specified.
enable	Enables the specified ICMP message.
disable	Disables the specified ICMP message.
gap	The number of microseconds required between ICMP messages of this type.

Defaults

parameter	default
enable | disable	**enable**
gap	0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command allows you to enable or disable all types of ICMP messages and set the minimum packet gap between messages of the specified type. The ICMP message types are specified in RFC 792, and are listed below:

ICMP Message	Type	Code
echo reply	**0**	**0**
network unreachable	**0**	**3**
host unreachable	**3**	**1**
protocal unreachable	**3**	**2**
port unreachable	**3**	**3**
frag needed but DF bit set	**3**	**4**
source route failed	**3**	**5**
destination network unknown	**3**	**6**
destination host unknown	**3**	**7**
source host isolated	**3**	**8**
dest network admin prohibited	**3**	**9**
host admin prohibited by filter	**3**	**10**
network unreachable for TOS	**3**	**11**
host unreachable for TOS	**3**	**12**
source quench	**4**	**0**
redirect for network	**5**	**0**
redirect for host	**5**	**1**
redirect for TOS and network	**5**	**2**
redirect for TOS and host	**5**	**3**
echo request	**8**	**0**
router advertisement	**9**	**0**
router solicitation	**10**	**0**
time exceeded during transmit	**11**	**0**
time exceeded during reassembly	**11**	**1**
ip header bad	**12**	**0**
required option missing	**12**	**1**
timestamp request	**13**	**0**
timestamp reply	**14**	**0**
information request (obsolete)	**15**	**0**
information reply (obsolete)	**16**	**0**
address mask request	**17**	**0**
address mask reply	**18**	**0**

- While this command can be used to enable or disable all ICMP messages, some of the more common ICMP messages have their own CLI commands, as described in the pages below. The following ICMP message have specific commands to enable and disable:

ICMP Message	Command
Network unreachable (type 0, code 3)	**icmp unreachable**
Host unreachable (type 3, code 1)	**icmp unreachable**
Protocol unreachable (type 3, code 2)	**icmp unreachable**
Port unreachable (type 3, code 3)	**icmp unreachable**
Echo reply (type 0, code 0)	**icmp echo**
Echo request (type 8, code 0)	**icmp echo**
Timestamp request (type 13, code 0)	**icmp timestamp**
Timestamp reply (type 14, code 0)	**icmp timestamp**
Address Mask request (type 17, code 0)	**icmp addr-mask**
Address Mask reply (type 18, code 0)	**icmp addr-mask**

Examples

```
-> icmp type 4 code 0 enabled
-> icmp type 4 code 0 min-pkt-gap 40
-> icmp type 4 code 0 disable
```

Release History

Release 5.1; command was introduced.

Related Commands

icmp messages	Enables or disables all ICMP messages.
show icmp control	This command allows the viewing of the ICMP control settings.

MIB Objects

```
alaIcmpCtrlTable
   alaIcmpCtrlType
alaIcmpCtrlTable
   alaIcmpCtrlCode
   alaIcmpCtrlStatus
   alaIcmpCtrlPktGap
```

icmp unreachable

This command allows the enabling or disabling of ICMP messages pertaining to unreachable destinations, and sets the minimum packet gap. The minimum packet gap is the number of microseconds that must pass between ICMP messages of the same type.

icmp unreachable [net-unreachable | host-unreachable | protocol-unreachable | port-unreachable] {{enable | disable} | min-pkt-gap *gap***}**

Syntax Definitions

net-unreachable	Sets the unreachable network ICMP message.
host-unreachable	Sets the unreachable host ICMP message.
protocol-unreachable	Sets the unreachable protocol ICMP message.
port-unreachable	Sets the unreachable port ICMP message.
enable	Enables the specified ICMP message.
disable	Disables the specified ICMP message.
gap	The number of microseconds required between ICMP messages of this type.

Defaults

parameter	default
enable | disable	**disable**
gap	0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command enables ICMP messages relating to unreachable destinations. Unreachable networks, hosts, protocols, and ports can all be specified.
- The unreachable ICMP messages can also be enabled, disabled, and modified using the **icmp type** command. See the **icmp type** command information on the type and code for the unreachable ICMP messages.

Examples

```
-> icmp unreachable net-unreachable enable
-> icmp unreachable host-unreachable enable
-> icmp unreachable protocol-unreachable enable
-> icmp unreachable port-unreachable enable
-> icmp unreachable port-unreachable min-pkt-gap 50
```

Release History

Release 5.1; command was introduced.

Related Commands

show icmp control	This command allows viewing the ICMP control settings.

MIB Objects

```
alaIcmpCtrlTable
   alaIcmpCtrlType
alaIcmpCtrlTable
   alaIcmpCtrlCode
   alaIcmpCtrlStatus
   alaIcmpCtrlPktGap
```

icmp echo

This command allows the enabling or disabling of ICMP echo messages and sets the minimum packet gap. The minimum packet gap is the number of microseconds that must pass between ICMP messages of the same type.

icmp echo [request | reply] {{enable | disable} | min-pkt-gap *gap***}**

Syntax Definitions

request	Specifies the echo request ICMP message.
reply	Specifies the echo reply ICMP message.
enable	Enables the specified ICMP message.
disable	Disables the specified ICMP message.
gap	The number of microseconds required between ICMP messages of this type.

Defaults

parameter	default
enable | disable	**enable**
gap	0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command sets the ICMP echo messages. An echo request is sent to a destination and must be responded to with an echo reply message that contains the original echo request.
- Using this command without specifying a request or reply will enable, disable, or set the minimum packet gap for both types.
- The echo ICMP messages can also be enabled, disabled, and modified using the **icmp type** command. See the **icmp type** command information on the type and code for the echo ICMP messages.

Examples

```
-> icmp echo reply enable
-> icmp echo enable
-> icmp echo request enable
-> icmp echo request min-pkt-gap 50
```

Release History

Release 5.1; command was introduced.

Related Commands

show icmp control	This command allows viewing the ICMP control settings.

MIB Objects

```
alaIcmpCtrlTable
   alaIcmpCtrlType
alaIcmpCtrlTable
   alaIcmpCtrlCode
   alaIcmpCtrlStatus
   alaIcmpCtrlPktGap
```

icmp timestamp

This command allows the enabling or disabling of ICMP timestamp messages and sets the minimum packet gap. The minimum packet gap is the number of microseconds that must pass between ICMP messages of the same type.

icmp timestamp [request | reply] {{enable | disable} | min-pkt-gap *gap***}**

Syntax Definitions

request	Specifies timestamp request messages.
reply	Specifies timestamp reply messages.
enable	Enables the specified ICMP message.
disable	Disables the specified ICMP message.
gap	The number of microseconds required between ICMP messages of this type.

Defaults

parameter	default
enable | disable	**enable**
gap	0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The data received (a timestamp) in the message is returned in the reply together with an additional timestamp. The timestamp is 32 bits of milliseconds since midnight UT. The Originate timestamp is the time the sender last touched the message before sending it, the Receive timestamp is the time the echoer first touched it on receipt, and the Transmit timestamp is the time the echoer last touched the message on sending it.
- Using this command without specifying a request or reply will enable, disable, or set the minimum packet gap for both types.
- The timestamp ICMP messages can also be enabled, disabled, and modified using the **icmp type** command. See the **icmp type** command information on the type and code for the timestamp ICMP messages.

Examples

```
-> icmp timestamp reply enable
-> icmp timestamp enable
-> icmp timestamp request enable
-> icmp timestamp request min-pkt-gap 50
```

Release History

Release 5.1; command was introduced.

Related Commands

show icmp control	This command allows viewing the ICMP control settings.

MIB Objects

```
alaIcmpCtrlTable
   alaIcmpCtrlType
alaIcmpCtrlTable
   alaIcmpCtrlCode
   alaIcmpCtrlStatus
   alaIcmpCtrlPktGap
```

icmp addr-mask

This command allows the enabling or disabling of ICMP address mask messages and sets the minimum packet gap. The minimum packet gap is the number of microseconds that must pass between ICMP messages of the same type.

icmp add-mask [request | reply] {{enable | disable} | min-pkt-gap *gap***}**

Syntax Definitions

request	Specifies request address mask messages.
reply	Specifies reply address mask messages.
enable	Enables the specified ICMP message.
disable	Disables the specified ICMP message.
gap	The number of microseconds required between ICMP messages of this type.

Defaults

parameter	default
enable | disable	**enable**
gap	0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- A gateway receiving an address mask request should return it with the address mask field set to the 32-bit mask of the bits identifying the subnet and network for the subnet on which the request was received.
- Using this command without specifying a request or reply will enable, disable, or set the minimum packet gap for both types.
- The address mask ICMP messages can also be enabled, disabled, and modified using the **icmp type** command. See the **icmp type** command information on the type and code for the address mask ICMP messages.

Examples

```
-> icmp addr-mask reply enable
-> icmp addr-mask enable
-> icmp addr-mask request enable
-> icmp addr-mask request min-pkt-gap 50
```

Release History

Release 5.1; command was introduced.

Related Commands

show icmp control	This command allows viewing the ICMP control settings.

MIB Objects

```
alaIcmpCtrlTable
   alaIcmpCtrlType
alaIcmpCtrlTable
   alaIcmpCtrlCode
   alaIcmpCtrlStatus
   alaIcmpCtrlPktGap
```

icmp messages

Enables or disables all Internet Control Message Protocol (ICMP) messages.

icmp messages {enable | disable}

Syntax Definitions

enable	Enables ICMP messages.
disable	Disables ICMP messages.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> icmp messages enable
-> icmp messages disable
```

Release History

Release 5.1; command was introduced.

Related Commands

icmp type	Enables or disables a specific type of ICMP message and sets the minimum packet gap.
show icmp control	This command allows viewing the ICMP control settings.

MIB Objects

```
alaIcmpCtrl
   alaIcmpAllMsgStatus
```

ip dos scan close-port-penalty

Assigns a penalty value to be added to the Denial of Service penalty scan value when a TCP or UDP packet is received on a closed port.

ip dos scan close-port-penalty *penalty_value*

Syntax Definitions

penalty_value	A penalty value added to the penalty scan value. This value can be any non-negative integer.

Defaults

parameter	default
penalty_value	10

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This command creates a point value that is added to the total port scan penalty value when a TCP or UDP packet is received that is destined for a closed port.

Examples

```
-> ip dos scan close-port-penalty 25
```

Release History

Release 5.1; command was introduced.

Related Commands

ip dos scan threshold	Sets the threshold for the port scan value at which a DoS attack is recorded.
ip dos trap	Sets whether the switch generates SNMP DoS traps when an attack is detected.

MIB Objects

```
alaDoSConfig
   alaDoSPortScanClosePortPenalty
```

ip dos scan tcp open-port-penalty

Assigns a penalty value to be added to the Denial of Service penalty scan value when a TCP packet is received on an open port.

ip dos scan tcp open-port-penalty *penalty_value*

Syntax Definitions

penalty_value	A penalty value added to the penalty scan value. This value can be any non-negative integer.

Defaults

parameter	default
penalty_value	0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command creates a point value that is added to the total port scan penalty value when a TCP packet is received that is destined for an open port.
- The switch does not distinguished between a legal TCP packet and a port scan packet.

Examples

```
-> ip dos scan tcp open-port-penalty 10
```

Release History

Release 5.1; command was introduced.

Related Commands

ip dos scan threshold	Sets the threshold for the port scan value at which a DoS attack is recorded.
ip dos trap	Sets whether the switch generates SNMP DoS traps when an attack is detected.

MIB Objects

```
alaDoSConfig
   alaDoSPortScanTcpOpenPortPenalty
```

ip dos scan udp open-port-penalty

Assigns a penalty value to be added to the Denial of Service penalty scan value when a UDP packet is received on an open port.

ip dos scan udp open-port-penalty *penalty_value*

Syntax Definitions

penalty_value	A penalty value added to the penalty scan value. This value can be any non-negative integer.

Defaults

parameter	default
penalty_value	0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command creates a point value that is added to the total port scan penalty value when a UDP packet is received that is destined for an open port.
- The switch does not distinguished between a legal UDP packet and a port scan packet.

Examples

```
-> ip dos scan udp open-port-penalty 15
```

Release History

Release 5.1; command was introduced.

Related Commands

ip dos scan threshold	Sets the threshold for the port scan value at which a DoS attack is recorded.
ip dos trap	Sets whether the switch generates SNMP DoS traps when an attack is detected.

MIB Objects

```
alaDoSConfig
   alaDoSPortScanUdpOpenPortPenalty
```

ip dos scan threshold

Sets the threshold for the port scan value at which a DoS attack is recorded.

ip dos scan threshold *threshold_value*

Syntax Definitions

threshold_value	A numerical value representing the total acceptable penalty before a DoS attack is noted. This value can be any non-negative integer.

Defaults

parameter	default
threshold_value	1000

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If the total port scan penalty value exceeds this value, a port scan attack is recorded.
- The penalty value is incremented by recording TCP or UDP packets that are bound for open or closed ports. Such packets are given a penalty value, which are added together. The commands for setting the packet penalty value are the **ip dos scan close-port-penalty**, **ip dos scan tcp open-port-penalty**, and **ip dos scan udp open-port-penalty** commands.

Examples

```
-> ip dos scan threshold 1200
```

Release History

Release 5.1; command was introduced.

Related Commands

ip dos scan close-port-penalty	Assigns a penalty value to be added to the Denial of Service penalty scan value when a TCP or UDP packet is received on a closed port.
ip dos scan tcp open-port-penalty	Assigns a penalty value to be added to the Denial of Service penalty scan value when a TCP packet is received on an open port.
ip dos scan udp open-port-penalty	Assigns a penalty value to be added to the Denial of Service penalty scan value when a UDP packet is received on an open port.
show ip dos config	Displays the configuration parameters of the DoS scan for the switch.

MIB Objects

```
alaDoSConfig
   alaDoSPortScanThreshold
```

ip dos trap

Sets whether the switch generates SNMP DoS traps when an attack is detected.

ip dos trap {enable | disable}

Syntax Definitions

enable	Enables the generation of DoS traps.
disable	Disables the generation of DoS traps.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This command controls whether the switch generates an SNMP trap when a DoS attack is detected. It is assumed a DoS attack has occurred when the port scan penalty threshold is exceeded. This value is set using the **ip dos scan threshold** command.

Examples

```
-> ip dos trap enable
-> ip dos trap disable
```

Release History

Release 5.1; command was introduced.

Related Commands

ip dos scan threshold	Sets the threshold for the port scan value, at which a DoS attack is recorded.
show ip dos config	Displays the configuration parameters of the DoS scan for the switch.

MIB Objects

```
alaDoSConfig
   alaDoSTrapCnt1
```

ip dos scan decay

Sets the decay speed of the port scan penalty value for the switch when calculating DoS attacks.

ip dos scan decay *decay_value*

Syntax Definitions

decay_value	The decay value amount for reducing the port scan penalty. This value can be any non-negative integer.

Defaults

parameter	default
decay_value	2

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

The port scan penalty value is reduced every minute by dividing by the amount set in using this command. For example, if the decay value is set to 10, every minute the total port scan penalty value is divided by 10.

Examples

```
-> ip dos scan decay 10
```

Release History

Release 5.1; command was introduced.

Related Commands

ip dos scan threshold	Sets the threshold for the port scan value at which a DoS attack is recorded.
show ip dos config	Displays the configuration parameters of the DoS scan for the switch.

MIB Objects

```
alaDoSConfig
   alaDoSPortScanDecay
```

show ip traffic

Displays IP datagram traffic and errors.

show ip traffic

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The statistics show the cumulative totals since the last time the switch was powered on or since the last reset of the switch was executed.
- Packets received on a port that is a member of the UserPorts group are dropped if they contain a source IP network address that does not match the IP subnet for the port. This is done to block spoofed IP traffic. If the UserPorts group function is active and spoofed traffic was detected and blocked, the output display of this command will include statistics regarding the spoofed traffic.
- Note that the presence of spoofing event statistics in the output display of this command indicates that an attack was prevented, not that the switch is currently under attack.
- If statistics for spoofed traffic are not displayed, then a spoofing attempt has not occurred since the last time this command was issued. Note that the UserPorts group function is available on the OmniSwitch 7700/7800 and 8800 only.

Examples

```
-> show ip traffic

IP statistics
  Datagrams received
    Total                  =   621883,
    IP header error        =        0,
    Destination IP error   =    51752,
    Unknown protocol       =        0,
    Local discards         =        0,
    Delivered to users     =   567330,
    Reassemble needed      =        0,
    Reassembled            =        0,
    Reassemble failed      =        0
```

```
 Datagrams sent
   Fowarded               =     2801,
   Generated              =   578108,
   Local discards         =        0,
   No route discards      =        9,
   Fragmented             =     2801,
   Fragment failed        =        0,
   Fragments generated    =        0

Event        Source       Total        Last 33 seconds
-------------+-------+------------+-----------------------
spoof         5/26   18           2          last mac 00:08:02:e2:17:70
```

output definitions

Total	Total number of input datagrams received including those received in error.
IP header error	Number of IP datagrams discarded due to errors in the IP header (e.g., bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discarded in processing IP options).
Destination IP error	Number of IP datagrams discarded because the IP header destination field contained an invalid address. This count includes invalid addresses (e.g., 0.0.0.0) and addresses of unsupported classes (e.g., Class E).
Unknown protocol	Number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
Local discards	Number of IP datagrams received that were discarded, even though they had no errors to prevent transmission (e.g., lack of buffer space). This does not include any datagrams discarded while awaiting reassembly. Typically, this value should be zero.
Delivered to users	Total number of datagrams received that were successfully delivered to IP user protocols (including ICMP).
Reassemble needed	Number of IP fragments received that needed to be reassembled.
Reassembled	Number of IP datagrams received that were successfully reassembled.
Reassemble failed	Number of IP failures detected by the IP reassembly algorithm for all reasons (e.g., timed out, error). This is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
Fragmented	Number of successfully fragmented IP datagrams.
Fragment failed	Number of packets received and discarded by IP because they needed to be fragmented but could not be. This situation could happen if a large packet has the “Don’t Fragment” flag set.
Forwarded	Number of IP datagrams forwarded by the switch.
Generated	Total number of IP datagrams that local IP user protocols (including ICMP) generated in response to requests for transmission. This does not include any datagrams counted as “Forwarded.”
Local discards	Number of output IP datagrams that were discarded, even though they had no errors to prevent transmission (e.g., lack of buffer space). This number includes datagrams counted as “Forwarded” if the packets are discarded for these reasons.

output definitions (continued)

No route discards	Number of IP datagrams received and discarded by IP because no route could be found to transmit them to their destination. This includes any packets counted as "Forwarded" if the packets are discarded for these reasons. It also includes any datagrams that a host cannot route because all of its default routers are down.
Fragments generated	The of IP datagram fragments generated as a result of fragmentation.
Routing entry discards	Number of packets received and discarded by IP even though no problems were encountered to prevent their transmission to their destination (e.g., discarded because of lack of buffer space).
Event	The type of event (**spoof**).
Source	The slot and port number of the port that has received spoofed packets and is also a member of the UserPorts group. Ports are configured as members of the UserPorts group through the **policy port group** command.
Total	The total number of spoofed packets received on the source port.
Last *xx* **seconds**	The number of spoofed packets blocked in the last number of seconds indicated. Also includes the source MAC address of the last spoofed packet received.

Release History

Release 5.1; command was introduced.

Related Commands

show icmp statistics	Displays ICMP statistics and errors.

show ip interface

Displays the configuration and status of IP interfaces.

show ip interface [*name* | **emp | vlan** *vlan id***]**

Syntax Definitions

name	The name associated with the IP interface.
emp	Displays the configuration and status of the Ethernet Management Port interface.
vlan_id	VLAN ID (displays a list of IP interfaces associated with a VLAN).

Defaults

By default, all IP interfaces are displayed.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The basic **show ip interface** command displays information about all configured IP interfaces on the switch.
- Use the optional **vlan** parameter to display a list of interfaces configured for the specified VLAN.
- Specify an optional interface *name* to display detailed information about an individual interface.
- Use the optional **emp** parameter to display detailed information about the EMP interface.

Examples

```
-> show ip interface
Total 11 interfaces
        Name            IP Address     Subnet Mask   Status Forward  Device
--------------------+---------------+--------------+------+-------+--------
EMP                 172.22.16.115   255.255.255.0       UP      NO EMP
GMRULE              40.1.1.1        255.255.255.0     DOWN      NO vlan 40
Loopback            127.0.0.1       255.0.0.0           UP      NO Loopback
client              60.1.1.1        255.255.255.0     DOWN      NO vlan 60
firewall            11.1.1.1        255.0.0.0           UP     YES firewall 173

gbps                5.5.5.5         255.255.255.0     DOWN      NO vlan 7
if222               30.1.5.1        255.0.0.0           UP     YES vlan 222
ldap_client1        173.22.16.115   255.255.255.0       UP     YES vlan 173
ldap_server1        174.22.16.115   255.255.255.0       UP     YES vlan 174
radius_client3      110.1.1.101     255.255.255.0       UP     YES vlan 30
vlan-2              0.0.0.0         0.0.0.0           DOWN      NO unbound
```

output definitions

Name	Interface name. Generally, this is the name configured for the interface (e.g., Accounting). **EMP** refers to the Ethernet Management Port. **Loopback** refers to a loopback interface configured for testing.
IP Address	IP address of the interface. Configured through the **ip interface** command.
Subnet Mask	IP subnet mask for the interface IP address. Configured through the **ip interface** command.
Status	Interface status: • **UP**—Interface is ready to pass packets. • **DOWN**—Interface is down.
Forward	Indicates whether or not the interface is actively forwarding packets (**YES** or **NO**).
Device	The type of device bound to the interface: • **unbound**—No device is bound to the interface. • **vlan**—The VLAN ID that is bound to the interface. • **EMP**—The Ethernet Management Port is bound to the interface. • **Loopback**—A loopback interface is configured for testing. Configured through the **ip interface** command.

```
-> show ip interface Marketing
Interface Name = Marketing
  SNMP Interface Index          =   13600007,
  IP Address                    =   172.16.105.10,
  Subnet Mask                   =   255.255.0.0,
  Broadcast Address             =   172.16.255.255,
  Device                        =   vlan 200,
  Encapsulation                 =   eth2,
  Forwarding                    =   disabled,
  Administrative State          =   enabled,
  Operational State             =   down,
  Operational State Reason      =   device-down,
  Router MAC                    =   00:d0:95:6a:f4:5c,
  Local Proxy ARP               =   disabled,
  Maximum Transfer Unit         =   1500,
  Primary (config/actual)       =   no/yes
```

output definitions

SNMP interface index	Interface index.
IP Address	IP address associated with the interface. Configured through the **ip interface** command.
Subnet Mask	IP subnet mask for the interface. Configured through the **ip interface** command.
Broadcast Address	Broadcast address for the interface.

output definitions

Device	The type of device bound to the interface: • **unbound**—No device is bound to the interface. • **vlan**—The VLAN ID that is bound to the interface. • **EMP**—The Ethernet Management Port is bound to the interface. • **Loopback**—A loopback interface is configured for testing. Configured through the **ip interface** command.
Encapsulation	Displays the IP router encapsulation (**eth2** or **snap**) that the interface will use when routing packets. Configured through the **ip interface** command.
Forwarding	Indicates whether or not IP forwarding is active for the interface (**enabled** or **disabled**). Configured through the **ip interface** command.
Administrative State	Administrative state of the IP interface (**enabled** or **disabled**), which is independent of the state of the underlying device. Configured through the **ip interface** command.
Operational State	Indicates whether or not the interface is active (**up** or **down**).
Operation State Reason	Indicates why the operational state of the interface is down: • **unbound**—No device is bound to the interface. • **device-down—**Device bound to the interface is down. • **admin-down—**The admin state of the interface is down. • **no-such-device—**Device does not exist. • **no-router-mac—**No MAC address available for the interface. Note that this field is only included in the display output when the operational state of the interface is **down**.
Router MAC	Switch MAC address assigned to the interface. Note that each interface assigned to the same VLAN will share the same switch MAC address.
Local Proxy ARP	Indicates whether or not Local Proxy ARP is active for the interface (**enabled** or **disabled**). Configured through the **ip interface** command.
Maximum Transfer Unit	The Maximum Transmission Unit size set for the interface. Configured through the **ip interface** command.
Primary (config/actual)	Indicates if the interface is the configured and/or actual primary interface for the device (VLAN, EMP, Loopback). If the actual status is set to **yes** and the config status is set to **no**, the interface is the default interface for the VLAN. Configured through the **ip interface** command.

Release History

Release 5.1; command was introduced.
Release 5.1.6; command modified for OmniSwitch 6600 Family, 7700/7800, and 8800.

Related Commands

show icmp statistics	Displays ICMP statistics and errors.

MIB Objects

```
alaIpInterfaceTable
   alaIpInterfaceName
   alaIpInterfaceAddress
   alaIpInterfaceMask
   alaIpInterfaceAdminState
   alaIpInterfaceDeviceType
   alaIpInterfaceVlanID
   alaIpInterfaceIpForward
   alaIpInterfaceEncap
   alaIpInterfaceMtu
   alaIpInterfaceLocalProxyArp
   alaIpInterfacePrimCfg
   alaIpInterfaceOperState
   alaIpInterfaceOperReason
   alaIpInterfaceRouterMac
   alaIpInterfaceBcastAddr
   alaIpInterfacePrimAct
```

show ip route

Displays the IP Forwarding table.

show ip route [summary]

Syntax Definitions

summary	Displays a summary of routing protocols that appear in the IP Forwarding table.

Defaults

By default, all routes are displayed.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The IP Forwarding table includes static routes as well as all routes learned through routing protocols (e.g., RIP, OSPF).
- Use the optional **summary** keyword to display a list of routing protocols and the number of routes for each protocol that appear in the IP Forwarding table.

Examples

```
-> show ip route

+ = Equal cost multipath routes
 Total 4 routes

  Dest Address      Subnet Mask       Gateway Addr      Age       Protocol
------------------+-----------------+-----------------+---------+-----------
  0.0.0.0           0.0.0.0           10.255.11.254     01:50:33  NETMGMT
  10.255.11.0       255.255.255.0     10.255.11.225     01:50:33  LOCAL
  127.0.0.1         255.255.255.255   127.0.0.1         01:51:47  LOCAL
  212.109.138.0     255.255.255.0     212.109.138.138   00:33:07  LOCAL

-> show ip route summary

  Protocol        Route Count
----------------+--------------
  All                      4
  Local                    3
  Netmgmt                  1
  RIP                      0
  ISIS                     0
  OSPF                     0
  BGP                      0
  Other                    0
```

output definitions

Dest Addr	Destination IP address.
Subnet Mask	Destination IP address IP subnet mask.
Gateway Addr	IP address of the gateway from which this address was learned.
Age	Age of the entry. If the entry is less than a day old, it is displayed in *hh/mm/ss* format. If it is more than a day old, it is displayed in *dd/hh* format (e.g., a route that is 2 days and 12 hours old is displayed as 2d12h).
Protocol	Protocol by which this IP address was learned (e.g., RIP). NETMGT indicates a static route. LOCAL indicates a local interface.
Route Count	The number of routes that appear in the IP Forwarding table for each protocol type listed.

Release History

Release 5.1; command was introduced.

Related Commands

ping	Used to test whether an IP destination can be reached from the local switch.
traceroute	Used to find the path taken by an IP packet from the local switch to a specified destination.
show ip route	Displays a list of all routes (static and dynamic) that exist in the IP router database.

show ip route-pref

Displays the configured route preference of a router.

Show ip route-pref [static | ospf | rip | bgp]

Syntax defns

static	Displays the route preference of static routes.
ospf	Displays the route preference of OSPF routes.
rip	Displays the route preference of RIP routes.
bgp	Displays the route preference of BGP routes.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- BGP is not supported on OmniSwitch 6600.

Examples

```
-> show ip route-pref
  Protocol    Route Preference Value
------------+------------------------
  Local                  1
  Static                 2
  OSPF                  10
  BGP                   20
  RIP                  100
```

Release History

Release 5.4.1; command was introduced.

Related Commands

ip route-pref	Configures the route preference of a router.

MIB Objects

```
alaIprmRtPrefTable
  alaIprmRtPrefLocal
  alaIprmRtPrefStatic
  alaIprmRtPrefOspf
  alaIprmRtPrefRip
  alaIprmRtPrefBgp
```

show ip router database

Displays a list of all routes (static and dynamic) that exist in the IP router database. This database serves as a central repository where routes are first processed for redistribution and where duplicate routes are compared to determine the best route to use. If a route does not appear in the IP router database list, then the switch does not know about it. In the case of dynamically learned routes, this could indicate that the route was never received by the switch.

show ip router database [protocol *type* | **gateway** *ip_address* | **dest** *ip_address mask***]**

Syntax Definitions

type	Routing protocol type (local, static, OSPF, RIP, or BGP).
ip_address	Destination IP address.
mask	Subnet mask corresponding to the destination IP address.

Defaults

By default, all routes are displayed.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Command options are not mutually exclusive. You can use them on the same command line to narrow and/or customize the output display of this command. For example, use the **protocol** and **dest** options to display only those routes that are of a specific protocol type and have the specified destination network.
- The IP Forwarding table is derived from IP router database processing performed by the switch and contains only unique routes that the switch currently uses. Use the **show ip route** command to view the forwarding table.
- If an expected route does not appear in the IP Forwarding table, use the **show ip router database** command to see if the switch knows about the route and/or if a duplicate route with a higher precedence was selected instead.
- The switch compares the protocol of duplicate routes to determine which one to use. Regardless of whether or not a route has a higher priority metric value, protocol determines precedence. Local routes are given the highest level of precedence followed by static, OSFP, RIP, then BGP routes. As a result, a route that is known to the switch may not appear in the IP ForwardingTable if a duplicate route with a higher protocol precedence exists.
- A list of inactive static routes is also included in the **show ip router database** output display. A route becomes inactive if the interface for its gateway goes down. Inactive routes are unable to get to their destination and further investigation is warranted to determine why their gateway is unavailable.
- Routes that appear inactive are not included in the main IP router database listing. However, if an inactive route becomes active it is removed from the inactive list and added to the active route list.

Examples

```
-> show ip router database
Destination         Gateway          Protocol Metric VLAN
------------------+----------------+--------+------+-----
10.212.31.0/24      10.212.60.27     OSPF     2      44
10.212.31.0/24      10.212.61.27     OSPF     2      43
10.212.59.0/24      10.212.59.17     LOCAL    1      45
10.212.60.0/24      10.212.60.17     LOCAL    1      44
10.212.61.0/24      10.212.61.17     LOCAL    1      43
10.212.62.0/24      10.212.60.27     OSPF     2      44
10.212.62.0/24      10.212.61.27     OSPF     2      43
10.212.63.0/24      10.212.60.27     OSPF     2      44
10.212.63.0/24      10.212.61.27     OSPF     2      43
10.212.66.0/24      10.212.66.17     LOCAL    1      46
143.209.92.0/24     172.28.6.254     STATIC   1      N/A
172.28.6.0/24       172.28.6.2       LOCAL    1      6
172.28.6.0/24       10.212.60.27     OSPF     1      44
172.28.6.0/24       10.212.61.27     OSPF     1      43
172.28.6.0/24       10.212.66.18     OSPF     1      46

Inactive Static Routes

Destination       Gateway        Metric
-----------------+--------------+------
1.0.0.0/8          8.4.5.3         1

-> show ip router database protocol ospf dest 10.212.62.0 255.255.255.0

Destination         Gateway          Protocol Metric VLAN
------------------+----------------+--------+------+-----
10.212.62.0/24      10.212.60.27     OSPF     2      44
10.212.62.0/24      10.212.61.27     OSPF     2      43

Inactive Static Routes

Destination       Gateway        Metric
-----------------+--------------+------
1.0.0.0/8          8.4.5.3         1
```

output definitions

Destination	Destination IP address. Also includes the mask prefix length notation after the address to indicate the subnet mask value. For example, **/24** indicates the destination IP address has a 24-bit mask (255.255.255.0).
Gateway	IP address of the gateway from which this route was learned.
Protocol	Protocol by which this IP address was learned: LOCAL, STATIC, OSPF, RIP, BGP).
Metric	RIP metric or cost (hop-count) for the route. Indicates a priority for the route. The lower the metric value, the higher the priority.
VLAN	The VLAN on which the route was *learned*, not forwarded. Note that **N/A** appears in this field for static routes as they are not learned on a VLAN.

Release History

Release 5.1; command was introduced.

Related Commands

show ip route	Displays the IP Forwarding table.

show ip emp-route

Displays the IP routes associated with the Ethernet Management Port (EMP).

show ip emp-route

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- This command displays the routes that are connected to the Ethernet Management Port (EMP).
- The EMP cannot handle routing protocols such as RIP or OSPF.
- The default route for the switch cannot be set up on the EMP.

Examples

```
-> show ip route

Dest Address      Subnet Mask       Gateway Addr      Age       Protocol
------------------+-----------------+-----------------+---------+-----------
  127.0.0.1         255.255.255.255   127.0.0.1           2d 4h  LOCAL
  172.17.1.10       255.255.255.255   10.255.11.225       1d 5h  LOCAL
```

output definitions

Dest Addr	Destination IP address.
Subnet Mask	Destination IP address IP subnet mask.
Gateway Addr	IP address of the gateway from which this address was learned.
Age	Age of the entry. If the entry is less than a day old, it is displayed in *hh/mm/ss* format. If it is more than a day old, it is displayed in *dd/hh* format (e.g., a route that is 2 days and 12 hours old is displayed as 2d12h).
Protocol	Protocol by which this IP address was learned (e.g., RIP). NETMGT indicates a static route. LOCAL indicates a local interface.

Release History

Release 5.1; command was introduced.

Related Commands

ping	Used to test whether an IP destination can be reached from the local switch.
traceroute	Used to find the path taken by an IP packet from the local switch to a specified destination.

show ip config

Displays IP configuration parameters.

show ip config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show ip config

IP directed-broadcast   =   OFF,
IP default TTL          =   64
```

output definitions

IP directed-broadcast	Indicates whether the IP directed-broadcast feature is on or off.
IP default TTL	IP default TTL interval.

Release History

Release 5.1; command was introduced.

Related Commands

ip directed-broadcast	Enables or disables IP directed broadcasts routed through the switch.
ip default-ttl	Sets TTL value for IP packets.

show ip protocols

Displays switch routing protocol information and status.

show ip protocols

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This command also displays the switch's primary IP address and router ID, if configured, and debug information.

Examples

```
-> show ip protocols
Router ID                           = 10.255.11.243,
Primary addr                        = 10.255.11.243,

RIP status                          = Not Loaded,
OSPF status                         = Not Loaded,
BGP status                          = Not Loaded,
DVMRP status                        = Not Loaded,
PIMSM status                        = Not Loaded,

Debug level                         = 1,
Debug sections                      = error,
```

output definitions

Router ID	The set routing ID. The router ID is how the router is identified in IP.
Primary addr	The primary interface address the route uses.
RIP status	Whether RIP is loaded or not.
OSPF status	Whether OSPF is loaded or not.
BGP status	Whether BGP is loaded or not.
DVMRP status	Whether DVMRP is loaded or not.
PIMSM status	Whether PIMSM is loaded or not.
Debug level	What the current router debug level is.
Debug sections	What types of debugging information are being tracked.

Release History

Release 5.1; command was introduced.

Related Commands

ip router primary-address	Configures the router primary IP address.
ip router router-id	Configures the router ID for the router.

MIB Objects

```
alaIpRouteSumTable
   alaIpRouteProtocol
```

show ip service

Displays the current status of TCP/UDP service ports.

show ip service

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

The display output from this command also includes the service port number.

Examples

```
-> show ip service
Name                     Port    Status
-----------------------+-------+---------
ftp                        21   enabled
ssh                        22   disabled
telnet                     23   disabled
udp-relay                  67   disabled
http                       80   disabled
network-time              123   disabled
snmp                      161   disabled
avlan-telnet              259   disabled
avlan-http                260   disabled
avlan-secure-http         261   disabled
secure_http               443   enabled
proprietary              1024   disabled
proprietary              1025   disabled
```

output definitions

Name	Name of the TCP/UDP service.
Port	The TCP/UDP well-known port number associated with the service.
Status	The status of the well-known service port: **enabled** (port is closed) or **disabled** (port is open).

Release History

Release 5.1; command was introduced.

Related Commands

ip service	Enables (opens) or disables (closes) well-known TCP/UDP service ports.

MIB Objects

```
alaIpServiceTable
   alaIpServiceType
   alaIpServicePort
   alaIpServiceStatus
alaIpPortServiceTable
   alaIpPortServicePort
   alaIpPortServiceStatus
```

show arp

Displays the ARP table. The ARP table contains a listing of IP addresses and their corresponding translations to physical MAC addresses.

show arp [*ip_address* **|** *hardware_address***]**

Syntax Definitions

ip_address	IP address of the entry you want to view.
hardware_address	MAC address of the entry you want to view.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the basic command (**show arp**) to view all of the entries in the table. Enter a specific IP address or MAC address to view a specific entry.

Examples

```
-> show arp

Total 8 arp entries
 Flags (P=Proxy, A=Authentication, V=VRRP)

 IP Addr           Hardware Addr       Type       Flags   Port     Interface
-----------------+------------------+----------+-------+--------+----------
 10.255.11.59      00:50:04:b2:c9:ee   DYNAMIC               3/20  vlan 1
 10.255.11.48      00:50:04:b2:ca:11   DYNAMIC               3/20  vlan 1
 10.255.11.201     00:10:83:03:e7:e4   DYNAMIC               3/20  vlan 1
 10.255.11.14      00:10:5a:04:19:a7   DYNAMIC               3/20  vlan 1
 10.255.11.64      00:b0:d0:62:fa:f1   DYNAMIC               3/20  vlan 1
 10.255.11.25      00:b0:d0:42:80:24   DYNAMIC               3/20  vlan 1
 10.255.11.26      00:b0:d0:42:82:59   DYNAMIC               3/20  vlan 1
 10.255.11.254     00:20:da:db:00:47   DYNAMIC               3/20  vlan 1
```

output definitions

IP Address	Device IP address.
Hardware Addr	MAC address of the device that corresponds to the IP address.
Type	Indicates whether the ARP cache entries are dynamic or static.
Flags	Indicates the type of entry: • P = Proxy • A = Authentication (AVLAN) • V = VRRP

output definitions (continued)

Port	The port on the switch attached to the device identified by the IP address.
Interface	The interface to which the entry belongs (e.g., VLAN, EMP).

Release History

Release 5.1; command was introduced.

Related Commands

ip service	Adds a permanent entry to the ARP table.
clear arp-cache	Deletes all dynamic entries from the ARP table.

MIB Objects

```
ipNetToMediaTable
   ipNetToMediaIfIndex
   ipNetToMediaNetAddress
   ipNetToMediaPhyAddress
   ipNetToMediaType
ipNetToMediaAugTable
   ipNetToMediaSlot
   ipNetToMediaPort
alaIpNetToMediaTable
   alaIpNetToMediaPhyAddress
   alaIpNetToMediaProxy
   alaIpNetToMediaVRRP
   alaIpNetToMediaAuth
```

show arp filter

Displays a list of ARP filters configured for the switch.

show arp filter [*ip_address***]**

Syntax Definitions

ip_address	IP address of the filter entry you want to view.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If an IP address is not specified with this command, a list of all ARP filters is displayed.
- Enter a specific IP address to view the configuration for an individual filter.

Examples

```
-> show arp filter

 IP Addr           IP Mask             Vlan   Type       Mode
-----------------+------------------+------+----------+-------
171.11.1.1         255.255.255.255        0   target     block
172.0.0.0          255.0.0.0              0   target     block
198.0.0.0          255.0.0.0              0   sender     block
198.172.16.1       255.255.255.255      200   target     allow

-> show arp filter 198.172.16.1

 IP Addr           IP Mask             Vlan   Type       Mode
-----------------+------------------+------+----------+-------
198.0.0.0          255.0.0.0              0   sender     block
198.172.16.1       255.255.255.255      200   target     allow
```

output definitions

IP Addr	The ARP packet IP address to which the filter is applied.
IP Mask	The IP mask that specifies which part of the IP address to which the filter is applied.
Vlan	A VLAN ID. The filter is applied only to ARP packets received on ports associated with this VLAN.
Type	Indicates which IP address in the ARP packet (**sender** or **target**) is used to identify if a filter exists for that address.
Mode	Indicates whether or not to **block** or **allow** a switch response to an ARP packet that matches the filter.

Release History

Release 5.1.6; command was introduced.

Related Commands

arp filter	Adds a permanent entry to the ARP table.
clear arp filter	Deletes all dynamic entries from the ARP table.

MIB Objects

```
alaIpArpFilterTable
   alaIpArpFilterIpAddr
   alaIpArpFilterIpMask
   alaIpArpFilterVlan
   alaIpArpFilterMode
   alaIpArpFilterType
```

show icmp control

This command allows viewing of the ICMP control settings.

show icmp control

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use this command to view the status of the various ICMP messages. It is also useful to determine the type and code of the less common ICMP messages.

Examples

```
-> show icmp control

  Name                                Type   Code   Status    min-pkt-gap(us)
--------------------------------------+------+------+---------+-----------------
  echo reply                            0      0   enabled             0
  network unreachable                   3      0   enabled             0
  host unreachable                      3      1   enabled             0
  protocal unreachable                  3      2   enabled             0
  port unreachable                      3      3   enabled             0
  frag needed but DF bit set            3      4   enabled             0
  source route failed                   3      5   enabled             0
  destination network unknown           3      6   enabled             0
  destination host unknown              3      7   enabled             0
  source host isolated                  3      8   enabled             0
  dest network admin prohibited         3      9   enabled             0
  host admin prohibited by filter       3     10   enabled             0
  network unreachable for TOS           3     11   enabled             0
  host unreachable for TOS              3     12   enabled             0
  source quench                         4      0   enabled             0
  redirect for network                  5      0   enabled             0
  redirect for host                     5      1   enabled             0
  redirect for TOS and network          5      2   enabled             0
  redirect for TOS and host             5      3   enabled             0
  echo request                          8      0   enabled             0
  router advertisement                  9      0   enabled             0
  router solicitation                  10      0   enabled             0
  time exceeded during transmit        11      0   enabled             0
  time exceeded during reassembly      11      1   enabled             0
  ip header bad                        12      0   enabled             0
  required option missing              12      1   enabled             0
```

```
timestamp request                  13      0   enabled           0
timestamp reply                    14      0   enabled           0
information request(obsolete)      15      0   enabled           0
information reply(obsolete)        16      0   enabled           0
address mask request               17      0   enabled           0
address mask reply                 18      0   enabled           0
```

output definitions

Name	The name of the ICMP message.
Type	The ICMP message type. This along with the ICMP code specify the kind of ICMP message.
Code	The ICMP message code. This along with the ICMP type specify the kind of ICMP message.
Status	Whether this message is **Enabled** or **Disabled**.
min-pkt-gap	The minimum packet gap, in microseconds, for this ICMP message. The minimum packet gap is the amount of time that must pass between ICMP messages of like types.

Release History

Release 5.1; command was introduced.

Related Commands

icmp type	Enables or disables a specific type of ICMP message, and sets the minimum packet gap.
icmp unreachable	This command allows the enabling or disabling of ICMP messages pertaining to unreachable destinations, and sets the minimum packet gap.
icmp echo	This command allows the enabling or disabling of ICMP echo messages, and sets the minimum packet gap.
icmp timestamp	This command allows the enabling or disabling of ICMP timestamp messages, and sets the minimum packet gap.
icmp addr-mask	This command allows the enabling or disabling of ICMP address mask messages, and sets the minimum packet gap.
icmp messages	Enables or disables all ICMP messages.

show icmp statistics

Displays Internet Control Message Protocol (ICMP) statistics and errors. ICMP is a network layer protocol within the IP protocol suite that provides message packets to report errors and other IP packet processing information back to the source. ICMP generates several kinds of useful messages, including Destination Unreachable, Echo Request and Reply, Redirect, Time Exceeded, and Router Advertisement and Solicitation. If an ICMP message cannot be delivered, no second one is generated. This is to avoid an endless flood of ICMP messages.

show icmp [statistics]

Syntax Definitions

statistics	Optional syntax.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

The ICMP table can be used to monitor and troubleshoot the switch.

Examples

```
-> show icmp

Messages                 Received    Sent
-------------------------+-----------+------------
  Total                       2105        2105
  Error                          0           0
  Destination unreachable        0           0
  Time exceeded                  0           0
  Parameter problem              0           0
  Source quench                  0           0
  Redirect                       0           0
  Echo request                2105           0
  Echo reply                     0        2105
  Time stamp request             0           0
  Time stamp reply               0           0
  Address mask request           0           0
  Address mask reply             0           0
```

output definitions

Total	Total number of ICMP messages the switch received or attempted to send. This counter includes all those counted as errors.
Error	Number of ICMP messages the switch sent/received but was unable to process because of ICMP-specific errors (e.g., bad ICMP checksums, bad length).
Destination unreachable	Number of “destination unreachable” messages that were sent/received by the switch.
Time exceeded	Number of “time exceeded” messages that were sent/received by the switch. These occur when a packet is dropped because the TTL counter reaches zero. When a large number of these occur, it is a symptom that packets are looping, that congestion is severe, or that the TTL counter value is set too low. These messages also occur when all the fragments trying to be reassembled do not arrive before the reassembly timer expires.
Parameter problem	Number of messages sent/received which indicate that an illegal value has been detected in a header field. These messages can indicate a problem in the sending host’s IP software or possibly in the gateway’s software.
Source quench	Number of messages sent/received tell a host that it is sending too many packets. A host should attempt to reduce its transmissions upon receiving these messages.
Redirect	Number of ICMP redirect messages sent/received by the switch.
Echo request	Number of ICMP echo messages sent/received by the switch to see if a destination is active and unreachable.
Echo reply	Number of echo reply messages received by the switch.
Time stamp request	Number of time stamp request messages sent/received by the switch.
Time stamp reply	Number of time stamp reply messages sent/received by the switch.
Address mask request	Number of address mask request messages that were sent/received by the switch in an attempt to determine the subnet mask for the network.
Address mask reply	Number of address mask reply messages that were sent/received by the switch.

Release History

Release 5.1; command was introduced.

Related Commands

show udp statistics	Displays UDP errors and statistics.

show tcp statistics

Displays TCP statistics.

show tcp statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show tcp statistics

Total segments received =   235080,
Error segments received =        0,
Total segments sent     =   363218,
Segments retransmitted  =       38,
Reset segments sent     =       97,
Connections initiated   =    57185,
Connections accepted    =      412,
Connections established =        1,
Attempt fails           =    24393,
Established resets      =      221
```

output definitions

Total segments received	Total number of segments received, including those received in error. This count includes segments received on currently established connections.
Error segments received	Total number of segments received in error (e.g., bad TCP checksums).
Total segments sent	Total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
Segments retransmitted	Number of TCP segments transmitted containing one or more previously transmitted octets.
Reset segments sent	Number of TCP segments containing the reset flag.
Connections initiated	Number of connections attempted.
Connections accepted	Number of connections allowed.
Connections established	Number of successful connections.

output definitions (continued)

Attempt fails	Number of times attempted TCP connections have failed.
Established resets	Number of times TCP connections have been reset from the "Established" or "Close Wait" state to the “Closed” state.

Release History

Release 5.1; command was introduced.

Related Commands

show icmp statistics	Displays ICMP statistics and errors.
show tcp ports	Displays the TCP connection table.

show tcp ports

Displays the TCP connection table.

show tcp ports

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use this table to check the current available TCP connections.

Examples

```
-> show tcp ports

Local Address     Local Port   Remote Address    Remote Port    State
------------------+------------+-----------------+--------------+-------------
  0.0.0.0                  21   0.0.0.0                     0    LISTEN
  0.0.0.0                  23   0.0.0.0                     0    LISTEN
  0.0.0.0                  80   0.0.0.0                     0    LISTEN
  0.0.0.0                 260   0.0.0.0                     0    LISTEN
  0.0.0.0                 261   0.0.0.0                     0    LISTEN
  0.0.0.0                 443   0.0.0.0                     0    LISTEN
  0.0.0.0                6778   0.0.0.0                     0    LISTEN
  10.255.11.223            23   128.251.16.224           1867    ESTABLISHED
  10.255.11.223          2509   10.255.11.33              389    TIME-WAIT
  10.255.11.223          2510   10.255.11.25              389    TIME-WAIT
  10.255.11.223          2513   10.255.11.33              389    TIME-WAIT
  10.255.11.223          2514   10.255.11.25              389    TIME-WAIT
  10.255.11.223          2517   10.255.11.33              389    TIME-WAIT
  10.255.11.223          2518   10.255.11.25              389    TIME-WAIT
  10.255.11.223          2521   10.255.11.33              389    TIME-WAIT
  10.255.11.223          2522   10.255.11.25              389    TIME-WAIT
  10.255.11.223          2525   10.255.11.33              389    TIME-WAIT
  10.255.11.223          2526   10.255.11.25              389    TIME-WAIT
  10.255.11.223          2529   10.255.11.33              389    TIME-WAIT
  10.255.11.223          2530   10.255.11.25              389    TIME-WAIT
```

output definitions

Local Address	Local IP address for this TCP connection. If a connection is in the LISTEN state and will accept connections for any IP interface associated with the node, IP address 0.0.0.0 is used.
Local Port	Local port number for this TCP connection. The range is 0–65535.
Remote Address	Remote IP address for this TCP connection.
Remote Port	Remote port number for this TCP connection. The range is 0–65535.
State	State of the TCP connection, as defined in RFC 793. A connection progresses through a series of states during its lifetime: • Listen—Waiting for a connection request from any remote TCP and port. • Syn Sent—Waiting for a matching connection request after having sent a connection request. • Syn Received—Waiting for a confirming connection request acknowledgment after having both received and sent a connection request. • Established—Open connection. Data received can be delivered to the user. This is the normal state for the data transfer phase of the connection. • Fin Wait 1—Waiting for a connection termination request from the remote TCP, or an acknowledgment of the connection termination request previously sent. • Fin Wait 2—Waiting for a connection termination request from the remote TCP. • Close Wait—Waiting for a connection termination request from the local user. • Closing—Waiting for a connection termination request acknowledgment from the remote TCP. • Last Ack—Waiting for an acknowledgment of the connection termination request previously sent to the remote TCP (which includes an acknowledgment of its connection termination request). • Time Wait—Waiting for enough time to pass to be sure the remote TCP received the acknowledgment of its connection termination request. • Closed—No connection state.

Release History

Release 5.1; command was introduced.

Related Commands

show ip interface	Displays the status and configuration of IP interfaces.
show tcp statistics	Displays TCP statistics.

show udp statistics

Displays UDP errors and statistics.

show udp statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This command displays cumulative statistics since the last time the switch was powered on or since the last reset of the switch.

Examples

```
-> show udp statistics

Total datagrams received   =   214937,
Error datagrams received   =        0,
No port datagrams received =    32891,
Total datagrams sent       =   211884
```

output definitions

Total datagrams received	Total number of UDP datagrams delivered to UDP applications.
Error datagrams received	Number of UDP datagrams that could not be delivered for any reason.
No port datagrams received	Number of UDP datagrams that could not be delivered for reasons other than lack of application at the destination.
Total datagrams sent	Total number of UDP datagrams sent from this switch.

Release History

Release 5.1; command was introduced.

Related Commands

show udp ports	Displays the UDP Listener table.

show udp ports

Displays the UDP Listener table. The table shows the local IP addresses and the local port number for each UDP listener.

show udp ports

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- An IP address of zero (0.0.0.0) indicates that it is listening on all interfaces.
- This table contains information about the UDP end-points on which a local application is currently accepting datagrams.

Examples

```
-> show udp port

Local Address     Local Port
------------------+--------------
  0.0.0.0                  67
  0.0.0.0                 161
  0.0.0.0                 520
```

output definitions

Local Address	Local IP address for this UDP connection.
Local Port	Local port number for this UDP connection.

Release History

Release 5.1; command was introduced.

Related Commands

show udp statistics	Displays UDP errors and statistics.

show ip dos config

Displays the configuration parameters of the DoS scan for the switch.

show ip dos config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This command allows the user to view the configuration parameters of the DoS scan. The scan keeps a record of the penalties incurred by certain types of packets on TCP and UDP ports. When the set penalty threshold is reached, it is assumed that a DoS attack is in progress, and a trap is generated to inform the system administrator.

Examples

```
-> show ip dos config
DoS trap generation = ENABLED,
DoS port scan threshold = 1000,
DoS port scan decay = 2,
DoS port scan close port penalty = 10,
DoS port scan TCP open port penalty = 0,
DoS port scan UDP open port penalty = 0
```

output definitions

DoS trap generation	Displays the status of DoS trap generation. It is either **ENABLED** or **DISABLED**. This is set using the **ip dos trap** command.
DoS port scan threshold	The penalty threshold setting. When enough packets have increased the penalty number to this setting, a trap is generated to warn the administrator that a DoS attack is in progress. This is set using the **ip dos scan threshold** command.
DoS port scan decay	The decay value for the switch. The penalty value of the switch is decreased by this number every minute. This is set using the **ip dos scan decay** command.
DoS port scan close port penalty	The penalty value for packets received on closed UDP and TCP ports. The penalty number for the switch is increased by this amount every time a packet is received on a closed UDP or TCP port. This is set using the **ip dos scan close-port-penalty** command.

output definitions (continued)

DoS port scan TCP open port penalty	The penalty value for packets received on open TCP ports. The penalty number for the switch is increased by this amount every time a packet is received on an open TCP port. This is set using the **ip dos scan tcp open-port-penalty** command.
DoS port scan UDP open port penalty	The penalty value for packets received on open UDP ports. The penalty number for the switch is increased by this amount every time a packet is received on an open UDP port. This is set using the **ip dos scan udp open-port-penalty** command.

Release History

Release 5.1; command was introduced.

Related Commands

show ip dos statistics	Displays the statistics on detected DoS attacks for the switch.

show ip dos statistics

Displays the statistics on detected DoS attacks for the switch.

show ip dos statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command displays the number of attacks the switch has detected for several types of DoS attacks.
- Just because an attack is detected and reported doesn't necessarily mean an attack occurred. The switch assumes that a DoS attack is underway anytime the penalty threshold is exceeded. It is possible for this threshold to be exceeded when no attack is in progress.

Examples

```
-> show ip dos statistics
DoS type             Attacks detected
---------------------+--------------------
port scan            46
tcp sync flood       0
ping of death        1
smurf                0
pepsi                0
land                 1
teardrop/bonk/boink  1
```

output definitions

DoS type	The type of DoS attack. The most common seven are displayed.
Attacks detected	The number of attacks noted for each DoS type.

Release History

Release 5.1; command was introduced.

Related Commands

show ip dos config	Displays the configuration parameters of the DoS scan for the switch.

debug ip packet

Enables/disables/configures the IP packet debug feature. This command is generally used only when working with a field engineer to debug a problem on the switch.

debug ip packet [start] [timeout *seconds***] [stop] [direction {in | out | all}] [format {header | text | all}] [output {console | file** *filename***}] [board {cmm | ni [1-16] | all | none} [ether-type {arp | ip | hex** [*hex_number*] **| all}] [ip-address** *ip_address***] [ip-address** *ip_address***] [ip-pair** [*ip1*] [*ip2*]**] [protocol {tcp | udp | icmp | igmp | num** [*integer*] **| all}] [show-broadcast {on | off}] show-multicast {on | off}]**

Syntax Definitions

start	Starts an IP packet debug session.
timeout	Sets the duration of the debug session, in seconds. To specify a duration for the debug session, enter **timeout**, and then enter the session length.
seconds	The debug session length, in seconds.
stop	Stops IP packet debug session.
direction	Specifies the type of the packets you want to debug. Specify **in** to debug incoming packets; specify **out** to debug outgoing packets; specify **all** to debug both incoming and outgoing packets.
format	Specifies the area of the packet you want to debug. Specify **header** to debug the packets header; specify **hex** to debug the packet text; specify **all** to debug the entire packet.
output	Specifies where you want the debug information to go. Specify **console** to print the output to the screen; specify **file** to save the output to a log file.
filename	The filename for the output file.
board	Specifies the slot (board) that you want to debug. Specify **cmm** to debug CMM packets; specify **ni**, then enter the slot number of the NI to debug a network interface card; specify **all** to debug packets for all CMMs and NIs on the switch; specify **none** to clear the previous board settings.
ether-type	Specifies a specific Ethernet packet type to debug. Specify **arp** to debug ARP packets; specify **ip** to debug IP packets; specify **hex** and enter an ethernet packet type in hex format (e.g., 800) to debug a specific ethernet packet type; specify **all** to debug all Ethernet packet types.
ip-address	Specifies an IP address to debug. The debug output will only be for packets received from this IP address. Enter **ip-address,** then enter the IP address that you want to debug.
ip-pair	Use this option to match packets exchanged between two network addresses. Enter **ip-pair**, then enter each IP address.

protocol	Specifies a protocol type to debug. Specify **tcp** to debug TCP packets; specify **udp** to debug UPD packets; specify **icmp** to debug ICMP packets; specify **igmp** to debug IGMP packets; specify **num** to numerically specify a protocol (e.g., 89); specify **all** to debug all protocol types.
show-broadcast	Specifies whether or not to display broadcast packets. Specify **on** to display broadcast packets on the screen or in the log; specify **off** if you do not want to display broadcast packets.
show-multicast	Specifies whether or not to display multicast packets. Specify **on** to display multicast packets on the screen or in the log; specify **off** if you do not want to display multicast packets.

Defaults

parameter	default
timeout	-1
in | out | all	**all**
header | text | all	**header**
console | file	**console**
cmm | ni | all | none	**all**
arp | ip | hex | all	**all**
tcp | udp | icmp | igmp | num | all	**all**
on | off	**on**
on | off	**on**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If you use the basic command to start debug (**debug ip packet start**), the switch will use default parameters for all of the debug options. Once you configure one of the optional parameters, the switch will use the new parameter(s) until changed.
- If you do not specify a timeout value, the session will continue until it is stopped.
- You must enter the **start** keyword to begin debugging.
- The command **debug ip packet** without the **start** keyword displays IP debug configuration parameters.

Examples

```
-> debug ip packet start timeout 1
```

Release History

Release 5.1; command was introduced.

Related Commands

debug ip level	Configures IP debug level. This command allows you to set the level (amount) of information displayed.

MIB Objects

N/A

debug ip level

Configures the IP debug level. This command allows you to set the level (amount) of information displayed. The lower the level, the more significant the event. For example, a level of 1 will display only the most critical problems. A level of 99 would display all of the available information for the specified debug type. It is best to use the default level of 1 unless instructed to increase the level by a field engineer. If more information is needed to debug a problem, a higher level can be selected.

debug ip level *level*

Syntax Definitions

level	Debug level. Valid range is 0–255.

Defaults

parameter	default
level	1

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

The debug level applies to the debug configuration set with the **debug ip packet** command. You cannot set different levels for different configurations.

Examples

```
-> debug ip level 1
```

Release History

Release 5.1; command was introduced.

Related Commands

debug ip packet	Enables/disables/configures the IP packet debug feature.

MIB Objects

N/A

debug ip packet default

Returns IP packet debug options to default values.

debug ip packet default

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

See "Defaults" on page 23-86 for default values.

Examples

```
-> debug ip packet default
```

Release History

Release 5.1; command was introduced.

Related Commands

debug ip packet	Configures IP packet debug.

MIB Objects

N/A

debug ip packet

Displays IP debug configuration parameters. This command is generally used only when working with a field engineer to debug a problem on the switch.

debug ip packet

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This command is used to display IP debug configuration parameters. To start IP debugging you must enter the **start** keyword.

Examples

```
-> debug ip packet

packet dump                                              off,
timeout in seconds                                         0,
output device                                        console,
board                                                    all,
ether-type                                               all,
protocol                                                 all,
direction                                          in + out,
mcast/bcast                                              on,
format                                                header,
IP address filter
```

output definitions

packet dump	IP debug administrative status (on/off).
timeout in seconds	Duration of the debug session, in seconds. (0 = off).
output device	Output device for debug information (e.g., file, console).
ether-type	Ethernet packet type to debug (e.g., ARP, IP).
protocol	Protocol type to debug (e.g., TCP, UDP).
direction	Type of traffic to debug incoming (in) or outgoing (out).
mcast/bcast	Specifies whether or not to show broadcast/multicast packets.
format	Area of the packet to debug (e.g., header, text).
ip address filter	Interface to debug.

Release History

Release 5.1; command was introduced.

Related Commands

debug ip packet	Configures IP packet debug.

MIB Objects

N/A

24 IPv6 Commands

This chapter details Internet Protocol Version 6 (IPv6) commands for the switch (including RIPng commands). IPv6 (documented in RFC 2460) is designed as a successor to IPv 4. The changes from IPv4 to IPv6 fall primarily into the following categories:

Expanded Routing and Addressing Capabilities - IPv6 increases the IP address size from 32 bits to 128 bits, to support more levels of addressing hierarchy and a much greater number of addressable nodes, and simpler auto-configuration of addresses. The scalability of multicast routing is improved by adding a "scope" field to multicast addresses.

Header Format Simplification - Some IPv4 header fields were dropped or made optional, to reduce the common-case processing cost of packet handling and to keep the bandwidth cost of the IPv6 header as low as possible despite the increased size of the addresses. Even though the IPv6 addresses are four times longer than the IPv4 addresses, the IPv6 header is only twice the size of the IPv4 header.

Anycast Addressing - A new type of address called a "anycast address" is defined, to identify sets of nodes where a packet sent to an anycast address is delivered to one of the nodes. The use of anycast addresses in the IPv6 source route allows nodes to control the path which their traffic flows.

Improved Support for Options - Changes in the way IP header options are encoded allows for more efficient forwarding, less stringent limits on the length of options, and greater flexibility for introducing new options in the future.

Authentication and Privacy Capabilities - IPv6 includes the definition of extensions which provide support for authentication, data integrity, and confidentiality. This is included as a basic element of IPv6 and will be included in all implementations.

IPv6 is supported on 6600/7700/7800/8800 series switches running software Release 5.1.6 and up.

Note. On OmniSwitch 6600/7700/7800/8800 series switches, IPv6 is a software based implementation.

MIB information for the IPv6 and RIPng commands is as follows:

Filename: Ipv6.mib
Module: Ipv6-MIB, Ipv6-TCP-MIB, Ipv6-UDP-MIB

Filename: AlcatelIND1Ipv6.mib
Module: alcatelIND1IPv6MIB

Filename: AlcatelIND1Ripng.mib
Module: alcatelIND1RipngMIB

A summary of the IPv6 commands is listed here:

IPv6	**ipv6 interface** **ipv6 address** **ipv6 hop-limit** **ipv6 interface tunnel source destination** **ipv6 hop-limit** **ipv6 pmtu-lifetime** **ipv6 host** **ipv6 neighbor** **ipv6 prefix** **ipv6 route** **ping6** **traceroute6** **debug ipv6 packet** **debug ipv6 trace-category** **show ipv6 hosts** **show ipv6 icmp statistics** **show ipv6 interface** **show ipv6 pmtu table** **clear ipv6 pmtu table** **clear ipv6 neighbors** **show ipv6 prefixes** **show ipv6 routes** **show ipv6 tcp ports** **show ipv6 traffic** **clear ipv6 traffic** **show ipv6 tunnel** **show ipv6 udp ports**
IPv6 RIP	**ipv6 load rip** **ipv6 rip status** **ipv6 rip invalid-timer** **ipv6 rip garbage-timer** **ipv6 rip holddown-timer** **ipv6 rip jitter** **ipv6 rip route-tag** **ipv6 rip update-interval** **ipv6 rip triggered-sends** **ipv6 rip interface metric** **ipv6 rip interface recv-status** **ipv6 rip interface send-status** **ipv6 rip interface horizon** **ipv6 rip debug-level** **ipv6 rip debug-type** **show ipv6 rip** **show ipv6 rip interface** **show ipv6 rip peer** **show ipv6 rip routes** **show ipv6 rip debug**

ipv6 interface

Configures an IPv6 interface on a VLAN or IPv6 tunnel.

ipv6 interface *if_name* **[vlan** *vid* **| tunnel {***tid* **| 6to4}] [enable | disable]**
[mtu *size***]**
[ra-send {yes | no}]
[ra-max-interval *interval***]**
[ra-managed-config-flag {true | false}]
[ra-other-config-flag {true | false}]
[ra-reachable-time *time***]**
[ra-retrans-timer *time***]**
[ra-default-lifetime *time* **| no ra-default-lifetime]**
[ra-send-mtu] {yes | no}

no ipv6 interface *if_name*

Syntax Definitions

if_name	IPv6 interface name.
vlan	Creates a VLAN interface.
vid	VLAN ID number.
tunnel	Creates a tunnel interface.
tid	Tunnel ID number.
6to4	Enables 6to4 tunneling.
mtu *size*	Maximum Transmission Unit for the interface.
ra-send	Specifies whether the router advertisements are sent on this interface.
ra-max-interval *interval*	Maximum time, in seconds, allowed between the transmission of unsolicited multicast router advertisements in this interface. The range is 4 - 1,800.
ra-managed-config-flag	Value to be placed in the managed address configuration flag field in router advertisements sent on this interface.
ra-other-config-flag	Value to be placed in the other stateful configuration flag in router advertisements sent on this interface.
ra-reachable-time *time*	Value, in milliseconds, to be placed in the reachable time field in router advertisements sent on this interface. The range is 0 - 3,600,000). The special value of zero indicates that this time is unspecified by the router.
ra-retrans-timer *time*	Value, in milliseconds, to be placed in the retransmit timer field in router advertisements sent on this interface. The value zero indicates that the time is unspecified by the router.

ra-default-lifetime *time*	Value, in seconds, to be placed in the router lifetime field in router advertisements sent on this interface. The time must be zero or between the value of "ra-max-interval" and 9,000 seconds. A value of zero indicates that the router is not to be used as a default router. The "no ra-default-lifetime" option will calculate the value using the formula (3 * ra-max-interval).
enable | disable	Administratively enable or disable the interface.
ra-send-mtu	Specifies whether the MTU option is included in the router advertisements sent on the interface.

Defaults

parameter	default
ra-send	yes
ra-max-interval	600
ra-managed-config-flag	false
ra-reachable-time	0
ra-retrans-timer	0
ra-default-lifetime	no
ra-send-mtu	no

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- When you create an IPv6 interface it is enabled by default.
- Use the "no" form of the command to delete an interface.
- All IPv6 VLAN and tunnel interfaces must have a name.
- When creating an IPv6 interface you must specify a VLAN ID, Tunnel ID, or **6to4**. When modifying or deleting an interface, you do not need to specify one of these options unless the name assigned to the interface is being changed. If it is present with a different value from when the interface was created, the command will be in error.
- A 6to4 interface cannot send advertisements (**ra-send**).
- To enable IPv6 routing you must first create a VLAN, then create an IPv6 interface on the VLAN. See Chapter 21, "VLAN Management Commands," for information on creating VLANs.
- To route IPv6 traffic over an IPv4 network, you must create an IPv6 tunnel using the **ipv6 interface tunnel source destination** command.

Example

```
-> ipv6 interface Test vlan 1
-> ipv6 interface Test_Tunnel tunnel 2
-> ipv6 interface Test_6to4 tunnel 6to4
```

Release History

Release 5.1.6; command was introduced.

Related Commands

show ipv6 interface	Displays IPv6 Interface Table
show ipv6 tunnel	Displays IPv6 Tunnel information and whether the 6to4 tunnel is enabled.

MIB Objects

```
IPv6IfIndex
alaIPv6InterfaceTable
   alaIPv6InterfaceName
   alaIPv6InterfaceMtu
   alaIPv6InterfaceSendRouterAdvertisements
   alaIPv6InterfaceMaxRtrAdvInterval
   alaIPv6InterfaceAdvManagedFlag
   alaIPv6InterfaceAdvOtherConfigFlag
   alaIPv6InterfaceAdvRetransTimer
   alaIPv6InterfaceAdvDefaultLifetime
   alaIPv6InterfaceAdminStatus
   alaIPv6InterfaceAdvReachableTime
   alaIPv6InterfaceAdvSendMtu
   alaIPv6InterfaceRowStatus
```

ipv6 address

Configures an IPv6 address for an IPV6 interface on a VLAN, configured tunnel, or a 6to4 tunnel. There are different formats for this command depending on the address type.

ipv6 address *ipv6_address /prefix_length* **[anycast]** {*if_name* | **loopback**}

no ipv6 address *ipv6_address /prefix_length* **[anycast]** {*if_name* | **loopback**}

ipv6 address *ipv6_prefix/prefix_length* **eui-64** {*if_name* | **loopback**}

no ipv6 address *ipv6_prefix/prefix_length* **eui-64** {*if_name* | **loopback**}

Syntax Definitions

ipv6_address	IPv6 address.
/prefix_length	The number of bits that are significant in the IPv6 address (mask). (0...128).
anycast	Indicates the address is an anycast address.
eui-64	Append an EUI-64 identifier to the prefix.
if_name	Name assigned to the interface.
loopback	Configures the loopback interface.

Defaults

parameter	default
/prefix_length	0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- You can assign multiple IPv6 addresses to an IPv6 interface.
- Use the “no” form of the command to delete an address.
- The “eui” form of the command is used to add or remove an IPv6 address for a VLAN or configured tunnel using an EUI-64 interface ID in the low order 64 bits of the address.
- To enable IPv6 routing you must first create a VLAN, then create an IPv6 interface on the VLAN. See Chapter 21, “VLAN Management Commands,” for information on creating VLANs.
- To route IPv6 traffic over and IPv4 network, you must create an IPv6 tunnel using the **ipv6 interface tunnel source destination** command.

Example

```
-> ipv6 address 4132:86::19A/64 Test_Lab
-> ipv6 address 2002:d423:2323::35/64 Test_6to4
```

Release History

Release 5.1.6; command was introduced.

Related Commands

show ipv6 interface	Displays IPv6 Interface Table.

MIB Objects

```
IPv6IfIndex
alaIPv6InterfaceAddressTable
   alaIPv6InterfaceAddress
   alaIPv6InterfaceAddressAnycastFlag
   alaIPv6InterfaceEUI64AddressPrefixLength
   alaIPv6InterfaceEUI64AddressrowStatus

For EUI-64 Addresses:
alaIPv6InterfaceEUI64AddresssTable
   alaIPv6InterfaceEUI64Address
   alaIPv6InterfaceEUI64AddressPrefixLength
   alaIPv6InterfaceEUI64AddressRowStatus
```

ipv6 interface tunnel source destination

Configures the source and destination IPv4 addresses for a configured tunnel.

ipv6 interface *if_name* **tunnel {[source** *ipv4_source***] [destination** *ipv4_destination***]}**

Syntax Definitions

if_name	Name assigned to the tunnel interface.
ipv4_source	Source IPv4 address for the configured tunnel.
ipv4_destination	Destination IPv4 address for the configured tunnel.

Defaults

N/A.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **ipv6 interface** command to create an IPv6 tunnel interface.

Example

```
-> ipv6 interface Test tunnel 2 source 10.255.11.242 destination 10.255.11.242
```

Release History

Release 5.1.6; command was introduced.

Related Commands

ipv6 interface	Creates an IPv6 tunnel interface.
show ipv6 tunnel	Displays IPv6 Tunnel information.

MIB Objects

```
IPv6IfIndex
   alaIPv6ConfigTunnelv4Source
   alaIPv6ConfigTunnelv4Dest
   alaIPv6ConfigTunnelRowStatus
```

ipv6 dad-check

Runs a Duplicate Address Detection (DAD) check on an address that was marked as duplicated.

ipv6 dad-check *ipv6_address if_name*

Syntax Definitions

ipv6_address	IPv6 address.
ip_name	Name assigned to the interface.

Defaults

N/A.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

The switch performs DAD check when an interface is attached to the stack and its VLAN first enters the active state. Use this command to rerun a DAD check on an address that was marked as duplicated.

Example

```
-> ipv6 dad-check fe80::2d0:95ff:fe6a:f458/64 Test_Lab
```

Release History

Release 5.1.6; command was introduced.

Related Commands

N/A.

MIB Objects

```
alaIPv6InterfaceAddressTable
   alaIPv6InterfaceAddressDADStatus
```

ipv6 hop-limit

Configures the value placed in the hop limit field in the header of all IPv6 packets that are originated by the switch. It also configures the value placed in the hop limit field in router advertisements.

ipv6 hop-limit *value*

no ipv6 hop-limit

Syntax Definitions

value	Hop limit value. The range is 0 - 255.

Defaults

parameter	default
value	64

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the “no” form of the command to return the hop limit to its default value.

Example

```
-> ipv6 hop-limit 64
```

Release History

Release 5.1.6; command was introduced.

Related Commands

N/A.

MIB Objects

```
ipv6MibObjects
   Ipv6DefaultHopLimit
```

ipv6 pmtu-lifetime

Configures the minimum lifetime for entries in the path MTU Table.

ipv6 pmtu-lifetime *time*

Syntax Definitions

time	Minimum path MTU entry lifetime, in minutes. Valid range is 10–1440.

Defaults

parameter	default
time	60

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A.

Example

```
-> ipv6 pmtu-lifetime 30
```

Release History

Release 5.1.6; command was introduced.

Related Commands

show ipv6 pmtu table	Displays the IPv6 path MTU Table.
clear ipv6 pmtu table	Removes all entries from the IPv6 path MTU Table.

MIB Objects

```
alaIPv6ConfigTable
   alaIPv6PMTUMinLifetime
```

ipv6 host

Configures a static host name to IPv6 address mapping to the local host table.

ipv6 host *name ipv6_address*

no ipv6 host *name ipv6_address*

Syntax Definitions

name	Host name associated with the IPv6 address (1 - 255 characters).
ipv6_address	IPv6 address.

Defaults

N/A.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the “no” form of the command to remove the mapping from the host table.

Example

```
-> ipv6 host Lab 4235::1200:0010
```

Release History

Release 5.1.6; command was introduced.

Related Commands

show ipv6 hosts	Displays IPv6 Local Hosts Table.

MIB Objects

```
alaIPv6HostTable
   alaIPv6HostName
   alaIPv6HostAddress
   alaIPv6HostRowStatus
```

ipv6 neighbor

Configures a static entry in the IPv6 Neighbor Table.

ipv6 neighbor *ipv6_address hardware_address* {*if_name*} *slot/port*

no ipv6 neighbor *ipv6_address* {*if_name*}

Syntax Definitions

ipv6_address	IPv6 address that corresponds to the hardware address.
hardware_address	MAC address in hex format (e.g., 00:00:39:59:F1:0C).
if_name	Name assigned to the interface on which the neighbor resides.
slot/port	Slot/port used to reach the neighbor.

Defaults

N/A.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the “no” form of the command to remove an entry from the IPv6 Neighbor Table.

Example

```
-> ipv6 neighbor 4132:86::203 00:d0:c0:86:12:07 Test 1/1
```

Release History

Release 5.1.6; command was introduced.

Related Commands

show ipv6 neighbors	Displays IPv6 Neighbor Table.

MIB Objects

```
IPv6IfIndex
alaIPv6NeighborTable
   alaIPv6NeighborNetAddress
   alaIPv6NeighborPhysAddress
   alaIPv6NeighborSlot
   alaIPv6NeighborPort
   alaIPv6NeighborRowStatus
```

ipv6 prefix

Configures an IPv6 prefix on an interface. Used for configuring prefixes for router advertisements.

ipv6 prefix *ipv6_address /prefix_length if_name*
[valid-lifetime *time***]**
[preferred-lifetime *time***]**
[on-link-flag {true | false}
[autonomous-flag {true | false}] *if_name*

no ipv6 prefix *ipv6_address /prefix_length if_name*

Syntax Definitions

ipv6_address	IPv6 address of the interface.
/prefix_length	The number of bits that are significant in the iPv6 address (mask). (0...128).
valid-lifetime *time*	Length of time, in seconds, that this prefix will remain valid, i.e. time until deprecation. A value of 4,294,967,295 represents infinity.
preferred-lifetime *time*	Length of time, in seconds, that this prefix will remain preferred, i.e. time until deprecation. A value of 4,294,967,295 represents infinity.
on-link-flag	On-link configuration flag. When “true.” this prefix can be used for on-link determination.
autonomous-flag	Autonomous address configuration flag. When “true,” indicates that this prefix can be used for autonomous address configuration (i.e., can be used to form a local interface address).
if_name	Name assigned to the interface.

Defaults

parameter	default
valid-lifetime *time*	2,592,000
preferred-lifetime *time*	604,800
on-link-flag	true
autonomous-flag	true

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the “no” form of the command to delete a prefix.

Example

```
-> ipv6 prefix 4132:86::/64 Test
```

Release History

Release 5.1.6; command was introduced.

Related Commands

show ipv6 prefixes	Displays IPv6 prefixes used in router advertisements.

MIB Objects

```
IPv6IfIndex
alaIPv6InterfacePrefixTable
   alaIP6vInterfacePrefix
   alaIP6vInterfacePrefixLength
   alaIP6vInterfacePrefixValidLifetime
   alaIP6vInterfacePrefixPreferredLifetime
   alaIP6vInterfacePrefixonLinkFlag
   alaIP6vInterfacePrefixAutonomousFlag
   alaIP6vInterfacePrefixRowStatus
```

ipv6 route

Configures a static entry in the IPv6 route.

ipv6 route *ipv6_prefix/prefix_length ipv6_address* [*if_name*]

no ipv6 route *ipv6_prefix/prefix_length ipv6_address* [*if_name*]

Syntax Definitions

ipv6_prefix	IPv6 network that is the destination of this static route.
/prefix_length	The number of bits that are significant in the iPv6 address (mask). (0...128).
ipv6_address	IPv6 address of the next hop used to reach the specified network.
if_name	If the next hop is a link-local address, the name of the interface used to reach it.

Defaults

N/A.

Platforms Supported

OmniSwitch 6600, 7700, 7800

Usage Guidelines

Use the “no” form of the command to remove a static route.

Example

```
-> ipv6 route 212:95:5::/64 fe80::2d0:95ff:fe6a:f458 v6if-137
```

Release History

Release 5.1.6; command was introduced.

Related Commands

show ipv6 routes	Displays IPv6 Forwarding Table.

MIB Objects

```
alaIPv6StaticRouteTable
   alaIPv6StaticRouteNextHop
   alaIPv6StaticRouteIfIndex
   alaIPv6StaticRouteDest
   alaIPv6StaticRoutePrefixLength
   alaIPv6StaticRouteRowStatus
```

ping6

Used to test whether an IPv6 destination can be reached from the local switch. This command sends an ICMPv6 echo request to a destination and then waits for a reply. To ping a destination, enter the **ping6** command and enter either the destination's IPv6 address or hostname. The switch will ping the destination using the default frame count, packet size, and interval (6 frames, 64 bytes, and 1 second respectively). You can also customize any or all of these parameters as described below.

ping6 {*ipv6_address* | *hostname***}** [*if_name*] **[count** *count***] [size** *data_size***] [interval** *seconds***]**

Syntax Definitions

ipv6_address	IP address of the system to ping.
hostname	DNS name of the system to ping.
if_name	If the target is a link-local address, the name of the interface used to reach it.
count	Number of packets to be transmitted.
size	Size of the data portion of the packet sent for this ping, in bytes.
seconds	Interval, in seconds, at which ping packets are transmitted.

Defaults

parameter	default
count	6
size	56
interval *seconds*	1

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If you change the default values they will only apply to the current ping. The next time you use the ping command, the default values will be used unless you again enter different values.
- When the next hop address is a local link address, the name of the interface used to reach the destination must be specified.

Example

```
-> ping6 fe80::2d0:95ff:fe6a:f458/64
```

Release History

Release 5.1.6; command was introduced.

Related Commands

traceroute6	Used to find the path taken by an IPv6 packet from the local switch to a specified destination.

traceroute6

Used to find the path taken by an IPv6 packet from the local switch to a specified destination. This command displays the individual hops to the destination as well as some timing information.

traceroute6 {*ipv6_address* | *hostname*} [*if_name*] **[max-hop** *hop_count***] [wait-time** *time***] [port** *port_number***] [probe-count** *probe***]**

Syntax Definitions

ipv6_address	Destination IPV6 address IPv6 address of the host whose route you want to trace.
hostname	DNS name of the host whose route you want to trace.
if_name	If the target is a link-local address, the name of the interface used to reach it.
hop_count	Maximum hop count for the trace.
time	Delay time, in seconds between probes
port	Specific UDP port destination. By default, the destination port is chosen by traceroute6.
probe	Number of probes to be sent to a single hop.

Defaults

parameter	default
hop_count	30
time	5
probe	3

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- When using this command, you must enter the name of the destination as part of the command line (either the IPv6 address or hostname).
- Use the optional **max-hop** parameter to set a maximum hop count to the destination. If the trace reaches this maximum hop count without reaching the destination, the trace stops.

Example

```
-> traceroute6 41EA:103::65C3
```

Release History

Release 5.1.6; command was introduced.

Related Commands

ping6	Used to test whether an IPv6 destination can be reached from the local switch.

debug ipv6 packet

Configures the display of IPv6 debug messages.

debug ipv6 packet
[defaults]
[v6header {concise | verbose}]
[extheader {none | payload | concise | verbose}]
[etherheader {yes | no}]
[raw *bytes***]**
[board {all | cmm | ni [*slot_number*] **| none}]**
[ether-filter *mac_address* **| either-filter-pair** *mac_address mac_address* | **no ether-filter]**
[ipv6-filter *ipv6_address* [*/prefix_length*] **| ipv6-filter-pair** *ipv6_address* [*/prefix_length*] | **no ipv6-filter]**
[direction {all | in | out | from-cmm | from-ipv4 | to-cmm | to-ipv4}]
[output {console | file *filename***}]**

no debug ipv6 packet

Syntax Definitions

defaults	Resets all settings to default values.
v6header	Sets the display format for the IPv6 header.
extheader	Sets the display format for IPv6 extension headers: **none** - No extension headers will be displayed **payload** - Information on the final payload header only **concise** - Concise information on all extension headers **verbose** - Verbose information on all extension headers.
etherheader	Specifies whether the packet's Ethernet header will be displayed.
raw *bytes*	If bytes is not zero, this number of raw hex bytes of the packet will be displayed.
board	Specifies the board(s) on which packet debug is enabled.
ether-filter	Allows filtering of packets based on their source and destination MAC addresses. If a single MAC address is specified, only packets whose source or destination MAC address match the specified value will be displayed. If a pair of MAC addresses is specified, only those packets being exchanged between the two MAC addresses will be displayed.
ipv6-filter	Allows filtering of packets based on their source and destination IPv6 addresses. If a single IPv6 address is specified, only packets sent to or received from that address will be displayed. If a pair of addresses is specified, only those packets being exchanged between the two addresses will be displayed.

direction	Allows filtering of packets based on the direction of flow: **all** - debug both incoming and outgoing packets **in** - debug incoming IPv6 packets **out** - debug outgoing packets **from-cmm** - debug packets received from the CMM. **from-ipv4** - debug packets received from an IPv4 interface. **to-cmm** - debug packets sent to the CMM. **to-ipv4** - debug packets sent to an IPv4 interface.
output	Specifies the destination for the debug information. **console** - write debug information to the console screen or file **file** *filename* - write debug information to the specified file.

Defaults

parameter	default
v6header	concise
extheader	payload
etherheader	yes
raw *bytes*	0
board	all
ether-filter	no ether-filter
ipv6-filter	no ipv6-filter
direction	all
output	console

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to turn off IPv6 debugging.
- Options are additive across multiple command lines until reset with the “default” option.

Example

```
-> debug ipv6 packet defaults
```

Release History

Release 5.1.6; command was introduced.

Related Commands

debug ipv6 trace-category	Enables/disables specific IPv6 EDR trace categories.

MIB Objects

N/A

debug ipv6 trace-category

Enables/disables specific IPv6 EDR trace categories. If a category is enabled (e.g., vlan, tunnel), switch log messages generated for that category are written to the switch log.

debug ipv6 trace-category [all | default | general | cmm-control | ni-data | ni-control | vlan | tunnel | neighbor | route | mip | ipc | cd | pm | sm | monitor | rtadv]

no debug ipv6 trace-category [all | default | general | cmmcontrol | nidata | nicontrol | vlan | tunnel | neigh | route | mip | ipc | cd | pm | sm | monitor | rtadv]

Syntax Definitions

all	Enable/disable all trace categories.
default	Enable the default trace categories (general and monitor).
general	Enable/disable the general trace category
cmm-control	Enable/disable trace messages pertaining to the CMM control socket.
ni-data	Enable/disable trace messages pertaining to the exchange of IPv6 packets with the NIs.
ni-control	Enable/disable trace messages pertaining to the control messages exchanged with the NIs.
vlan	Enable/disable trace messages pertaining to VLAN interfaces.
tunnel	Enable/disable trace messages pertaining to tunnel interfaces.
neighbor	Enable/disable trace messages pertaining to the neighbor cache.
route	Enable/disable trace messages pertaining to the forwarding table.
mip	Enable/disable trace messages pertaining to MIP processing.
ipc	Enable/disable trace messages pertaining to IPC communications.
cs	Enable/disable trace messages pertaining to chassis supervision.
pm	Enable/disable trace messages pertaining to port manager.
sm	Enable/disable trace messages pertaining to session manager.
monitor	Enable/disable debug and monitoring trace messages.
rtadv	Enable/disable router advertisement trace messages.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to disable debug messages for a category.
- The general and monitor categories are the only ones enabled by default.
- Options are additive across multiple command lines until reset with the “default” option.
- This command controls only debug level switch log messages (Debug 1,2,3). Messages at higher levels are always logged.

Example

```
-> debug ipv6 trace-category all
```

Release History

Release 5.1.6; command was introduced.

Related Commands

debug ipv6 packet	Configures the display of IPv6 debug messages.

MIB Objects

N/A.

show ipv6 hosts

Displays IPv6 Local Hosts Table.

show ipv6 hosts [*substring*]

Syntax Definitions

substring	Limits the display to host names starting with the specified substring.

Defaults

N/A.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

If you do not specify a substring, all IPv6 hosts are displayed.

Example

```
-> show ipv6 hosts

Name                                        IPv6 Address
--------------------------------------------+------------------------------------
ipv6-test1.alcatel.com                      4235::1200:0010
ipv6-test2.alcatel.com                      4235::1200:0020
otheripv6hostname                           4143:1295:9490:9303:00d0:6a63:5430:9031
```

output definitions

Name	Name associated with the IPv6 address.
IPv6 Address	IPv6 address associated with the host name.

Release History

Release 5.1.6; command was introduced.

Related Commands

ipv6 host	Configures a static host name to IPv6 address mapping to the local host table.

MIB Objects

```
alaIPv6HostTable
   alaIPv6HostName
   alaIPv6HostAddress
```

show ipv6 icmp statistics

Displays IPv6 ICMP statistics.

show ipv6 icmp statistics [*if_name*]

Syntax Definitions

if_name	Display statistics only for this interface.

Defaults

N/A.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

The ICMP Table can be used to monitor and troubleshoot the switch.

Example

```
-> show ipv6 icmp statistics

Message                          Received   Sent
-------------------------------+----------+----------
 Total                                    0          0
 Errors                                   0          0
 Destination Unreachable                  0          0
 Administratively Prohibited              0          0
 Time Exceeded                            0          0
 Parameter Problems                       0          0
 Packet Too Big                           0          0
 Echo Requests                            0          0
 Echo Replies                             0          0
 Router Solicitations                     0          0
 Router Advertisements                    0          0
 Neighbor Solicitations                   0          0
 Neighbor Advertisements                  0          0
 Redirects                                0          0
 Group Membership Queries                 0          0
 Group Membership Responses               0          0
 Group Membership Reductions              0          0
```

output definitions

Total	Total number of ICMPv6 messages the switch received or attempted to send.
Errors	Number of ICMPv6 messages the switch sent or received but was unable to process because of ICMPv6-specific errors (bad checksums, bad length, etc.).
Destination Unreachable	Number of Destination Unreachable messages that were sent or received by the switch.
Administratively Prohibited	Number of Destination Unreachable/Communication Administratively Prohibited messages sent or received by the switch.
Time Exceeded	Number of Time Exceeded messages sent or received by the switch.
Parameter Problems	Number of Parameter Problem messages sent or received by the switch.
Packet Too Big	Number of Packet Too Big messages sent or received by the switch.
Echo Requests	Number of Echo Request messages sent or received by the switch.
Echo Replies	Number of Echo Reply messages sent or received by the switch.
Router Solicitations	Number of Router Solicitations sent or received by the switch.
Router Advertisements	Number of Router Advertisements sent or received by the switch.
Neighbor Solicitations	Number of Neighbor Solicitations sent or received by the switch.
Neighbor Advertisements	Number of Neighbor Advertisements sent or received by the switch.
Redirects	Number of Redirect messages sent or received by the switch.
Group Membership Queries	Number of Group Membership Queries sent or received by the switch.
Group Membership Responses	Number of Group Membership Responses sent or received by the switch.
Group Membership Reductions	Number of Group Membership Reductions sent or received by the switch.

Release History

Release 5.1.6; command was introduced.

Related Commands

show ipv6 traffic	Displays IPv6 traffic statistics.

MIB Objects

```
ipv6IfIcmpTable
   ipv6IfIcmpInMsgs
   ipv6IfIcmpInErrors
   ipv6IfIcmpInDestUnreachs
   ipv6IfIcmpInAdminProhibs
   ipv6IfIcmpInTimeExcds
   ipv6IfIcmpInParmProblems
   ipv6IfIcmpInPktTooBigs
   ipv6IfIcmpInEchos
   ipv6IfIcmpInEchoReplies
   ipv6IfIcmpInRouterSolicits
   ipv6IfIcmpInRouterAdvertisements
   ipv6IfIcmpInNeighborSolicits
   ipv6IfIcmpInNeighborAdvertisements
   ipv6IfIcmpInRedirects
   ipv6IfIcmpInGroupMembQueries
   ipv6IfIcmpInGroupMembResponses
   ipv6IfIcmpInGroupMembReductions
   ipv6IfIcmpOutMsgs
   ipv6IfIcmpOutErrors
   ipv6IfIcmpOutDestUnreachs
   ipv6IfIcmpOutAdminProhibs
   ipv6IfIcmpOutTimeExcds
   ipv6IfIcmpOutParmProblems
   ipv6IfIcmpOutPktTooBigs
   ipv6IfIcmpOutEchos
   ipv6IfIcmpOutEchoReplies
   ipv6IfIcmpOutRouterSolicits
   ipv6IfIcmpOutRouterAdvertisements
   ipv6IfIcmpOutNeighborSolicits
   ipv6IfIcmpOutNeighborAdvertisements
   ipv6IfIcmpOutRedirects
   ipv6IfIcmpOutGroupMembQueries
   ipv6IfIcmpOutGroupMembResponses
   ipv6IfIcmpOutGroupMembReductions
```

show ipv6 interface

Displays IPv6 Interface Table.

show ipv6 interface [*if_name* | **loopback**]

Syntax Definitions

if_name	Interface name. Limits the display to a specific interface.
loopback	Limits display to loopback interfaces.

Defaults

N/A.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If you do not specify an interface name, all IPv6 interfaces are displayed.
- Specify an interface name (e.g., VLAN 12) to obtain more detailed information about a specific interface.

Example

```
-> show ipv6 interface

Name                IPv6 Address/Prefix Length               Status    Device
--------------------+----------------------------------------+---------+--------
smbif-5             fe80::2d0:95ff:fe12:f470/64              Active    VLAN 955
                    212:95:5::35/64
                    212:95:5::/64
v6if-to-eagle       fe80::2d0:95ff:fe12:f470/64              Disabled  VLAN 1002
                    195:35::35/64
                    195:35::/64
V6if-6to4-137       2002:d423:2323::35/64                    Active    6to4 Tunnel
                    2002:d423:2323::/64
v6if-tunnel-137     fe80::2d0:95ff:fe12:f470/64              Disabled  Tunnel 2
                    137:35:35::35/64
                    137:35:35::/64                           Active    loopback
loopback            ::1/128
```

output definitions

Name	Interface name. This is usually the VLAN on which the interface is configured.
IPv6 Address/Prefix Length	IPv6 address and prefix length assigned to the interface. If an interface has more than one IPv6 address assigned to it, each address is shown on a separate line.
Status	Interface status (e.g., Active/Inactive).
Device	The device on which the interface is configured (e.g., VLAN 955).

```
-> show ipv6 interface v6if-6to4-137

v6if-6to4-137
  IPv6 interface index        = 16777216(0x01000000)
  Administrative status       = Enabled
  Operational status          = Active
  Link-local address(es):
  Global unicast address(es):
    2002:d423:2323::35/64
  Anycast address(es):
    2002:d423:2323::/64
  Joined group addresses:
    ff02::1:ff00:0
    ff02::2:93da:68lb
    ff02::1
    ff02::1:ff00:35
  Maximum Transfer Unit (MTU) = 1280
  Send Router Advertisements  = No
  Maximum RA interval (sec)   = 600
  Minimum RA interval (sec)   = 198
  RA managed config flag      = False
  RA other config flag        = False
  RA reachable time (ms)      = 30000
  RA retransmit timer (ms)    = 1000
  RA default lifetime (sec)   = 1800
  Packets received            = 215686
  Packets sent                = 2019
  Bytes received              = 14108208
  Bytes sent                  = 178746
  Input errors                = 0
  Output errors               = 0
  Collisions                  = 0
  Dropped                     = 0
```

```
-> show ipv6 interface v6if-tunnel-137

v6if-tunnel-137
  IPv6 interface index        = 16777216(0x01000000)
  Administrative status       = Disabled
  Operational status          = Inactive
  Link-local address(es):
    fe80::2d0:95ff:fe12:f470/64
  Global unicast address(es):
    137:35:35:35/64
  Anycast address(es):
    137:35:35:35/64
  Joined group addresses:
    ff02::1:ff00:0
    ff02::1:ff00:35
    ff02::2:93da:68lb
    ff02::1
    ff02::1:ff12:f470
  Maximum Transfer Unit (MTU) = 1280
  Send Router Advertisements  = Yes
  Maximum RA interval (sec)   = 600
  Minimum RA interval (sec)   = 198
  RA managed config flag      = False
  RA other config flag        = False
  RA reachable time (ms)      = 30000
  RA retransmit timer (ms)    = 1000
  RA default lifetime (sec)   = 1800
  Packets received            = 0
  Packets sent                = 2
  Bytes received              = 0
  Bytes sent                  = 144
  Input errors                = 0
  Output errors               = 2
  Collisions                  = 0
  Dropped                     = 0
```

output definitions

IPv6 interface index	IPv6IfIndex value that should be used in SNMP requests pertaining to this interface.
Administrative status	Administrative status of this interface (Enabled/Disabled).
Operational status	Indicates whether the physical interface is connected to a device (Active/Inactive).
Hardware address	Interface's MAC address
Link-local address	Link-local address assigned to the interface.
Global unicast address(es)	Global unicast address(es) assigned to the interface.
Joined group address(es)	Addresses of the multicast groups that this interface has joined.
Maximum Transfer Unit	Interface MTU value.
Send Router Advertisements	Indicates if the router sends periodic router advertisements and responds to router solicitations on the interface.
Maximum RA interval (sec)	Maximum time between the transmission of unsolicited router advertisements over the interface.
Minimum RA interval (sec)	Minimum time between the transmission of unsolicited router advertisements over the interface (0.33 * Maximum RA Interval).

output definitions (continued)

RA managed config flag	True/False value in the managed address configuration flag field in router advertisements.
RA other config flag	The True/False value in the other stateful configuration flag field in router advertisements sent over this interface.
RA reachable time (ms)	Value placed in the reachable time field in the router advertisements sent over this interface.
RA retransmit timer (ms)	Value placed in the retransmit timer field in router advertisements sent over this interface.
RA default lifetime (ms)	The value placed in the router lifetime field in the router advertisements sent over this interface.
Packets received	Number of IPv6 packets received since the last time the counters were reset.
Packets sent	Number of IPv6 packets sent since the last time the counters were reset
Bytes received	Number of bytes of data received since the last time the counters were reset.
Bytes sent	Number of bytes of data sent since the last time the counters were reset.
Input errors	Number of input errors received since the last time the counters were reset.
Output errors	Number of output errors received since the last time the counters were reset.
Collisions	Number of collisions since the last time the counters were reset.
Dropped	Number of packets dropped since the last time the counters were reset

Release History

Release 5.1.6; command was introduced.

Related Commands

ipv6 address	Configures an IPv6 address on a VLAN, configured tunnel, or a 6to4 tunnel.
ipv6 interface	Configures an IPv6 interface on a VLAN.

MIB Objects

```
ipv6InterfaceTable
   ipv6AdminStatus
   ipv6PhysicalAddress
   ipv6InterfaceAddress
   ipv6Address
   ipv6AddressPrefix
   ipv6IfEffectiveMtu
   ipv6IfStatsInReceives
   ipv6IfStatsOutRequests
   ipv6IfStatsOutForwDatagrams
```

```
alaIPv6InterfaceTable
   alaIPv6InterfaceName
   alaIPv6InterfaceAddress
   alaIPv6InterfaceAdminStatus
   alaIPv6InterfaceRowStatus
   alaIPv6InterfaceDescription
   alaIPv6InterfaceMtu
   alaIPv6InterfaceType
   alaIPv6InterfaceAdminStatus
   alaIPv6InterfaceSendRouterAdvertisements
   alaIPv6InterfaceMaxRtrAdvInterval
   alaIPv6InterfaceAdvManagedFlag
   alaIPv6InterfaceAdvOtherConfigFlag
   alaIPv6InterfaceAdvReachableTime
   alaIPv6InterfaceAdvRetransTimer
   alaIPv6InterfaceAdvDefaultLifetime
   alaIPv6InterfaceName
   alaIPv6InterfaceAdvSendMtu
```

show ipv6 pmtu table

Displays the IPv6 Path MTU Table.

show ipv6 pmtu table

Syntax Definitions

N/A.

Defaults

N/A.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A.

Example

```
-> show ipv6 pmtu table

1-PMTU Entry
Destination Address                                      MTU      Expires
---------------------------------------------------------+--------+-------
fe80::02d0:c0ff:fe86:1207                                1280     1h 0m
```

output definitions

Destination Address	IPv6 address of the path's destination.
MTU	Path’s MTU.
Expires	Minimum remaining lifetime for the entry.

Release History

Release 5.1.6; command was introduced.

Related Commands

ipv6 pmtu-lifetime	Configures the configure the minimum lifetime for entries in the path MTU Table.
clear ipv6 pmtu table	Removes all entries from the IPv6 path MTU Table.

MIB Objects

```
alaIPv6ConfigTable
   alaIPv6PMTUDest
   alaIPv6PMTUexpire
```

clear ipv6 pmtu table

Removes all entries from the IPv6 path MTU Table.

clear ipv6 pmtu table

Syntax Definitions

N/A.

Defaults

N/A.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A.

Example

```
-> clear ipv6 pmtu table
```

Release History

Release 5.1.6; command was introduced.

Related Commands

ipv6 pmtu-lifetime	Configures the configure the minimum lifetime for entries in the path MTU Table.
show ipv6 pmtu table	Displays the IPv6 path MTU Table.

MIB Objects

```
alaIPv6ConfigTable
   alaIpv6ClearPMTUTable
```

show ipv6 neighbors

Displays IPv6 Neighbor Table.

show ipv6 neighbors [*ipv6_prefix/prefix_length* | *if_name* | **hw** *hardware_address* | **static]**

Syntax Definitions

ipv6_prefix/prefix_length	IPv6 prefix. Restricts the display to those neighbors starting with the specified prefix.
if_name	Interface name. Restricts the display to those neighbors reached via the specified interface.
hardware_address	MAC address. Restricts the display to the specified MAC address.
static	Restricts display to statically configured neighbors.

Defaults

N/A.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

If you do not specify an option (e.g., if_name), all IPv6 neighbors are displayed.

Example

```
-> show ipv6 neighbors

IPv6 Address                 Hardware Address    State     Type    Port  Interface
-----------------------------+------------------+----------+-------+-----+---------
fe80::02d0:c0ff:fe86:1207    00:d0:c0:86:12:07   Probe     Dynamic  1/15   vlan_4
fe80::020a:03ff:fe71:fe8d    00:0a:03:71:fe:8d   Reachable Dynamic  1/ 5   vlan_17
```

output definitions

IPv6 Address	The neighbor's IPv6 address.
Hardware Address	The MAC address corresponding to the IPv6 address.
State	The neighbor's state: - **Unknown** - **Incomplete** - **Reachable** - **Stale** - **Delay** - **Probe**.
Type	Indicates whether the neighbor entry is a **Static** or **Dynamic** entry.
Port	The port used to reach the neighbor.
Interface	The neighbor's interface name (e.g., vlan_1)

Release History

Release 5.1.6; command was introduced.

Related Commands

ipv6 neighbor	Configures a static entry in the IPv6 Neighbor Table.

MIB Objects

```
ipv6IfIndex
alaIPv6NeighborTable
   alaIPv6NeighborNetAddress
   alaIPv6NeighborPhysAddress
   alaIPv6NeighborSlot
   alaIPv6NeighborPort
   alaIPv6NeighborType
   alaIPv6NeighborState
```

clear ipv6 neighbors

Removes all entries, except static entries, from the IPv6 Neighbor Table.

clear ipv6 neighbors

Syntax Definitions

N/A.

Defaults

N/A.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This commands only clears dynamic entries. If static entries have been added to the table, they must be removed using the **no** form of the **ipv6 neighbor** command.

Example

```
-> clear ipv6 neighbors
```

Release History

Release 5.1.6; command was introduced.

Related Commands

ipv6 neighbor	Configures a static entry in the IPv6 Neighbor Table.
show ipv6 neighbors	Displays IPv6 Neighbor Table.

MIB Objects

```
alaIPv6NeighborTable
   alaIPv6ClearNeighbors
```

show ipv6 prefixes

Displays IPv6 prefixes used in router advertisements.

show ipv6 prefixes

Syntax Definitions

N/A.

Defaults

N/A.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A.

Example

```
-> show ipv6 prefixes

Legend: Flags: A = Autonomous Address Configuration, L = OnLink

                                          Valid     Preferred
Name           IPv6 Address/Prefix Length   Lifetime   Lifetime   Flags   Source
---------------+---------------------------+----------+----------+-------+---------
vlan 955       212:95:5::/64                 2592000    604800     LA     dynamic
vlan 1002      195:35::/64                   2592000    604800     LA     dynamic
6to4tunnel     2002:d423:2323::/64           2592000    604800     LA     dynamic
tunnel 2       137:35:35::/64                2592000    604800     LA     dynamic
```

output definitions

Name	The interface name. This is usually the VLAN on which the interface is configured.
IPv6 Address/Prefix Length	The IPv6 prefix and prefix length for a Router Advertisement Prefix Option.
Valid Lifetime	Length of time, in seconds, that this prefix will remain valid (i.e., time until deprecation). A value of 4,294,967,295 represents infinity.
Preferred Lifetime	Length of time, in seconds, that this prefix will remain preferred (i.e. time until deprecation). A value of 4,294,967,295 represents infinity.
Flags	**L** - Prefix can be used for onlink determination. **A** - Prefix can be used for autonomous address configuration (i.e., can be used to form a local interface address).
Source	**config** - Prefix has been configured by management. **dynamic** - Router Advertisements are using interface prefixes.

Release History

Release 5.1.6; command was introduced.

Related Commands

ipv6 prefix	Configures an IPv6 prefix on an interface. Used for configuring prefixes for router advertisements.

MIB Objects

```
IPv6AddrPrefixTable
   IPv6AddressPrefixEntry
   IPv6AddressPrefixLength
   IPv6AddressPrefixLinkFlag
   IPv6AddressPrefixAdvvalidLifetime
   IPv6AddressPrefixAdvPreferredLifetime
alaIPv6InterfacePrefixTable
   alaIPv6InterfacePrefix
   alaIPv6InterfacePrefixLength
   alaIPv6InterfacePrefixValidLifetime
   alaIPv6InterfacePrefixPreferredLifetime
   alaIPv6InterfacePrefixOnLinkFlag
   alaIPv6InterfacePrefixsource
```

show ipv6 routes

Displays IPv6 Forwarding Table.

show ipv6 routes [*ipv6_prefix/prefix_length* | **static]**

Syntax Definitions

ipv6_prefix/prefix_length	IPv6 prefix. Restricts the display to those routes starting with the specified prefix.
static	Restricts display to statically configured routes.

Defaults

N/A.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

If you do not specify an option (e.g., “static”), all IPv6 interfaces are displayed.

Example

```
-> show ipv6 routes

Legend:Flags:U = Up, G = Gateway, H = Host, S = Static, C = Cloneable, D = Dynamic,
             M = Modified, R = Unreachable, X = Externally resolved, B = Discard,
             L = Link-layer, 1 = Protocol specific, 2 = Protocol specific

Destination Prefix  Gateway Address           Interface         Age          Protocol  Flags
------------------+---------------+--------+-----------------+------------+---------+-----
::/0                2002:d468:8a89::137       v6if-6to4-137     18h 47m 26s  Static    UGS
137:35:35::/64      fe80::2d0:95ff:fe12:f470  v6if-tunnel-137   18h 51m 55s  Local     UC
195:35::/64         fe80::2d0:95ff:fe12:f470  v6if-to-eagle     18h 51m 55s  Local     UC
212:95:5::/64       fe80::2d0:95ff:fe12:f470  smbif-5           18h 51m 55s  Local     UC
2002::/16           2002:d423:2323::35        v6if-6to4-137     18h 51m 55s  Other     U
```

output definitions

Destination Prefix	IPv6 destination address and prefix.
Gateway Address	IPv6 address of the gateway used to reach the destination network.
Interface	The device the interface is using (e.g., VLAN 6to4tunnel); or loopback.
Age	Age of the entry. Entries less than 1 day old are displayed in hh:mm:ss format. Entries more than 1 day old are displayed in dd:hh format.
Protocol	Protocol by which the route was learned.

Release History

Release 5.1.6; command was introduced.

Related Commands

ipv6 route	Configures a static entry in the IPv6 route.

MIB Objects

```
IPv6RouteTable
   IPv6Routes
   IPv6RoutesPrefix
   IPV6RoutesStatic
alaIPv6StaticRouteTable
   alaIPv6StaticRouteEntry
```

show ipv6 tcp ports

Displays TCP Over IPv6 Connection Table. This table contains information about existing TCP connections between IPv6 endpoints.

show ipv6 tcp ports

Syntax Definitions

N/A.

Defaults

N/A.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Only connections between IPv6 addresses are contained in this table.

Example

```
-> show ipv6 tcp ports

Local Address        Port Remote Address                    Port   Interface      State
--------------------+--------------------------------------+------+--------------+--------
::                   21 ::                                  0                     listen
::                   23 ::                                  0                     listen
2002:d423:2323::35   21 212:61:61:0:2b0:doff:fe43:d4f8      34144  v6if-6to4-137  established
2002:d423:2323::35   49153 212:61:61:0:2b0:d0ff:fe43:d4f8   34144  v6if-6to4-137  established
```

output definitions

Local Address	Local address for this TCP connection. For ports in the “Listen” state, which accepts connections on any IPv6 interface, the address is ::0.
Port	Local port number for the TCP connection.
Remote Address	Remote IPv6 address for the connection. If the connection is in the “Listen” state, the address is ::0.
Port	Remote port number for the TCP connection. If the connection is in the “Listen” state, the port number is 0.
Interface	Name of the interface (or “unknown”) over which the connection is established.
State	State of the TCP connection as defined in RFC 793.

Release History

Release 5.1.6; command was introduced.

Related Commands

show ipv6 udp ports	Displays the UDP Over IPv6 Listener Table.

MIB Objects

```
IPv6TcpConnTable
   IPv6TcpConnEntry
   IPv6TcpConnLocalAddress
   IPv6TcpConnLocalPort
   IPv6TcpConnRemAddress
   IPv6TcpConnRemPort
   IPv6TcpConnIfIndex
   IPv6TcpConnState
```

show ipv6 traffic

Displays IPv6 traffic statistics.

show ipv6 traffic [*if_name*]

Syntax Definitions

if_name	Interface name. restricts the display to the specified interface instead of global statistics.

Defaults

N/A.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

The statistics show the cumulative totals since the last time the switch was powered on, the last reset of the switch was executed or the traffic statistics were cleared using the command.

Example

```
-> show ipv6 traffic

IPv6 statistics
  Packets received
    Total               = 598174
    Header errors       = 0
    Too big             = 12718
    No route            = 4
    Address errors      = 0
    Unknown protocol    = 0
    Truncated packets   = 0
    Local discards      = 0
    Delivered to users  = 582306
    Reassembly needed   = 0
    Reassembled         = 0
    Reassembly failed   = 0
    Multicast Packets   = 118
  Packets sent
    Forwarded           = 3146
    Generated           = 432819
    Local discards      = 0
    Fragmented          = 0
    Fragmentation failed = 0
    Fragments generated  = 0
    Multicast packets   = 265
```

output definitions

Total	Total number of input packets received, including those received in error.
Header errors	Number of input packets discarded due to errors in their IPv6 headers (e.g., version number mismatch, other format errors, hop count exceeded, errors discovered in processing their IPv6 options).
Too big	Number of input packets that could not be forwarded because their size exceeded the link MTU of the outgoing interface.
No route	Number of input packets discarded because no route could be found to transmit them to their destination.
Address errors	Number of input packets discarded because the IPv6 address in their IPv6 header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., ::0) and unsupported addresses (e.g., addresses with unallocated prefixes).
Unknown protocol	Number of locally-addressed packets received successfully but discarded because of an unknown or unsupported protocol.
Truncated packets	Number of input packets discarded because the packet frame did not carry enough data.
Local discards	Number of input IPv6 packets for which no problems were encountered to prevent their continued processing, ut which were discarded (e.g., for lack of buffer space). Note that this counter does not include any packets discarded while awaiting re-assembly.
Delivered to users	Total number of packets successfully delivered to IPv6 user protocols (including ICMP).
Reassembly needed	Number of IPv6 fragments received that needed to be reassembled.
Reassembled	Number of IPv6 packets successfully reassembled.
Reassembly failed	Number of failures detected by the IPv6 reassembly algorithm (for whatever reason: timed out, errors, etc.).
Multicast packets	Number of multicast packets received.
Forwarded	Number of output packets that this entity received and forwarded to their final destinations.
Generated	Total number of IPv6 packets that local IPv6 user-protocols (including ICMP) supplied to IPv6 in requests for transmission. Note that this counter does not include any packets counted by the Forwarded statistic.
Local discards	Number of output IPv6 packets for which no problem was encountered to prevent their transmission to their destination, but were discarded (e.g., for lack of buffer space). Note that this counter would include packets counted by the Forwarded statistic if any such packets met this (discretionary) discard criterion.
Fragmented	Number of IPv6 packets successfully fragmented.
Fragmentation failed	Number of IPv6 packets discarded because they needed to be fragmented but could not be.
Fragments generated	Number of output packet fragments generated as a result of fragmentation.
Multicast packets	Number of multicast packets transmitted.

Release History

Release 5.1.6; command was introduced.

Related Commands

show ipv6 icmp statistics	Displays IPv6 ICMP statistics.

MIB Objects

```
ipv6IfStatsTable
   ipv6IfStatsInReceives
   ipv6IfStatsInHdrErrors
   ipv6IfStatsInTooBigErrors
   ipv6IfStatsInNoRoutes
   ipv6IfStatsInAddrErrors
   ipv6IfStatsInUnknownProtos
   ipv6IfStatsInTruncatedPkts
   ipv6IfStatsInDiscards
   ipv6IfStatsInDelivers
   ipv6IfStatsOutForwDatagrams
   ipv6IfStatsOutRequests
   ipv6IfStatsOutDiscards
   ipv6IfStatsOutFragOKs
   ipv6IfStatsOutFragFails
   ipv6IfStatsOutFragCreates
   ipv6IfStatsReasmReqds
   ipv6IfStatsReasmOKs
   ipv6IfStatsReasmFails
   ipv6IfStatsInMcastPkts
   ipv6IfStatsOutMcastPkts
```

clear ipv6 traffic

Resets all IPv6 traffic counters.

clear ipv6 traffic

Syntax Definitions

N/A.

Defaults

N/A.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **show ipv6 traffic** command to view current IPv6 traffic statistics.

Example

```
-> clear ipv6 traffic
```

Release History

Release 5.1.6; command was introduced.

Related Commands

show ipv6 traffic	Displays IPv6 traffic statistics.

MIB Objects

```
alaIPv6ConfigTable
   alaIPv6ClearTraffic
```

show ipv6 tunnel

Displays IPv6 Tunnel information and whether the 6to4 tunnel is enabled.

show ipv6 tunnel

Syntax Definitions

N/A.

Defaults

N/A.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A.

Example

```
-> show ipv6 tunnel

IPv6 6to4 tunnel: Enabled
Configured Tunnels:
Tunnel              IPv6 Address/Prefix Length    Source IPv4     Destination IPv4
------------------+-----------------------------+---------------+-----------------
1                   2001:0000:0200::101/48        192.16.10.101   192.28.5.254
23                  2001:0000:0200::102/48        192.15.10.102   10.27.105.25
v6if-tunnel-137     fe80::2d0:95ff:fe12:f470/64   212.35.35.35    212.104.138.137
```

output definitions

IPv6 6to4 tunnel	Indicates whether 6to4 tunneling is enabled or disabled on the switch.
Tunnel	Tunnel ID.
IPv6 Address/Prefix Length	IPv6 address associated with the tunnel.
Source IPv4	Source IPv4 address for the tunnel.
Destination IPv4	Destination IPv4 address for the tunnel.

Release History

Release 5.1.6; command was introduced.

Related Commands

ipv6 interface tunnel source destination	Configures the source and destination IPv4 addresses for a configured tunnel.

MIB Objects

```
alaIPv6ConfigTunnelTable
   alaIPv6Tunnel6to4
   alaIPv6ConfigTunnelv4Source
   alaIPv6ConfigTunnelv4Dest
```

show ipv6 udp ports

Displays the UDP Over IPv6 Listener Table. This table contains information about UDP/IPv6 endpoints.

show ipv6 udp ports

Syntax Definitions

N/A.

Defaults

N/A.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Only endpoints utilizing IPv6 addresses are displayed in this table.

Example

```
-> show ipv6 udp ports

Local Address            Port    Interface
-----------------------+-------+--------------------
```

output definitions

Local Address	Local IPv6 address for this UDP listener. If a UDP listener accepts packets for any IPv6 address associated with the switch, the value is ::0.
Port	Local Port number for the UDP connection.
Interface	Name of the interface the listener is using or “unknown.”

Release History

Release 5.1.6; command was introduced.

Related Commands

show ipv6 tcp ports	Displays TCP Over IPv6 Connection Table.

MIB Objects

```
IPv6UdpTable
   IPv6UdpEntry
   IPv6UdpLocalAddress
   IPv6UdpLocalPort
   IPv6UdpIfIndex
```

ipv6 load rip

Loads RIPng into memory. When the switch is initially configured, you must load RIPng into memory to enable RIPng routing.

ipv6 load rip

Syntax Definitions

N/A.

Defaults

N/A.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- RIPng will support a maximum of 1,000 routes.
- RIPng will support a maximum of 20 interfaces.
- Use the **ipv6 rip status** command to enable RIPng on the switch.

Example

```
-> ipv6 load rip
```

Release History

Release 5.1.6; command was introduced.

Related Commands

ipv6 rip status	Enables/disables RIPng routing on the switch.
show ipv6 rip	Displays RIPng status and general configuration parameters.

MIB Objects

```
alaDrcTmConfig
   alaDrcTmIPRipngStatus
```

ipv6 rip status

Enables/disables RIPng on the switch.

ipv6 rip status {enable | disable}

Syntax Definitions

N/A

Defaults

parameter	default
enable | disable	enable

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

RIPng must be loaded on the switch (**ipv6 load rip**) to enable RIP on the switch.

Example

```
-> ipv6 rip status enable
```

Release History

Release 5.1.6; command was introduced.

Related Commands

ipv6 load rip	Loads RIPng into memory.
show ipv6 rip	Displays RIPng status and general configuration parameters.

MIB Objects

```
alaProtocolripng
   alaRipngProtoStatus
```

ipv6 rip invalid-timer

Configures the amount of time a route remains active in RIB before being moved to the "Garbage" state.

ipv6 rip invalid-timer *seconds*

Syntax Definitions

seconds	Time, in seconds, that a route will remain in an “Active” state. Valid range is 1 - 300.

Defaults

parameter	default
seconds	180

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This timer is reset each time a routing update is received.

Example

```
-> ipv6 rip invalid-timer 300
```

Release History

Release 5.1.6; command was introduced.

Related Commands

ipv6 rip garbage-timer	Configures the RIPng garbage timer value.
ipv6 rip holddown-timer	Configures the amount of time a route is placed in a holddown state.

MIB Objects

```
alaProtocolripng
   alaRipngInvalidTimer
```

ipv6 rip garbage-timer

Configures the RIPng garbage timer value. When a route in the RIB exceeds the configured Invalid Timer Value, the route is moved to a “Garbage” state in the the RIB. The garbage timer is the length of time a route will stay in this state before it is flushed from the RIB.

ipv6 rip garbage-timer *seconds*

Syntax Definitions

seconds	Time, in seconds, that a route will remain in the RIPng Routing Table before it is flushed from the RIB. Valid range is 0 - 180.

Defaults

parameter	default
seconds	120

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **ipv6 rip invalid-timer** command to set the Invalid Timer Value.

Example

```
-> ipv6 rip garbage-timer 180
```

Release History

Release 5.1.6; command was introduced.

Related Commands

ipv6 rip invalid-timer	Configures the amount of time a route remains active in RIB before being moved to the "Garbage" state.
ipv6 rip holddown-timer	Configures the amount of time a route is placed in a holddown state.

MIB Objects

```
alaProtocolripng
   alaRipngGarbageTimer
```

ipv6 rip holddown-timer

Configures the amount of time a route is placed in a holddown state. Whenever a route is seen from the same gateway with a higher metric than the route in the RIB, the route goes into holddown. This excludes route updates with an INFINITY metric.

ipv6 rip holddown-timer *seconds*

Syntax Definitions

seconds	Time, in seconds, that a route will remain in a holddown state. Valid range is 0 - 120.

Defaults

parameter	default
seconds	0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

While in holddown, the route continues being announced as usual and used in the RIB. This interval is used to control route flap dampening.

Example

```
-> ipv6 rip holddown-timer 60
```

Release History

Release 5.1.6; command was introduced.

Related Commands

ipv6 rip invalid-timer	Configures the amount of time a route remains active in RIB before being moved to the "Garbage" state.
ipv6 rip garbage-timer	Configures the RIPng garbage timer value.

MIB Objects

```
alaProtocolripng
   alaRipngHolddownTimer
```

ipv6 rip jitter

Configures an offset value for RIPng updates. This is the maximum (positive or negative) value that can be used to offset the update interval. For example, with an update interval of 30 seconds, and a jitter value of 5 seconds, the RIPng update packet would be sent somewhere (random) between 25 and 35 seconds from the previous update.

ipv6 rip jitter *value*

Syntax Definitions

value	Time, in seconds, that a routing update is offset. Valid range is 0 to one-half the updated interval value (e.g., if the updated interval is 30, the range would be 0 - 300).

Defaults

parameter	default
value	5

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

As you increase the number of RIPng interfaces/peers, it is recommended that you increase the Jitter value to reduce the number of RIPng updates being sent over the network.

Example

```
-> ipv6 rip jitter 10
```

Release History

Release 5.1.6; command was introduced.

Related Commands

ipv6 rip update-interval	Configures the RIPng update interval.
show ipv6 rip	Displays RIPng status and general configuration information.

MIB Objects

```
alaProtocolripng
   alaRipngJitter
```

ipv6 rip route-tag

Configures the route tag value for RIP routes generated by the switch.

ipv6 rip route-tag *value*

Syntax Definitions

value	Route tag value. Valid range is 0 – 65535.

Defaults

parameter	default
value	0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This value does not apply to routes learned from other routers. For these routes, the route tag propagates with the route.

Example

```
-> ipv6 rip route-tag 30
```

Release History

Release 5.1.6; command was introduced.

Related Commands

show ipv6 rip	Displays RIPng status and general configuration information.

MIB Objects

```
alaProtocolripng
   alaRipngRouteTag
```

ipv6 rip update-interval

Configures the RIPng update interval. This is the interval, in seconds, that RIPng routing updates will be sent out.

ipv6 rip update-interval *seconds*

Syntax Definitions

seconds	Interval, in seconds, that RIPng routing updates are sent out. Valid range is 0 - 120.

Defaults

parameter	default
seconds	30

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use this command, along with the **ipv6 rip jitter** command to configure RIPng updates.

Example

```
-> ipv6 rip update-interval 30
```

Release History

Release 5.1.6; command was introduced.

Related Commands

ipv6 rip jitter	Configures an offset value for RIPng updates.
show ipv6 rip	Displays RIPng status and general configuration information.

MIB Objects

```
alaRipng
   alaRipngUpdateInterval
```

ipv6 rip triggered-sends

Configures the behavior of triggered updates.

ipv6 rip triggered-sends {all | updated-only | none}

Syntax Definitions

all	All RIPng routes are added to any triggered updates.
updated-only	Only route changes that are causing the triggered update are included in the update packets.
none	RIPng routes are not added to triggered updates.

Defaults

parameter	default
all | updated-only | none	**updated-only**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If set to “all”, all routes are sent in the update, not just route changes, which increases RIPng traffic on the network.
- If set to “none”, no triggered updates are sent, which can cause delays in network convergence.

Example

```
-> ipv6 rip triggered-sends none
```

Release History

Release 5.1.6; command was introduced.

Related Commands

show ipv6 rip	Displays RIPng status and general configuration information.

MIB Objects

```
alaProtocolripng
   alaRipngTriggeredSends
```

ipv6 rip interface

Creates/deletes a RIPng interface.

ipv6 rip interface *if_name*

[no] ipv6 rip interface *if_name*

Syntax Definitions

if_name	IPv6 interface name.

Defaults

N/A.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- By default, a RIPng interface is created in the enabled state.
- Routing is enabled on a VLAN when you create a router port. However, to enable RIPng routing, you must also configure and enable a RIPng routing interface on the VLAN's IP router port. For more information on VLANs and router ports, see Chapter 21, "VLAN Management Commands".
- RIPng will support a maximum of 20 interfaces.

Example

```
-> ipv6 rip interface Test_Lab
```

Release History

Release 5.1.6; command was introduced.

Related Commands

ipv6 load rip	Loads RIPng into memory.
ipv6 rip status	Enables/disables RIPng on the switch.
ipv6 rip interface recv-status	Configures IPv6 RIPng interface “Receive” status. When this status is set to "enable", packets can be received on this interface.
ipv6 rip interface send-status	Configures IPv6 RIPng interface “Send” status. When this status is set to "enable", packets can be sent on this interface.
show ipv6 rip interface	Displays information for all or specified RIPng interfaces.

MIB Objects

```
alaRipngInterfaceTable
   alaRipngInterfaceStatus
```

ipv6 rip interface metric

Configures the RIPng metric or cost for a specified interface. You can set priorities for routes generated by a switch by assigning a metric value to routes generated by that switch's RIPng interface. For example, routes generated by a neighboring switch may have a hop count of 1. However, you can lower the priority of routes generated by that switch by increasing the metric value for routes generated by the RIPng interface.

ipv6 rip interface *if_name* **metric** *value*

Syntax Definitions

if_name	IPv6 interface name.
value	Metric value. Valid range is 1 - 15.

Defaults

parameter	default
value	1

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

When you configure a metric for a RIPng interface, this metric cost is added to the metric of the incoming route.

Example

```
-> ipv6 rip Test_Lab metric 1
```

Release History

Release 5.1.6; command was introduced.

Related Commands

ipv6 rip interface	Creates/deletes a RIPng interface.
show ipv6 rip interface	Displays information for all or specified RIPng interfaces.

MIB Objects

```
alaRipngInterfaceTable
   alaRipngInterfaceMetric
```

ipv6 rip interface recv-status

Configures IPv6 RIPng interface “Receive” status. When this status is set to "enable", packets can be received on this interface. When it is set to "disable", packets will not be received on this interface.

ipv6 rip interface *if_name* **recv-status {enable | disable}**

Syntax Definitions

if name	IPv6 interface name.
enable | disable	Interface “Receive” status.

Defaults

parameter	default
enable | disable	enable

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

RIPng must be loaded (**ipv6 load rip**) and enabled (**ipv6 rip status**)on the switch to send or receive packets on the interface.

Example

```
-> ipv6 rip interface Test_Lab recv-status disable
```

Release History

Release 5.1.6; command was introduced.

Related Commands

ipv6 load rip	Loads RIPng into memory.
ipv6 rip status	Enables/disables RIPng on the switch.
ipv6 rip interface send-status	Configures IPv6 RIPng interface “Send” status.

MIB Objects

```
alaRipngInterfaceTable
   alaRipngInterfaceRecvStatus
```

ipv6 rip interface send-status

Configures IPv6 RIPng interface “Send” status. When this status is set to "enable", packets can be sent from this interface. When it is set to "disable", packets will not be sent from this interface.

ipv6 rip interface *if_name* **send-status {enable | disable}**

Syntax Definitions

if name	IPv6 interface name.
enable | disable	Interface “Send” status.

Defaults

parameter	default
enable | disable	enable

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

RIPng must be loaded (**ipv6 load rip**) and enabled (**ipv6 rip status**)on the switch to send or receive packets on the interface.

Example

```
-> ipv6 rip interface Test_Lab send-status enable
```

Release History

Release 5.1.6; command was introduced.

Related Commands

ipv6 load rip	Loads RIPng into memory.
ipv6 rip status	Enables/disables RIPng on the switch.
ipv6 rip interface recv-status	Configures IPv6 RIPng interface “Receive” status.

MIB Objects

```
alaRipngInterfaceTable
   alaRipngInterfaceSendStatus
```

ipv6 rip interface horizon

Configures the routing loop prevention mechanisms.

ipv6 rip interface *if_name* **horizon {none | split-only | poison}**

Syntax Definitions

if_name	IPv6 interface name.
none | split-only | poison	**none** - Disables loop prevention mechanisms. **split-only** - Enables split-horizon, without poison-reverse. **poison** - Enables split-horizon with poison-reverse.

Defaults

parameter	default
none | split-only | poison	**poison**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If set to “none” the route is not sent back to the peer.
- If set to ‘split-only”, the route received from the peer is sent back with an increased metric.
- If set to “poison” the route received from the peer is sent back with an “infinity” metric.

Example

```
-> ipv6 rip interface Test_Lab none
```

Release History

Release 5.1.6; command was introduced.

Related Commands

show ipv6 rip interface	Displays information for all or specified RIPng interfaces.
show ipv6 rip routes	Displays all or a specific set of routes in the RIPng Routing Table.

MIB Objects

```
alaRipngInterfaceTable
   alaRipngInterfaceHorizon
```

ipv6 rip debug-level

Configures the RIPng debug level for all debug types.

ipv6 rip debug-level *level*

Syntax Definitions

level	Debug level. Valid range is 0 - 255.

Defaults

parameter	default
level	0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command sets the debug level for **all** configured types. You cannot set different levels for each type.
- Use the **ipv6 rip debug-type** command to specify the type of RIPng messages to debug.
- When the debug level is set to 0, the log is turned off.

Example

```
-> ipv6 rip debug-level 50
```

Release History

Release 5.1.6; command was introduced.

Related Commands

ipv6 rip debug-type	Configures the type of RIPng messages to debug.

MIB Objects

```
alaRipngDebug
   alaRipngDebugLevel
```

ipv6 rip debug-type

Configures the type of RIPng messages to debug.

ipv6 rip debug-type [error] [warning] [recv] [send] [rdb] [age] [mip] [info] [setup] [time] [tm] [all]

Syntax Definitions

error	Includes error conditions, failures, processing errors, etc.
warning	Includes general warnings, non-fatal conditions.
recv	Enables debugging in the receive flow path of the code.
send	Enables debugging in the send flow path of the code.
rdb	Debugs RIP database handling.
age	Debugs code handling database entry aging/timeouts.
mip	Debugs RIPng MIP messages.
info	Provides general information.
setup	Provides information during initialization.
time	Debugs timeout handler.
tm	Debugs RIPng Task Manager messages.
all	Enables all debug options.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to disable a debug type.
- You can configure more than on debug type in the same command (see example below).
- Use the **ipv6 rip debug-level** command to set the debug level. This command sets the debug level for **all** configured types. You cannot set different levels for each type.

Example

```
-> ipv6 rip debug-type error warning recv send
```

Release History

Release 5.1.6; command was introduced.

Related Commands

ipv6 rip debug-level	Configures the RIPng debug level.

MIB Objects

```
alaRipngDebug
   alaRipngDebugError
   alaRipngDebugWarn
   alaRipngDebugRecv
   alaRipngDebugSend
   alaRipngDebugRdb
   alaRipngDebugAge
   alaRipngDebugMip
   alaRipngDebugInfo
   alaRipngDebugSetup
   alaRipngDebugTime
   alaRipngDebugTm
   alaRipngDebugAll
```

show ipv6 rip

Displays RIPng status and general configuration parameters.

show ipv6 rip

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show ipv6 rip

Status              = Enabled,
Number of routes    = 10,
Route tag           = 0,
Update interval     = 30,
Invalid interval    = 180,
Garbage interval    = 120,
Holddown interval   = 0,
Jitter interval     = 5,
Triggered Updates   = All Routes,
```

output definitions

Status	RIPng protocol status (enabled or disabled).
Number of routes	Number of RIPng routes in Forwarding Information Base (FIB).
Route tag	Route tag value for RIP routes generated by the switch. Valid range is 0-65535. Default is 0.
Invalid interval	Invalid Timer setting, in seconds.
Garbage interval	Garbage Timer setting, in seconds.
Holddown interval	Holddown Timer setting, in seconds.
Jitter interval	Jitter setting.
Triggered updates	Triggered Updates setting (All Routes, Updated Routes, None).

Release History

Release 5.1; command was introduced.

Related Commands

ipv6 rip status	Enables/disables RIPng routing on the switch.
ipv6 rip route-tag	Configures the route tag value for RIP routes generated by the switch.
ipv6 rip update-interval	Configures the Interval, in seconds, that RIPng routing updates are sent out.
ipv6 rip invalid-timer	Configures the amount of time a route remains active in RIB before being moved to the "garbage" state.
ipv6 rip invalid-timer	Configures the RIPng garbage timer value. Routes move into the garbage collection state because the timer expired or a route update with an INFINITY metric was received.
ipv6 rip holddown-timer	Configures the amount of time a route is placed in a holddown state.
ipv6 rip jitter	Configures an offset value for RIPng updates. This is the maximum (positive or negative) value that can be used to offset the update interval.
ipv6 rip triggered-sends	Configures the behavior of triggered updates.

MIB Objects

```
alaRipngInterfaceTable
   alaRipngInterfaceStatus
   alaRipngRouteTag
   laRipngInvalidTimer
   alaRipngGarbageTimer
   alaRipngHolddownTimer
   alaRipngJitter
   alaRipngTriggeredSends
```

show ipv6 rip interface

Displays information for all or specified RIPng interfaces.

show ipv6 rip interface [*if_name*]

Syntax Definitions

if_name	IPv6 interface name.

Defaults

N/A.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

If you do not specify an interface, all IPv6 RIP interfaces are displayed.

Example

```
-> show ipv6 rip interface

    Interface                       Packets
       Name          Status     Recvd   Sent     Metric
--------------------+----------+---------+--------+---------
Test_Lab            Active     12986     12544    1
Test_Lab_2          Active     12556     12552    1


-> show ipv6 rip interface if3

Name                           = Test_Lab,
IPv6 interface index           = 3,
Interface status               = Active,
Next Update                    = 27 secs,
Horizon Mode                   = Split and Poison-reverse,
MTU size                       = 1500,
Metric                         = 1,
Send status                    = Enabled,
Receive status                 = Enabled,
Packets received               = 12986,
Packets sent                   = 12544,
```

output definitions

Interface name	Interface name.
IPv6 interface index	IPv6 index of this interface.
Status	Interface status (Active/Inactive).
Packets Recvd	Number of packets received by the interface.

output definitions

Packets Sent	Number of packets sent by the interface.
Metric	RIPng metric (cost) configured for the interface.
IPv6 interface index	IPv6 interface index number.
Interface status	Interface status (Active/Inactive).
Next update	Seconds remaining until the next update on this interface.
Horizon mode	Interface Horizon Mode (routing loop prevention mechanisms). Displayed modes are none/split-only/poison-reverse.
MTU size	Maximum transmission size for RIPng packets on the interface.
Send status	Interface “Send” status. When this status is set to "enable", packets can be sent from this interface. When it is set to "disable", packets will not be sent from this interface.
Receive status	Interface “Receive” status. When this status is set to "enable", packets can be received by this interface. When it is set to "disable", packets cannot be received by this interface.
Packets received	Number of packets received by the interface.
Packets sent	Number of packets sent by the interface.

Release History

Release 5.1.6; command was introduced.

Related Commands

ipv6 rip interface	IPv6 interface name.
ipv6 rip status	Enables/disables RIPng routing on the switch.
ipv6 rip interface recv-status	Configures the interface “Receive” status. When this status is set to "enable", packets can be received by this interface. When it is set to "disable", packets cannot be received by this interface.
ipv6 rip interface send-status	Configures the interface “Send” status. When this status is set to "enable", packets can be sent from this interface. When it is set to "disable", packets will not be sent from this interface.
ipv6 rip interface metric	Configures the RIPng metric (cost) for the interface.
ipv6 rip interface horizon	Configures the interface Horizon Mode (routing loop prevention mechanisms).
show ipv6 rip	Displays RIPng status and general configuration parameters (e.g., force holddown timer).

MIB Objects

```
alaRipngInterfaceTable
   alaRipngInterfaceEntry
   alaRipngInterfaceStatus
   alaRipngInterfacePacketsRcvd
   alaRipngInterfacePacketsSent
   alaRipngInterfaceMetric
   alaRipngInterfaceIndex
   alaRipngInterfaceNextUpdate
   alaRipngInterfaceHorizon
   alaRipngInterfaceMTU
   alaRipngInterfaceSendStatus
   alaRipngInterfaceRecvStatus
```

show ipv6 rip peer

Displays a summary of the observed RIPng peers, or specific information about a peer when a peer address is provided.

show ipv6 rip peer [*ipv6_addresss*]

Syntax Definitions

ipv6_addresss	IPv6 address of the peer.

Defaults

N/A.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

If you do not specify a peer, all IPv6 RIP peers are displayed.

Example

```
-> show ipv6 peer
                              Seen on       Packets   Last
Address                       Interface     Recv      Update
------------------------------+-------------+--------+----------
fe80::200:39ff:fe1f:710c      vlan172       23       20
fe80::2d0:95ff:fe12:da40      bkbone20      33       2
fe80::2d0:95ff:fe12:da40      vlan150       26       25
fe80::2d0:95ff:fe6a:5d41      nssa23        20       25



-> show ipv6 rip peer fe80::2d0:95ff:fe12:da40

Peer#1 address          = fe80::2d0:95ff:fe12:da40,
Seen on interface       = bkbone20,
Last Update             = 8 secs,
Received packets        = 33,
Received bad packets    = 0
Received routes         = 5,
Received bad routes     = 0

Peer#2 address          = fe80::2d0:95ff:fe12:da40,
Seen on interface       = vlan150,
Last Update             = 1 secs,
Received packets        = 27,
Received bad packets    = 0
Received routes         = 2,
Received bad routes     = 0
```

output definitions

Address	IPv6 address of the peer.
Seen on Interface	Interface used to reach the peer.
Packets Recvd	Number of packets received from the peer.
Last Update	Number of seconds since the last updated was received from the peer.
Peer address	Peer IPv6 address.
Received packets	Number of packets received from the peer.
Received bad packets	Number of bad packets received from the peer.
Received routes	Number of RIPng routes received from the peer.
Received bad routes	Number of bad RIPng routes received from the peer.

Release History

Release 5.1.6; command was introduced.

Related Commands

show ipv6 rip interface	Displays all or specified RIPng interface status
show ipv6 rip routes	Displays all or a specific set of routes in the RIPng Routing Table.

MIB Objects

```
alaRipngPeerTable
   alaRipngPeerEntry
   alaRipngPeerAddress
   alaRipngPeerIndex
   alaRipngPeerLastUpdate
   alaRipngPeerNumUpdates
   alaRipngPeerBadPackets
   alaRipngPeerNumRoutes
   alaRipngPeerBadRoutes
```

show ipv6 rip routes

Displays all or a specific set of routes in the RIPng Routing Table.

show ipv6 rip routes [dest <*ipv6_prefix/prefix_length*>**] | [gateway** <*ipv6_addr*>**] | [detail** <*ipv6 prefix/prefix_length*>**]**

Syntax Definitions

dest	Displays all routes whose destination matches the IPv6 prefix/prefix length.
gateway	Displays all routes whose gateway matches the specified IPv6 address.
detail	Displays detailed information about a single route matching the specified destination.
ipv6_addr	IPv6 address.
ipv6_prefix/prefix length	IPv6 address and prefix/prefix length.

Defaults

N/A.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

If you do not enter one of the optional parameters, all IPv6 RIP routes are displayed.

Example

```
-> show ipv6 rip routes

Legends: State: A = Active, H = Holddown, G = Garbage
Destination     Gateway                     State    Metric Proto
---------------+---------------------------+-------+------+------
100::1/128      +fe80::200:39ff:fe1f:710c     A       2      Rip
100::100:1/128  +fe80::200:39ff:fe1f:710c     A       2      Rip
400::/100       +fe80::2d0:95ff:fe12:e050     A       1      Local
900::/100       +fe80::2d0:95ff:fe12:e050     A       1      Local
8900::/100      +fe80::2d0:95ff:fe12:da40     A       2      Rip
9800::/100      +fe80::2d0:95ff:fe12:da40     A       2      Rip
9900::/100      +fe80::2d0:95ff:fe12:e050     A       1      Local
```

```
-> show ipv6 rip routes detail 9900::/100

Destination     = 9900::,
Mask length     = 100,
Gateway(1)      = fe80::2d0:95ff:fe12:e050,
Protocol        = Local,
Out Interface   = nssa23,
Metric          = 1,
Status          = Installed,
State           = Active,
Age             = 10544s,
Tag             = 0,
Gateway(2)      = fe80::2d0:95ff:fe12:da40,
Protocol        = Rip,
Out Interface   = bkbone20,
Metric          = 2,
Status          = Not Installed,
State           = Active,
Age             = 15s,
Tag             = 0,
```

output definitions

Destination	IPv6 address/address length of the destination.
Gateway	IPv6 gateway used to reach the destination.
State	Route status (Active/Inactive).
Metric	Routing metric for this route
Protocol	Protocol used to learn the route.
Mask Length	Prefix Length.
Out Interface	The interface used to reach the destination.
Status	Route status (Active/Inactive)
Age	The number of seconds since the route was last updated.
Tag	The route tag value for the route.

Release History

Release 5.1.6; command was introduced.

Related Commands

ipv6 rip interface	Creates/deletes a RIPng interface.
ipv6 rip interface metric	Configures the RIPng metric or cost for a specified interface.
show ipv6 rip interface	Displays all or specified RIPng interface status.

MIB Objects

```
alaRipngRouteTable
   alaRipngRouteEntry
   alaRipngRoutePrefixLen
   alaRipngRouteNextHop
   alaRipngRouteType
   alaRipngRouteAge
   alaRipngRouteTag
   alaRipngRouteStatus
   alaRipngRouteMetric
```

show ipv6 rip debug

Displays the current RIPng debug level and types.

show ipv6 rip debug

Syntax Definitions

N/A.

Defaults

N/A.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A.

Example

```
-> show ipv6 rip debug

Debug Level = 0,
error       = on,
warning     = off,
recv        = off,
send        = off,
rdb         = off,
age         = off,
mip         = off,
info        = off,
setup       = off,
time        = off,
tm          = off,
```

output definitions

Debug Level	Debug level. Valid range is 0 - 255. Default is 0.
Debug Type Status (on/off)	**error** - Includes error conditions, failures, processing errors, etc. **warning** - Includes general warnings, non-fatal conditions. **recv** - Enables debugging in the receive flow path of the code. **send** - Enables debugging in the send flow path of the code. **rdb** - Debugs RIP database handling. **age** - Debugs code handling database entry aging/timeouts. **mip** - Debugs RIPng MIP messages. **info** - Provides general information. **setup** - Provides information during initialization. **time** - Debugs timeout handler. **tm** - Debugs RIPng Task Manager messages. **all** - Enables all debug options.

Release History

Release 5.1.6; command was introduced.

Related Commands

ipv6 rip debug-level	Configures the RIPng debug level.
ipv6 rip debug-type	Configures the type of RIPng messages to debug.

MIB Objects

```
alaRipngDebug
   alaRipngDebugLevel
   alaRipngDebugError
   alaRipngDebugWarn
   alaRipngDebugRecv
   alaRipngDebugSend
   alaRipngDebugRdb
   alaRipngDebugAge
   alaRipngDebugMip
   alaRipngDebugInfo
   alaRipngDebugSetup
   alaRipngDebugTime
   alaRipngDebugTm
   alaRipngDebugAll
```

25 RDP Commands

This chapter details Router Discovery Protocol (RDP) commands for the switch. RDP is an extension of the Internet Control Message Protocol (ICMP) that provides a mechanism for end hosts to discover at least one router in the same network.

This implementation of RDP is based on the router requirements specified in RFC 1256. Switches that serve as a router can enable RDP to advertise themselves to clients on the same network at random intervals between a configurable range of time and in response to client solicitations.

MIB information for the RDP commands is as follows:

Filename: AlcatelIND1Rdp.mib
Module: alcatelIND1RDPMIB

A summary of the available commands is listed here:

ip router-discovery
ip router-discovery interface
ip router-discovery interface advertisement-address
ip router-discovery interface max-advertisement-interval
ip router-discovery interface min-advertisement-interval
ip router-discovery interface advertisement-lifetime
ip router-discovery interface preference-level
show ip router-discovery
show ip router-discovery interface

ip router-discovery

Enables or disables the Router Discovery Protocol (RDP) for the switch.

ip router-discovery {enable | disable}

Syntax Definitions

enable	Enables RDP on the switch.
disable	Disables RDP on the switch.

Defaults

By default, RDP is disabled on the switch.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The **ip router-discovery** command only activates RDP for the switch. No advertisements occur until an IP interface is configured with RDP.
- Note that if VRRP is enabled but there is no VRRP master on the network, RDP will not transmit advertisements. If a VRRP master is identified or VRRP is disabled, however, RDP will transmit advertisements as described in this chapter.

Example

```
-> ip router-discovery enable
-> ip router-discovery disable
```

Release History

Release 5.1; command was introduced.

Related Commands

ip router-discovery interface	Enables or disables an RDP interface.

MIB Objects

```
alaRDPConfig
   alaRDPStatus
```

ip router-discovery interface

Enables or disables RDP for the specified IP interface. An RDP interface is created for the specified IP interface name, which is then advertised by RDP as an active router on the local network.

ip router-discovery interface {*name* | *ip_address***} [enable | disable]**

no router-discovery interface {*name* | *ip_address***}**

Syntax Definitions

name	The IP interface name that was defined at the time the IP interface was configured.
ip_address	An existing 32-bit IP address that was defined at the time the IP interface was configured. *Not supported on the OmniSwitch 6600 Family, 7700/7800 or 8800*.
enable	Enables an RDP interface for the specified IP interface.
disable	Disables an RDP interface for the specified IP interface.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- When issuing this command on an OmniSwitch 6600 Family, 7700/7800, or 8800, specify the user-defined name that was assigned when the IP interface was configured.
- Do *not* use the **enable** option the first time this command is used to create an RDP interface, as it is not necessary and will return an error message. Once RDP is enabled and then is subsequently disabled, however, the **enable** option is then required the next time this command is used to enable the RDP interface.
- Use the **no** form of this command to remove the RDP interface from the switch configuration.
- The RDP interface is not active unless RDP is also enabled for the switch.

Example

The following examples apply to configuring an RDP interface on an OmniSwitch 6600 Family, 7700/7800, and 8800 (IP interface name is specified instead of IP address):

```
-> ip router-discovery interface Marketing
-> ip router-discovery interface Marketing disable
-> ip router-discovery interface Marketing enable
-> no ip router-discovery interface Marketing
```

Release History

Release 5.1; command was introduced.
Release 5.1.6; *ip_address* parameter replaced with *name* parameter on the OmniSwitch 6600 Family, 7700/7800, and 8800.

Related Commands

ip router-discovery	Enables or disables RDP for the switch.
ip interface	Configures an IP router interface for an OmniSwitch 6600 Family, 7700/7800, and 8800.

MIB Objects

```
alaRDPIfTable
   alaRDPIfStatus
```

ip router-discovery interface advertisement-address

Configures the destination address to which RDP will send router advertisement packets from the specified interface. Advertisement packets are sent at configurable intervals by routers to announce their IP addresses on the network.

ip router-discovery interface {*name* **|** *ip_address***} advertisement-address {all-systems-multicast | broadcast}**

Syntax Definitions

name	The IP interface name that was defined at the time the IP interface was configured.
ip_address	An existing 32-bit IP address that was defined at the time the IP interface was configured. *Not supported on the OmniSwitch 6600 Family, 7700/7800 or 8800*.
All-Systems-Multicast	Specifies 224.0.0.1 as the destination address for RDP advertisement packets.
Broadcast	Specifies 255.255.255.255 as the destination address for RDP advertisement packets. Use this address if IP multicast links are not available.

Defaults

parameter	default
all-systems-multicast | broadcast	**all-systems-multicast**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The RDP interface advertisement address is not active unless RDP is enabled for the switch and the specified interface is also enabled.
- RFC 1256 recommends the use of **all-system-multicast** on all links with “listening hosts” that support IP multicast.

Examples

The following examples apply to configuring an RDP interface on an OmniSwitch 6600 Family, 7700/7800, and 8800 (IP interface name is specified instead of IP address):

```
-> ip router-discovery interface Marketing advertisement-address all-systems-multi-
cast
-> ip router-discovery interface Accounting advertisement-address broadcast
```

Release History

Release 5.1; command was introduced.
Release 5.1.6; *ip_address* parameter replaced with *name* parameter on the OmniSwitch 6600 Family, 7700/7800, and 8800.

Related Commands

ip router-discovery	Enables or disables RDP for the switch.
ip router-discovery interface	Enables or disables an RDP interface.

MIB Objects

```
alaRDPIfTable
   alaRDPIfAdvtAddress
```

ip router-discovery interface max-advertisement-interval

Configures the maximum time, in seconds, RDP allows between each advertisement packet the router transmits on the specified interface.

ip router-discovery interface {*name* **|** *ip_address***} max-advertisement-interval** *seconds*

Syntax Definitions

name	The IP interface name that was defined at the time the IP interface was configured.
ip_address	An existing 32-bit IP address that was defined at the time the IP interface was configured. *Not supported on the OmniSwitch 6600 Family, 7700/7800 or 8800*.
seconds	The maximum amount of time allowed before the next advertisement occurs. The range is 4 to1800 seconds.

Defaults

parameter	default
seconds	600

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The RDP interface maximum advertisement time is not active unless RDP is enabled for the switch and the specified interface is also enabled.
- Do not specify a value for the maximum advertisement interval that is *less* than the value specified for the minimum advertisement interval. To set the minimum advertisement interval value, use the **ip router-discovery interface min-advertisement-interval** command.
- Note that the minimum and maximum advertisement values define an interval of time in which RDP transmits advertisement packets. RDP transmits packets at random times within this interval, waiting no longer than the maximum time specified and no sooner than the minimum time specified before the next transmission.

Examples

The following examples apply to configuring an RDP interface on an OmniSwitch 6600 Family, 7700/7800, and 8800 (IP interface name is specified instead of IP address):

```
-> ip router-discovery interface Marketing max-advertisement-interval 350
-> ip router-discovery interface Accounting max-advertisement-interval 20
```

Release History

Release 5.1; command was introduced.
Release 5.1.6; *ip_address* parameter replaced with *name* parameter on the OmniSwitch 6600 Family, 7700/7800, and 8800.

Related Commands

ip router-discovery	Enables or disables RDP for the switch.
ip router-discovery interface	Enables or disables an RDP interface.
ip router-discovery interface min-advertisement-interval	Configures the minimum time, in seconds, RDP allows between each advertisement packet the router transmits on the specified interface.
ip router-discovery interface advertisement-lifetime	Configures the maximum amount of time, in seconds, that router IP addresses received in advertisement packets are considered valid.

MIB Objects

```
alaRDPIfTable
   alaRDPIfMaxAdvtInterval
```

ip router-discovery interface min-advertisement-interval

Configures the minimum time, in seconds, RDP allows between each advertisement packet the router transmits on the specified interface.

ip router-discovery interface {*name* | *ip_address***} min-advertisement-interval** *seconds*

Syntax Definitions

name	The IP interface name that was defined at the time the IP interface was configured.
ip_address	An existing 32-bit IP address that was defined at the time the IP interface was configured. *Not supported on the OmniSwitch 6600 Family, 7700/7800 or 8800*.
seconds	The minimum amount of time allowed before the next advertisement occurs. The range is 3 seconds to the value set for the maximum advertisement interval.

Defaults

parameter	default
seconds	0.75 * maximum advertisement interval

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The RDP interface minimum advertisement time is not active unless RDP is enabled for the switch and the specified interface is also enabled.
- Do not specify a value for the minimum advertisement interval that is *greater* than the value specified for the maximum advertisement interval. To set the maximum advertisement interval value, use the **ip router-discovery interface max-advertisement-interval** command.
- Note that the minimum and maximum advertisement values define an interval of time in which RDP transmits advertisement packets. RDP transmits packets at random times within this interval, waiting no longer than the maximum time specified and no sooner than the minimum time specified before the next transmission.

Examples

The following examples apply to configuring an RDP interface on an OmniSwitch 6600 Family, 7700/7800, and 8800 (IP interface name is specified instead of IP address):

```
-> ip router-discovery interface Marketing min-advertisement-interval 20
-> ip router-discovery interface Accounting min-advertisement-interval 3
```

Release History

Release 5.1; command was introduced.
Release 5.1.6; *ip_address* parameter replaced with *name* parameter on the OmniSwitch 6600 Family, 7700/7800, and 8800.

Related Commands

ip router-discovery	Enables or disables RDP for the switch.
ip router-discovery interface	Enables or disables an RDP interface.
ip router-discovery interface max-advertisement-interval	Configures the maximum time, in seconds, RDP allows between each advertisement packet the router transmits on the specified interface.
ip router-discovery interface advertisement-lifetime	Configures the maximum amount of time, in seconds, that router IP addresses received in advertisement packets are considered valid.

MIB Objects

```
alaRDPIfTable
   alaRDPIfMinAdvtInterval
```

ip router-discovery interface advertisement-lifetime

Configures the maximum amount of time, in seconds, that router IP addresses advertised from the specified interface are considered valid. This value is set in the lifetime field of the advertisement packets transmitted on the specified RDP interface.

ip router-discovery interface {*name* **|** *ip_address***} advertisement-lifetime** *seconds*

Syntax Definitions

name	The IP interface name that was defined at the time the IP interface was configured.
ip_address	An existing 32-bit IP address that was defined at the time the IP interface was configured. *Not supported on the OmniSwitch 6600 Family, 7700/7800 or 8800.*
seconds	The length of time, in seconds, that advertised IP addresses are considered valid by the receiving host. The range is the value set for the maximum advertisement interval to 9000.

Defaults

parameter	default
seconds	3 * maximum advertisement interval

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The RDP interface advertisement lifetime value is not active unless RDP is enabled for the switch, and the specified interface is also enabled.
- Do not specify an advertisement lifetime value that is less than the value specified for the maximum advertisement interval. To set the maximum advertisement interval value, use the **ip router-discovery interface max-advertisement-interval** command.

Examples

The following examples apply to configuring an RDP interface on an OmniSwitch 6600 Family, 7700/7800, and 8800 (IP interface name is specified instead of IP address):

```
-> ip router-discovery interface Marketing advertisement-lifetime 2000
-> ip router-discovery interface Accounting advertisement-lifetime 750
```

Release History

Release 5.1; command was introduced.
Release 5.1.6; *ip_address* parameter replaced with *name* parameter on the OmniSwitch 6600 Family, 7700/7800, and 8800.

Related Commands

ip router-discovery	Enables or disables RDP for the switch.
ip router-discovery interface	Enables or disables an RDP interface.
ip router-discovery interface min-advertisement-interval	Configures the minimum time, in seconds, RDP allows between each advertisement packet the router transmits on the specified interface.
ip router-discovery interface max-advertisement-interval	Configures the maximum time, in seconds, RDP allows between each advertisement packet the router transmits on the specified interface.

MIB Objects

```
alaRDPIfTable
   alaRDPIfAdvLifeTime
```

ip router-discovery interface preference-level

Configures the preference level for each IP address advertised on the specified RDP interface. The end host selects the address with the highest preference level to use as its default router, if the host is not already redirected or configured to use another default router for a particular destination.

ip router-discovery interface {*name* **|** *ip_address***} preference-level** *level*

Syntax Definitions

name	The IP interface name that was defined at the time the IP interface was configured.
ip_address	An existing 32-bit IP address that was defined at the time the IP interface was configured. *Not supported on the OmniSwitch 6600 Family, 7700/7800 or 8800.*
level	Any positive, integer value.The higher the value, the higher the precedence.

Defaults

parameter	default
level	0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The RDP interface preference level value is not active unless RDP is enabled for the switch and the specified interface is also enabled.
- Set the preference level higher to encourage the use of an advertised router IP address.
- Set the preference level lower to discourage the use of an advertised router IP address.
- The preference level of an advertised router IP address is compared only to the preference levels of other addresses on the same subnet.

Examples

The following examples apply to configuring an RDP interface on an OmniSwitch 6600 Family, 7700/7800, and 8800 (IP interface name is specified instead of IP address):

```
-> ip router-discovery interface Marketing preference-level 10
-> ip router-discovery interface Accounting preference-level 50
```

Release History

Release 5.1; command was introduced.
Release 5.1.6; *ip_address* parameter replaced with *name* parameter on the OmniSwitch 6600 Family, 7700/7800, and 8800.

Related Commands

ip router-discovery	Enables or disables RDP for the switch.
ip router-discovery interface	Enables or disables an RDP interface.

MIB Objects

```
alaRDPIfTable
   alaRDPIfPrefLevel
```

show ip router-discovery

Displays the current RDP status and related statistics for the entire switch.

show ip router-discovery

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Each time RDP is enabled for the switch, all statistic parameter values are reset to zero for the new session. For example, if the RDP uptime was 160000 seconds when RDP was last disabled, the uptime starts out at zero the next time RDP is enabled.
- Use the **show ip router-discovery interface** command to display information about a specific RDP interface.

Examples

```
-> show ip router-discovery
Status                    = Enabled,
RDP uptime                = 161636 secs
#Packets Tx               = 4,
#Packets Rx               = 0,
#Send Errors              = 0,
#Recv Errors              = 0,
```

output definitions

Status	The status of RDP. **Enabled** allows RDP interfaces to advertise router IP addresses; **Disabled** stops RDP traffic on all switch interfaces. Use the **ip router-discovery** command to enable or disable RDP on the switch.
RDP uptime	Indicates the amount of time, in seconds, that RDP has remained active on the switch.
#Packets Tx	The number of RDP packets transmitted from all active RDP interfaces on the switch.
#Packets Rx	The number of RDP packets received on all active RDP interfaces on the switch.
#Send Errors	The number of RDP packet transmission errors that have occurred.
#Recv Errors	The number of errors that occurred when receiving RDP packets.

Release History

Release 5.1; command was introduced.

Related Commands

show ip router-discovery interface	Displays the current RDP status and related statistics for one or more switch router port interfaces.

MIB Objects

```
alaRDPConfig
   alaRDPStatus
```

show ip router-discovery interface

Displays the current RDP status, related parameter values, and RDP traffic statistics for one or more switch router interfaces.

show ip router-discovery interface [*name* **|** *ip_address***]**

Syntax Definitions

name	The IP interface name that was defined at the time the IP interface was configured.
ip_address	An existing 32-bit IP address that was defined at the time the IP interface was configured.

Defaults

By default, information for all RDP interfaces is displayed with this command.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- On the OmniSwitch 6600 Family, 7700/7800, and 8800, using either the IP interface name or the IP address is supported with this command.
- When an optional IP interface name or IP address is specified with this command, additional information about the RDP interface is displayed.
- Use the **show ip router-discovery** command to display global RDP status and statistics for the entire switch.

Examples

The following are examples of the **show ip router-discovery interface** output display on the OmniSwitch 6600 Family, 7700/7800, and 8800:

```
-> show ip router-discovery interface
                      IP i/f   RDP i/f  VRRP i/f      Next   #Pkts
         Name         status   status  status(#mast)  Advt sent/recvd
--------------------+--------+--------+--------------+----+----------
Marketing            Disabled  Enabled Disabled(0)    9    0   0
Accounting           Disabled  Enabled Disabled(0)    3    0   0
```

output definitions

Name	The user-defined IP interface name defined at the time the IP interface was configured.
IP i/f status	The IP status for this interface (**Enabled** or **Disabled)**.
RDP i/f status	The RDP status for this interface (**Enabled** or **Disabled**).

output definitions (continued)

VRRP i/f status (#mast)	The VRRP status for this interface (**Enabled** or **Disabled**), and the number of VRRP masters on the network for this interface.
Next Advt	Time remaining until the next advertisement is sent.
#Pkts sent/recvd	Number of advertisement packets sent from this interface; the number of solicitation packets received on this interface.

```
-> show ip router-discovery interface Marketing
Name                                    = Marketing,
IP Address                              = 11.255.4.1,
IP Mask                                 = 255.0.0.0,
IP Interface status                     = Enabled,
RDP Interface status                    = Enabled,
VRRP Interface status                   = Disabled,
Advertisement address                   = 224.0.0.1,
Max Advertisement interval              = 600 secs,
Min Advertisement interval              = 450 secs,
Advertisement lifetime                  = 1800 secs,
Preference Level                        = 0x0,
#Packets sent                           = 3,
#Packets received                       = 0,
```

output definitions

Name	The user-defined IP interface name defined at the time the IP interface was configured.
IP Address	The IP address associated with the IP interface name.
IP Mask	The subnet mask associated with the interface IP address.
IP Interface status	The IP status for this interface (**Enabled** or **Disabled**).
RDP Interface status	The RDP status for this interface (**Enabled** or **Disabled**).
VRRP Interface status	The VRRP status for this interface (**Enabled** or **Disabled**). See Chapter 29, "VRRP Commands," for more information.
Advertisement address	The destination address for RDP advertisement packets: **224.0.0.1** (all-systems-multicast) or **255.255.255.255** (broadcast). Configured using the **ip router-discovery interface advertisement-address** command.
Max Advertisement interval	The maximum time, in seconds, RDP allows between each advertisement packet the router transmits from this interface. Configured using the **ip router-discovery interface max-advertisement-interval** command.
Min Advertisement interval	The minimum time, in seconds, RDP allows between each advertisement packet the router transmits from this interface. Configured using the **ip router-discovery interface min-advertisement-interval** command.
Advertisement lifetime	The maximum amount of time, in seconds, that router IP addresses advertised from this interface are considered valid. Configured using the **ip router-discovery interface advertisement-lifetime** command.
Preference Level	The preference level, displayed in hex, for each IP address advertised on this interface. Configured using the **ip router-discovery interface preference-level** command.

output definitions (continued)

#Packets sent	The number of advertisement packets transmitted from this interface.
#Packets received	The number of solicitation packets received on this interface.

Release History

Release 5.1; command was introduced.
Release 5.1.6; command modified for the OmniSwitch 6600 Family, 7700/7800, and 8800.

Related Commands

show ip router-discovery	Displays the current RDP status and related statistics for the entire switch.
show vrrp	Displays the virtual router configuration for all virtual routers or for a particular virtual router.

MIB Objects

```
alaRDPIfTable
   alaRDPIfAdvtAdress
   alaRDPIfMaxAdvtInterval
   alaRDPIfMinAdvtInterval
   alaRDPIfAdvLifeTime
   alaRDPIfPrefLevel
```

26 DHCP Relay Commands

Bootstrap Protocol (BOOTP) and Dynamic Host Configuration Protocol (DHCP) packets contain configuration information for network hosts. DHCP Relay enables forwarding of BOOTP/DHCP packets between networks. This allows routing of DHCP traffic between clients and servers. It is not necessary to enable DHCP Relay if DHCP traffic is bridged through one network (i.e. clients and servers are on the same physical network).

This chapter includes a description of DHCP Relay commands that are used to define the IP address of DHCP servers, maximum number of hops, and forward delay time. Configure DHCP Relay on the switch where routing of BOOTP/DHCP packets occur.

MIB information for DHCP Relay commands is as follows:

Filename: AlcatelIND1UDPRelay.MIB
Module: ALCATEL-IND1-UDP-RELAY-MIB

A summary of the available commands is listed here.

ip helper address
ip helper address vlan
ip helper standard
ip helper avlan only
ip helper per-vlan only
ip helper forward delay
ip helper maximum hops
ip helper agent-information
ip helper agent-information policy
ip helper dhcp-snooping
ip helper dhcp-snooping mac-address verification
ip helper dhcp-snooping option-82 data-insertion
ip helper dhcp-snooping vlan
ip helper dhcp-snooping port
ip helper dhcp-snooping binding
ip helper dhcp-snooping binding timeout
ip helper dhcp-snooping binding action
ip helper boot-up
ip helper boot-up enable
ip udp relay
ip udp relay vlan
show ip helper
show ip helper stats
show ip helper dhcp-snooping vlan
show ip helper dhcp-snooping port
show ip helper dhcp-snooping binding
show ip udp relay service
show ip udp relay statistics
show ip udp relay destination

ip helper address

Adds or deletes a DHCP server IP address. DHCP Relay forwards BOOTP/DHCP broadcasts to and from the specified address. If multiple DHCP servers are used, configure one IP address for each server.

ip helper address *ip_address*

ip helper no address [*ip_address***]**

Syntax Definitions

ip_address	DHCP server IP address (e.g. 21.0.0.10).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Using this command enables a Global DHCP Relay service on the switch. When the DHCP Relay is specified by the DHCP server IP address, the service is called Global DHCP.
- When the DHCP Relay is specified by the VLAN number of the DHCP request, the service is referred to as Per-VLAN DHCP.
- Global DHCP and Per-VLAN DHCP are mutually exclusive. You may only configure one or the other.
- Use the **no** form of this command to delete an IP address from the DHCP Relay service. If an address is not specified, then all addresses are deleted.
- UPD Relay is automatically enabled on a switch when a DHCP server IP address is defined. There is no separate command for enabling or disabling the relay service.
- Configure DHCP Relay on switches where packets are routed between IP networks.
- You can configure up to 256 server IP addresses for one relay service.

Examples

```
-> ip helper address 75.0.0.10
-> ip helper no address 31.0.0.20
```

Release History

Release 5.1; command was introduced.

Related Commands

ip helper address vlan	Specifies or deletes DHCP Relay based on the VLAN of the DHCP request.
ip helper forward delay	Sets the forward delay time value. DHCP Relay will not process a client packet unless the packet contains an elapsed boot time value that is equal to or greater than the configured value of the forward delay time.
ip helper maximum hops	Sets the maximum number of hops value to specify how many relays a BOOTP/DHCP packet can traverse.
show ip helper	Displays current DHCP Relay configuration information.
show ip helper stats	Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

MIB Objects

```
iphelperTable
   iphelperService
   iphelperForwAddr
```

ip helper address vlan

Configures a DHCP Relay service for the specified VLAN. This command is used when a per-VLAN only relay service is active on the switch. It does not apply when using a standard relay service.

ip helper address *ip_address* **vlan** *vlan_id*

ip helper no address *ip_address* **vlan** *vlan_id*

Syntax Definitions

ip_address	IP address (e.g. 21.0.0.10) of the DHCP server VLAN.
vlan	Indicates that this command sets up a DHCP Relay based on the VLAN of the DHCP request.
vlan_id	VLAN identification number (e.g. 3) of the DHCP server VLAN. If no VLAN identification number is entered the default VLAN ID of 0 for this IP address is used.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of this command to delete the DHCP server VLAN from the DHCP Relay.
- The **ip helper address vlan** command does not work if the **per-vlan only** forwarding option is not active. Use the **ip helper per-vlan only** command to enable this option.
- Configure DHCP Relay on switches where packets are routed between IP networks.
- The per-VLAN only relay service supports a maximum of 256 VLANs.

Examples

```
-> ip helper address 75.0.0.10 3
-> ip helper no address 31.0.0.20 4
```

Release History

Release 5.1; command was introduced.

Related Commands

ip helper per-vlan only	Sets the DHCP Relay forwarding option to process only DHCP packets received from a specific, identified VLAN.
show ip helper	Displays current DHCP Relay configuration information.
show ip helper stats	Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

MIB Objects

```
iphelperTable
   iphelperService
   iphelperVlan
```

ip helper standard

Sets DHCP Relay forwarding option to standard. All DHCP packets are processed by a global relay service.

ip helper standard

Syntax Definitions

N/A

Defaults

By default, the DHCP Relay forwarding option is set to **standard**.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- To limit forwarding of DHCP packets to only packets that originate from authenticated ports, use the **ip helper avlan only** command.
- To process DHCP packets on a per VLAN basis, use the **ip helper per-vlan only** command.

Examples

```
-> ip helper standard
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip helper	Displays current DHCP Relay configuration information.
show ip helper stats	Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

MIB Objects

```
iphelperStatTable
   iphelperForwOption
```

ip helper avlan only

Sets DHCP Relay forwarding option to process only DHCP packets received on authenticated VLAN ports.

ip helper avlan only

Syntax Definitions

N/A

Defaults

By default, the UDP forwarding option is set to **standard**.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

When the forwarding option is set to **avlan only**, all other DHCP packets are not processed.

Examples

```
-> ip helper avlan only
```

Release History

Release 5.1; command was introduced.

Related Commands

ip helper standard	Sets DHCP Relay forwarding option to standard. All DHCP packets are processed.
ip helper per-vlan only	Sets the DHCP Relay forwarding option to process only DHCP packets received on authenticated ports from a specific, identified VLAN.
ip helper forward delay	Sets the forward delay time value. DHCP Relay will not process a client packet unless the packet contains an elapsed boot time value that is equal to or greater than the configured value of the forward delay time.
ip helper maximum hops	Sets the maximum number of hops value to specify how many relays a BOOTP/DHCP packet can traverse.
show ip helper	Displays current DHCP Relay configuration information.
show ip helper stats	Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

MIB Objects

```
iphelperStatTable
   iphelperForwOption
```

ip helper per-vlan only

Sets the DHCP Relay forwarding option to process only DHCP packets received from a specific, identified VLAN. This option allows each VLAN to have its own relay.

ip helper per-vlan only

Syntax Definitions

N/A

Defaults

By default, the UDP forwarding option is set to **standard**.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- When the forwarding option is set to **per-vlan only**, the **standard** (global) DHCP relay service is not available. These two types of services are mutually exclusive.
- Using the **per-vlan only** forwarding option requires you to specify a DHCP server IP address for each VLAN that will provide a relay service. The **ip helper address vlan** command performs this function and at the same time enables relay for the specified VLAN.

Examples

```
-> ip helper per-vlan only
```

Release History

Release 5.1; command was introduced.

Related Commands

ip helper address vlan	Configures a DHCP Relay service for the specified VLAN.
ip helper standard	Sets DHCP Relay forwarding option to standard. All DHCP packets are processed.
ip helper avlan only	Sets DHCP Relay forwarding option to process only DHCP packets received on authenticated VLAN ports from clients that are not yet authenticated.
show ip helper	Displays current DHCP Relay configuration information.
show ip helper stats	Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

MIB Objects

```
iphelperStatTable
   iphelperForwOption
```

ip helper forward delay

Sets the forward delay time value for the DHCP Relay configuration. The BOOTP/DHCP packet the client sends contains the elapsed boot time. This is the amount of time, in seconds, since the client last booted. DHCP Relay will not process the packet unless the client's elapsed boot time value is equal to or greater than the configured value of the forward delay time.

ip helper forward delay *seconds*

Syntax Definitions

seconds	Forward delay time value in seconds (1–65535). Do not use commas in the value.

Defaults

By default, the forward delay time is set to three seconds.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The time specified applies to all defined IP helper addresses.
- If a packet contains an elapsed boot time value that is less than the specified forward delay time value, DHCP Relay discards the packet.

Examples

```
-> ip helper forward delay 300
-> ip helper forward delay 120
```

Release History

Release 5.1; command was introduced.

Related Commands

ip helper address	Adds or deletes one or more DHCP server IP addresses to the DHCP Relay configuration.
ip helper maximum hops	Sets the maximum number of hops value to specify how many relays a BOOTP/DHCP packet can traverse.
show ip helper	Displays current DHCP Relay configuration information.
show ip helper stats	Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

MIB Objects

```
iphelperStatTable
   iphelperForwDelay
```

ip helper maximum hops

Sets the maximum number of hops value for the DHCP Relay configuration. This value specifies the maximum number of relays a BOOTP/DHCP packet is allowed to traverse until it reaches its server destination. Limiting the number of hops that can forward a packet prevents packets from looping through the network.

ip helper maximum hops *hops*

Syntax Definitions

hops	The maximum number of relays (1–16).

Defaults

By default, the maximum hops value is set to four hops.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If a packet contains a hop count equal to or greater than the *hops* value, DHCP Relay discards the packet.
- The maximum hops value only applies to DHCP Relay and is ignored by other services.

Examples

```
-> ip helper maximum hops 1
-> ip helper maximum hops 10
```

Release History

Release 5.1; command was introduced.

Related Commands

ip helper address	Adds or deletes one or more DHCP server IP addresses to the DHCP Relay configuration.
ip helper forward delay	Sets the forward delay time value. DHCP Relay will not process a client packet unless the packet contains an elapsed boot time value that is equal to or greater than the configured value of the forward delay time.
show ip helper	Displays current DHCP Relay configuration information.
show ip helper stats	Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

MIB Objects

```
iphelperStatTable
   iphelperMaxHops
```

ip helper agent-information

Enables or disables the DHCP relay agent information option (Option-82) feature.When this feature is enabled, local relay agent information is inserted into client DHCP packets when the agent forwards these packets to a DHCP server.

ip helper agent-information {enable | disable}

Syntax Definitions

enable	Enables the relay agent Option-82 feature for the switch.
disable	Disables the relay agent Option-82 feature for the switch.

Defaults

By default, this feature is disabled on the switch.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command enables the DHCP Option-82 feature for the entire switch; it is not configurable on a per-VLAN basis.
- When the DHCP Option-82 feature is enabled, DHCP Snooping is not available. These two features are mutually exclusive.
- When the relay agent receives a DHCP packet that already contains the Option-82 field, it will process the packet based on the agent information policy configured for the switch. This policy is configured using the **ip help agent-information policy** command.

Examples

```
-> ip helper agent-information enable
-> ip helper agent-information disable
```

Release History

Release 5.4.1; command was introduced.

Related Commands

ip helper agent-information policy	Configures a policy to determine how the relay agent handles DHCP packets that already contain the Option-82 field.
show ip helper	Displays current DHCP Relay configuration information.
show ip helper stats	Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

MIB Objects

```
iphelperAgentInformation
```

ip helper agent-information policy

Configures a policy that determines how the DHCP relay agent will handle DHCP packets that already contain an Option-82 field.

ip helper agent-information policy {drop | keep | replace}

Syntax Definitions

drop	Drop DHCP packets that already contain an Option-82 field.
keep	Keep the existing Option-82 field information and continue to relay the DHCP packet.
replace	Replace the existing Option-82 field information with local relay agent information and continue to relay the DHCP packet.

Defaults

By default, DHCP packets that already contain an Option-82 field are dropped.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The policy configured with this command is only applied if the DHCP Option-82 feature is enabled for the switch.
- The agent information policy is not applied if the DHCP relay agent receives a DHCP packet from a client that contains a non-zero value for the gateway IP address (giaddr). In this case, the agent will not insert the relay agent information option into the DHCP packet and will forward the packet to the DHCP server.
- Note that if a DHCP packet contains a gateway IP address (giaddr) value that matches a local subnet and also contains the Option-82 field, the packet is dropped by the relay agent.

Examples

```
-> ip helper agent-information policy drop
-> ip helper agent-information policy keep
-> ip helper agent-information policy replace
```

Release History

Release 5.4.1; command was introduced.

Related Commands

ip helper agent-information	Enables the insertion of relay agent information Option-82 into DHCP packets.
show ip helper	Displays current DHCP Relay configuration information.
show ip helper stats	Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

MIB Objects

```
iphelperAgentInformationPolicy
```

ip helper dhcp-snooping

Globally enables or disables DHCP Snooping for the switch. When this feature is enabled, all DHCP packets received on all switch ports are filtered.

ip helper dhcp-snooping {enable | disable}

Syntax Definitions

enable	Enables DHCP Snooping for the switch.
disable	Disables DHCP Snooping for the switch.

Defaults

By default, this feature is disabled.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If the DHCP relay agent Option-82 feature is enabled, DHCP Snooping is not available. These two features are mutually exclusive.
- If the DHCP Snooping feature is globally enabled for the switch, then configuring snooping on a per-VLAN basis is not allowed. The opposite is also true; invoking VLAN based snooping exudes the use of switch level snooping.
- When DHCP Snooping is enabled at the switch level, MAC address verification and Option-82 data insertion are enabled by default. In addition, the trust mode for all ports is set to the DHCP client only mode.

Examples

```
-> ip helper dhcp-snooping enable
-> ip helper dhcp-snooping disable
```

Release History

Release 5.4.1; command was introduced.

Related Commands

ip helper dhcp-snooping vlan .Enables or disables DHCP Snooping on a per VLAN basis.

MIB Objects

`iphelperDhcpSnooping`

ip helper dhcp-snooping mac-address verification

Globally enables or disables MAC address verification for incoming DHCP traffic. When this feature is enabled, the source MAC address is compared to the client hardware MAC address in the DHCP packet. If these two addresses do not match, the DHCP packet is dropped.

ip helper dhcp-snooping mac-address verification {enable | disable}

Syntax Definitions

enable	Enables DHCP MAC address verification for the switch.
disable	Disables DHCP MAC address verification for the switch.

Defaults

By default, this feature is disabled.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- When DHCP Snooping is enabled at the switch level, MAC address verification and Option-82 data insertion are enabled by default. In addition, the trust mode for all ports is set to the DHCP client only mode.
- Changing the enabled or disabled status for MAC address verification is only allowed when DHCP Snooping is globally enabled for the switch.

Examples

```
-> ip helper dhcp-snooping mac-address verification enable
-> ip helper dhcp-snooping mac-address verification disable
```

Release History

Release 5.4.1; command was introduced.

Related Commands

ip helper dhcp-snooping	.Globally enables or disables DHCP Snooping for the switch.
ip helper dhcp-snooping option-82 data-insertion	Globally enables or disables DHCP Option-82 data insertion for DHCP packets.

MIB Objects

```
iphelperDhcpSnoopingMacAddressVerificationStatus
```

ip helper dhcp-snooping option-82 data-insertion

Globally enables or disables DHCP Option-82 data insertion for DHCP packets. When this feature is enabled, the relay agent inserts the Option-82 field into DHCP packets before forwarding them to the DHCP server.

ip helper dhcp-snooping option-82 data-insertion {enable | disable}

Syntax Definitions

enable	Enables inserting the DHCP Option-82 field into DHCP packets.
disable	Disables inserting the DHCP Option-82 field into DHCP packets.

Defaults

By default, this feature is disabled.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- When DHCP Snooping is enabled at the switch level, Option-82 data insertion and MAC address verification are enabled by default. In addition, the trust mode for all ports is set to the DHCP client only mode.
- Using this command to change the operational status for Option-82 data insertion is only allowed when DHCP Snooping is globally enabled for the switch.
- Note that disabling the Option-82 data insertion operation is not allowed when the binding table functionality is enabled.

Examples

```
-> ip helper dhcp-snooping option-82 data-insertion enable
-> ip helper dhcp-snooping option-82 data-insertion disable
```

Release History

Release 5.4.1; command was introduced.

Related Commands

ip helper dhcp-snooping	.Globally enables or disables DHCP Snooping for the switch.
ip helper dhcp-snooping mac-address verification	Globally enables or disables MAC address verification for incoming DHCP traffic.
ip helper dhcp-snooping binding	Enables or disables the DHCP Snooping binding table functionality

MIB Objects

```
iphelperDhcpSnoopingOpt82DataInsertionStatus
```

ip helper dhcp-snooping vlan

Enables or disables DHCP Snooping on a per VLAN basis. When this feature is enabled, all DHCP packets received on ports associated with the DHCP Snooping VLAN are filtered.

ip helper dhcp-snooping vlan *vlan_id* **[mac-address verification {enable | disable}] [option-82 data-insertion {enable | disable}]**

no ip helper dhcp-snooping vlan *vlan_id*

Syntax Definitions

vlan_id	The VLAN identification number (1–4094).
mac-address verification	Enables or disables verifying the source MAC address of DHCP packets with the client MAC address contained in the same packet.
option-82 data-insertion	Enables or disables inserting Option-82 information into DHCP packets.

Defaults

By default, DHCP Snooping is disabled. When this feature is enabled for the specified VLAN, the following default parameter values apply:

parameter	default
mac-address verification	Enabled
option-82 data-insertion	Enabled

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of this command to disable DHCP Snooping for the specified VLAN.
- The MAC address verification and Option-82 data insertion are applied to packets received on ports associated with the DHCP Snooping VLAN.
- If the DHCP relay agent Option-82 feature is enabled, DHCP Snooping is not available. These two features are mutually exclusive.
- If the DHCP Snooping feature is globally enabled for the switch, then configuring snooping on a per-VLAN basis is not allowed. The opposite is also true; invoking VLAN based snooping exudes the use of switch level snooping.
- Note that disabling the Option-82 data insertion operation for a VLAN is not allowed when the binding table functionality is enabled.

Examples

```
-> ip helper dhcp-snooping vlan 100 enable
-> ip helper dhcp-snooping vlan 100 disable
```

Release History

Release 5.4.1; command was introduced.

Related Commands

ip helper dhcp-snooping	Globally enables or disables DHCP Snooping for the switch.
ip helper dhcp-snooping binding	Enables or disables the DHCP Snooping binding table functionality

MIB Objects

```
iphelperDhcpSnoopingVlanTable
   iphelperDhcpSnoopingVlanNumber
   iphelperDhcpSnoopingVlanMacVerificationStatus
   iphelperDhcpSnoopingVlanOpt82DataInsertionStatus
```

ip helper dhcp-snooping port

Configures the DHCP Snooping trust mode for the port. The trust mode determines if the port will accept all DHCP traffic, block all DHCP traffic, or accept only client DHCP traffic.

ip helper dhcp-snooping port *slot1/port1***[**-*port1a***] {block | client-only | trust}**

Syntax Definitions

*slot1/port1***[**-*port1a***]**	Specifies the slot number for the module and the physical port number on that module (e.g. 3/1 specifies port 1 on slot 3). Use a hyphen to specify a range of ports (e.g. 3/1-16).
block	Blocks all DHCP traffic on the port.
client-only	Allows only DHCP client traffic on the port.
trust	Allows all DHCP traffic on the port. The port behaves as if DHCP Snooping was not enabled.

Defaults

By default, the trust mode for a port is set to **client-only** when the DHCP Snooping feature is enabled for the switch or for a VLAN.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The DHCP trust mode only applies when the DHCP Snooping feature is enabled for the switch or for a VLAN.
- If DHCP Snooping is enabled at the switch level, the trust mode applies to all switch ports.
- If DHCP Snooping is enabled for a specific VLAN, then the trust mode applies to only those ports that are associated with that VLAN.
- Use the **ip helper dhcp-snooping port** command to display the current trust mode for a port and statistics regarding the number of packets dropped due to DHCP Snooping violations.

Examples

```
-> ip helper dhcp-snooping port 1/24 trust
-> ip helper dhcp-snooping port 2/1-10 block
-> ip helper dhcp-snooping port 4/8 client-only
```

Release History

Release 5.4.1; command was introduced.

Related Commands

ip helper dhcp-snooping	Globally enables or disables DHCP Snooping for the switch.
ip helper dhcp-snooping vlan	Enables or disables DHCP Snooping on a per-VLAN basis.

MIB Objects

```
iphelperDhcpSnoopingPortTable
   iphelperDhcpSnoopingPortIfIndex
   iphelperDhcpSnoopingPortTrustMode
```

ip helper dhcp-snooping binding

Enables or disables the DHCP Snooping binding table functionality. The binding table contains the MAC address, IP address, lease time, binding type (dynamic or static), VLAN number, and the interface information that corresponds to a local untrusted port on the switch. In addition, this command is also used to configure a static entry in the binding table.

ip helper dhcp-snooping port binding {[enable | disable] | [*mac_address* **port** *slot/port* **address** *ip_address* **lease-time** *time* **vlan** *vlan_id***]}**

no ip helper dhcp-snooping port binding *mac_address* **port** *slot/port* **address** *ip_address* **lease-time** *time* **vlan** *vlan_id*

Syntax Definitions

enable	Enables the creation of binding table entries.
disable	Disables the creation of binding table entries.
mac_address	The client MAC address.
slot/port	The slot and port number that received the DHCP request.
ip_address	The IP address that the DHCP server offered to the client.
time	The IP address lease time assigned by the DHCP server.
vlan_id	The VLAN identification number (1–4094) of the VLAN to which the client belongs.

Defaults

By default, the binding table functionality is enabled when the DHCP Snooping feature is enabled for the switch or for a VLAN.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of this command to remove a static entry from the DHCP Snooping binding table.
- The **enable** and **disable** parameters are independent of the other parameters, in that they are only used to turn the binding table functionality on and off. Enabling or disabling binding table functionality and creating a static binding table entry is not allowed on the same command line.
- Note that enabling the binding table functionality is not allowed if Option-82 data insertion is *not* enabled at either the switch or VLAN level.
- Static binding table entries are created using this command. If DHCP Snooping binding table functionality is not enabled, creating a static entry is not allowed.
- Dynamic binding table entries are created when the relay agent receives a DHCPACK packet.

Examples

```
-> ip helper dhcp-snooping binding disable
-> ip helper dhcp-snooping binding enable
-> ip helper dhcp-snooping binding 00:2a:95:51:6c:10 port 1/15 address 17.15.3.10
lease-time 3 vlan 200
-> no ip helper dhcp-snooping binding 00:2a:95:51:6c:10 port 1/15 address
17.15.3.10 lease-time 3 vlan 200
```

Release History

Release 5.4.1; command was introduced.

Related Commands

ip helper dhcp-snooping binding timeout	Configures the amount of time between each automatic save of the binding table contents to a file on the switch.
ip helper dhcp-snooping binding action	Synchronizes the contents of the DHCP Snooping binding table with the contents of the **dhcpBinding.db** file saved on the switch.

MIB Objects

```
iphelperDhcpSnoopingBindingStatus
iphelperDhcpSnoopingBindingTable
   iphelperDhcpSnoopingBindingMacAddress
   iphelperDhcpSnoopingBindingIfIndex
   iphelperDhcpSnoopingBindingIpAddress
   iphelperDhcpSnoopingBindingLeaseTime
   iphelperDhcpSnoopingBindingVlan
   iphelperDhcpSnoopingBindingType
```

ip helper dhcp-snooping binding timeout

Configures the amount of time between each automatic save of the DHCP Snooping binding table contents maintained in memory to a file on the switch. This functionality preserves binding table contents across switch reboots.

ip helper dhcp-snooping port binding timeout *seconds*

Syntax Definitions

seconds	The number of seconds (180 to 600) to wait before the next save.

Defaults

By default, the timeout value is set to 300 seconds.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The timeout value is only valid if the DHCP Snooping binding table functionality is enabled.
- The contents of the binding table is saved to the **dhcpBinding.db** file in the **/flash/switch** directory.
- The **dhcpBinding.db** file is time stamped when a save of the binding table contents is successfully completed.

Examples

```
-> ip helper dhcp-snooping binding timeout 600
-> ip helper dhcp-snooping binding timeout 250
```

Release History

Release 5.4.1; command was introduced.

Related Commands

ip helper dhcp-snooping binding	.Enables or disables the DHCP Snooping binding table functionality.
ip helper dhcp-snooping binding action	Synchronizes the contents of the DHCP Snooping binding table with the contents of the **dhcpBinding.db** file saved on the switch.

MIB Objects

```
iphelperDhcpSnoopingBindingDatabaseSyncTimeout
iphelperDhcpSnoopingBindingDatabaseLastSyncTime
```

ip helper dhcp-snooping binding action

Triggers a purge or renew action against the DHCP Snooping binding table. A purge action clears the contents of the table. A renew action populates the table with entries saved in the **dhcpBinding.db** file.

ip helper dhcp-snooping port binding action {purge | renew}

Syntax Definitions

purge	Clears all binding table entries that are maintained in switch memory.
renew	Populates the binding table with entries saved in the **dhcpBinding.db file** located in the **/flash/switch** directory on the switch.

Defaults

By default, the timeout value is set to 300 seconds.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

The DHCP Snooping binding table is maintained in the switch memory. Binding table entries are saved on a periodic basis to the **dhcpBinding.db** file on the switch. Use the **purge** and **renew** options available with this command to sync the binding table contents with the contents of the **dhcpBinding.db** file.

Examples

```
-> ip helper dhcp-snooping binding action purge
-> ip helper dhcp-snooping binding action renew
```

Release History

Release 5.4.1; command was introduced.

Related Commands

ip helper dhcp-snooping binding	.Enables or disables the DHCP Snooping binding table functionality.
ip helper dhcp-snooping binding timeout	Configures the amount of time between each automatic save of the binding table contents to a file on the switch.

MIB Objects

```
iphelperDhcpSnoopingBindingDatabaseAction
```

ip helper boot-up

Enables or disables automatic IP address configuration for default VLAN 1 when an unconfigured switch boots up. If enabled, the switch broadcasts a BootP or a DHCP request packet at boot time. When the switch receives an IP address from a BootP/DHCP server, the address is assigned to default VLAN 1.

Note. Automatic IP address configuration only supports the assignment of a *permanent* IP address to the switch. Make sure that the DHCP server is configured with such an address before using this feature.

ip helper boot-up {enable | disable}

Syntax Definitions

enable	Enables automatic IP address configuration for default VLAN 1.
disable	Disables automatic IP address configuration for default VLAN 1.

Defaults

By default, this feature is disabled on the switch.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **ip helper boot-up enable** command to specify BootP or DHCP for the request packet type.
- If an IP router port already exists for VLAN 1, a request packet is not broadcast even if automatic IP address configuration is enabled for the switch.

Examples

```
-> ip helper boot-up enable
-> ip helper boot-up disable
```

Release History

Release 5.1; command was introduced.

Related Commands

ip helper boot-up enable	Specifies BootP or DHCP as the type of request packet the switch will broadcast at boot time.

MIB Objects

```
iphelperStatTable
   iphelperBootupOption
```

ip helper boot-up enable

Specifies the type of packet to broadcast (BootP or DHCP) when automatic IP address configuration is enabled for the switch.

Note. Automatic IP address configuration only supports the assignment of a *permanent* IP address to the switch. Make sure that the DHCP server is configured with such an address before using this feature.

ip helper boot-up enable {BOOTP | DHCP}

Syntax Definitions

BOOTP	Broadcasts a BOOTP formatted request packet.
DHCP	Broadcasts a DHCP formatted request packet.

Defaults

parameter	default
BOOTP | DHCP	**BOOTP**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This command is only valid if automatic IP address configuration is already enabled for the switch.

Examples

```
-> ip helper boot-up enable DHCP
-> ip helper boot-up enable BOOTP
```

Release History

Release 5.1; command was introduced.

Related Commands

ip helper boot-up	Enables or disables automatic IP configuration for the switch.

MIB Objects

```
iphelperStatTable
   iphelperBootupPacketOption
```

ip udp relay

Enables or disables UDP port relay for BOOTP/DHCP and generic UDP service ports (i.e., NBNS/NBDD, other well-known UDP ports, and user-defined service ports that are not well-known).

ip udp relay {BOOTP | NBDD | NBNSNBDD | DNS | TACACS | TFTP | NTP | *port* **[***name***]}**

no ip udp relay {BOOTP | NBDD | NBNSNBDD | DNS | TACACS | TFTP | NTP | *port***}**

Syntax Definitions

BOOTP	BOOTP/DHCP well-known ports 67/68.
NBDD	NBDD well-known port 138.
NBNSNBDD	NBNS/NBDD well-known ports 137/138.
DNS	DNS well-known port 53.
TACACS	TACACS well-known port 65.
TFTP	TFTP well-known port 69.
NTP	NTP well-known port 123.
port	Any number that is not a well-known port number.
name	Text string description up to 30 characters.

Defaults

By default, relay is enabled on the BOOTP/DHCP well-known ports.

parameter	default
name	User Service Other#

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of this command to disable UDP Relay for the specified service port.
- Only use the *port* parameter to specify service port numbers that are not well known. For example, do not specify port 53 as it is the well-known port number for DNS. Instead, use the **DNS** parameter to enable relay for port 53.
- The *name* parameter is only used with the *port* parameter and provides a user-defined description to identify the not well-known port service.
- When entering a *name* for a user-defined service, quotes are required around ambiguous characters, such as hex characters, spaces, etc, so they are interpreted as text. For example, the *name* “A UDP Protocol” requires quotes because of the spaces between the words.

- When UDP Relay is disabled for BOOTP/DHCP, the **ip helper** configuration is *not* retained and all dependant functionality (i.e., automatic IP configuration for VLAN 1, Telnet and HTTP client authentication, etc.) is disrupted.
- Up to three types of UDP Relay services are supported at any one time and in any combination.

Note. If the relay service for BOOTP/DHCP is disabled when the switch reboots, the service is automatically enabled when the switch comes back up. If there were three non-BOOTP/DHCP relay services already enabled before the reboot, the most recent service enabled is disabled and replaced with the BOOTP/DHCP relay service.

- If port relay is enabled for the NBDD well-known port, NBNS is not automatically enabled by default. Specify **NBNS/NBDD** to enable relay for both well-known ports.
- Note that when UDP port relay is enabled for NTP, relay cannot forward NTP packets that contain a destination IP address that matches a VLAN router IP address on the switch.

Examples

```
-> ip udp relay DNS
-> ip udp 3047 “Generic Service”
-> no ip udp relay BOOTP
-> no ip udp relay 3047
```

Release History

Release 5.1; command was introduced.

Related Commands

ip udp relay vlan	Specifies the VLAN to which traffic from the specified UDP service port is forwarded.

MIB Objects

```
iphelperxServicePortAssociationTable
   iphelperxServicePortAssociationService
   iphelperxServicePortAssociationPort
   iphelperxServicePortAssociationName
iphelperxPortServiceAssociationTable
   iphelperxPortServiceAssociationService
   iphelperxPortServiceAssociationPort
   iphelperxPortServiceAssociationName
```

ip udp relay vlan

Specifies a VLAN on which traffic destined for a UDP port is forwarded.

ip udp relay {BOOTP | NBDD | NBNSNBDD | DNS | TACACS | TFTP | NTP | *port***} vlan** *vlan_id*

no ip udp relay {BOOTP | NBDD | NBNSNBDD | DNS | TACACS | TFTP | NTP | *port***} vlan** *vlan_id*

Syntax Definitions

BOOTP	BOOTP/DHCP well-known ports 67/68.
NBDD	NBDD well-known port 138.
NBNSNBDD	NBNS/NBDD well-known ports 137/138.
DNS	DNS well-known port 53.
TACACS	TACACS well-known port 65.
TFTP	TFTP well-known port 69.
NTP	NTP well-known port 123.
port	A user-specified port that is not a well-known port.
vlan_id	A numeric value (1–4094) that uniquely identifies an individual VLAN. Use a hyphen to specify a range of VLANs (e.g., 1-5).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of this command to remove the VLAN association with the UDP service port.
- The maximum number of VLANs that can receive forwarded UDP service port traffic is 256.
- Only specify service port numbers that are *not* well known when using the *port* parameter with this command. For example, do not specify port 53 as it is the well-known port number for the DNS UDP service. Instead, use the **DNS** parameter to enable relay for port 53.
- Specifying a VLAN for the BOOTP/DHCP service does not work if the **per-vlan only** forwarding option is not active. Use the **ip helper per-vlan only** command to enable this option.

Examples

```
-> ip udp relay DNS vlan 10
-> ip udp 3047 vlan 500
-> no ip udp relay DNS vlan 10
```

Release History

Release 5.1; command was introduced.

Related Commands

ip udp relay	Enables or disables relay for UDP service ports.

MIB Objects

```
iphelperxPortServiceAssociationTable
   iphelperxPortServiceAssociationService
```

show ip helper

Displays current DHCP Relay configuration.

show ip helper

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Displays information for all IP addresses configured.

Examples

The following example shows what the display output looks like when the DHCP Snooping feature is enabled and the DHCP relay agent information (Option-82) feature is disabled:

```
-> show ip helper
Forward Delay(seconds) = 3,
Max number of hops     = 4,
Relay Agent Information            =  Disabled,
  DHCP Snooping Status               =  Switch-Level Enabled,
      Option 82 Data Insertion Per Switch  =  Enabled,
      MAC Address Verification Per Switch  =  Enabled,
  DHCP Snooping Binding DB Status    =  Enabled,
      Database Sync Timeout          =  300,
      Database Last Sync Time        = 11:20:30 2/10/2006,
Forward option      = standard
  Vlan Number NA
Bootup Option Disable
  Forwarding Address:
    1.1.1.1
    21.2.2.10
    172.19.4.1
```

The following example shows what the display output looks like when the DHCP relay agent information (Option-82) feature is enabled and the DHCP Snooping feature is disabled:

```
-> show ip helper
Ip helper :
  Forward Delay(seconds) = 3,
  Max number of hops     = 4,
  Relay Agent Information            =  Enabled,
```

```
Relay Agent Information Policy     =  Keep
DHCP Snooping Status               =  Disabled
DHCP Snooping Binding DB Status    =  Disabled,
Forward option     = standard
    Vlan Number NA
Bootup Option Enable
Bootup Packet Option DHCP
    Forwarding Address :
      1.1.1.1
      21.2.2.10
      172.19.4.1
```

output definitions

Forward Delay	The current forward delay time (default is three seconds). Configured through the **ip helper forward delay** command.
Max number of hops	The current maximum number of hops allowed (default is four hops). Use the **ip helper maximum hops** command to change this value.
Forward option	The current forwarding option setting (**standard** or **avlan only**). Use the **ip helper standard** and **ip helper avlan only** commands to change this value.
Relay Agent Information	Indicates the status (**Enabled** or **Disabled**) of the DHCP relay agent information option (Option-82) feature. Configured through the **ip helper agent-information** command. This feature is disabled if the DHCP Snooping feature is enabled.
DHCP Snooping Status	Indicates the status (**Disabled**, **Switch-Level Enabled**, or **VLAN-Level Enabled**) of the DHCP Snooping feature. Configured through the **ip helper dhcp-snooping** or **ip helper dhcp-snooping vlan** command. This feature is disabled if the DHCP relay agent information option is enabled.
Option 82 Data Insertion Per Switch	Indicates whether or not the DHCP Option-82 field is added to DHCP packets (**Enabled** or **Disabled**). Configured through the **ip helper dhcp-snooping option-82 data-insertion** command. Note that this field only appears when DHCP Snooping is enabled at the switch level.
MAC Address Verification Per Switch	Indicates whether or not MAC address verification is performed on the DHCP packets (**Enabled** or **Disabled**). Configured through the **ip helper dhcp-snooping mac-address verification** command. Note that this field only appears when DHCP Snooping is enabled at the switch level.
DHCP Binding DB Status	Indicates if the DHCP Snooping binding table (database) functionality is **Enabled** or **Disabled**.
Database Sync Timeout	The amount of time, in seconds, that the switch waits between each synchronization of the DHCP Snooping binding table with the **dhcp-Binding.db** file (default is 300 seconds). Configured through the **ip helper dhcp-snooping binding timeout** command. Note that this field does not appear if the binding table functionality is disabled.
Database Last Sync Time	The last time and day the DHCP Snooping binding table was synchronized with the **dhcpBinding.db** file. Note that this field does not appear if the binding table functionality is disabled.

output definitions

Bootup Option	Indicates whether or not automatic IP address configuration for default VLAN 1 is done when the switch boots up (**Enabled** or **Disabled**). Configured through the **ip helper boot-up** command.
Bootup Packet Option	Indicates if the Bootup Option broadcasts a **DHCP** or **BOOTP** packet to obtain an IP address for default VLAN 1. Configured through the **ip helper boot-up enable** command. Note that this field does not appear if the Bootup Option is disabled.
Forwarding Addresses	IP addresses for DHCP servers that will receive BOOTP/DHCP packets forwarded by this DHCP Relay service. Use the **ip helper address** command to add or remove DHCP server IP addresses from the DHCP Relay configuration.

Release History

Release 5.1; command was introduced.
Release 5.4.1; new fields added for DHCP Option-82 and DHCP Snooping features.

Related Commands

show ip helper stats	Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

MIB Objects

```
iphelperTable
   iphelperService
   iphelperForwAddr
iphelperForwDelay
iphelperMaxHops
```

show ip helper stats

Displays the number of packets DHCP Relay has received, the number of packets dropped due to forward delay and maximum hops violations, and the number of packets processed since the last time these statistics were displayed. Also includes statistics that apply to a specific DHCP server, such as the number of packets transmitted to the server and the difference between the number of packets received from a client and the number transmitted to the server.

show ip helper stats

ip helper no stats

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **no** form of this command to clear all DHCP Relay statistics.

Examples

```
-> show ip helper stats
Global Statistics :
    Reception From Client :
      Total Count =        200, Delta =          0,
    Forw Delay Violation :
      Total Count =          0, Delta =          0,
    Max Hops Violation :
      Total Count =          0, Delta =          0,
 Server Specific Statistics :
    Server  2.2.2.1
        Tx Server :
          Total Count =          0, Delta =          0
Server  3.3.3.1
        Tx Server :
          Total Count =          0, Delta =          0
```

output definitions

Reception From Client	Number of packets DHCP Relay has received from the DHCP client.
Forw Delay Violation	Number of packets dropped as a result of forward delay violations. A violation occurs if a client packet contains an elapsed boot time value that is less than the configured DHCP Relay forward delay time value.

output definitions (continued)

Max Hops Violation	Number of packets dropped as a result of maximum hop violations. A violation occurs if a packet contains a hop count equal to or greater than the configured DHCP Relay maximum hops value.
Delta	The total number of packets processed since the last time ip helper statistics were checked during any user session.
Server	DHCP server IP address that receives BOOTP/DHCP packets forwarded by this DHCP Relay service. Use the **ip helper address** command to add or remove DHCP server IP addresses from DHCP Relay configuration.
Tx Server	Number of packets DHCP Relay has transmitted to the DHCP server.
Delta	The difference between the number of packets received from the client and the number of packets transmitted to the DHCP server since the last time DHCP Relay statistics were checked during any user session.

Release History

Release 5.1; command was introduced.

Related Commands

show ip helper	Displays current DHCP Relay configuration information.

MIB Objects

```
iphelperStatTable
   iphelperServerAddress
   iphelperRxFromClient
   iphelperTxToServer
   iphelperMaxHopsViolation
   iphelperForwDelayViolation
   iphelperResetAll
```

show ip helper dhcp-snooping vlan

Displays a list of VLANs that have DHCP Snooping enabled and whether or not MAC address verification and Option-82 data insertion is enabled for each VLAN.

show ip helper dhcp-snooping vlan

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command only applies if DHCP Snooping is enabled at the VLAN level.
- Use the **show ip helper** command to determine the status of DHCP Snooping at the switch level.

Examples

```
-> show ip helper dhcp-snooping vlan
VLAN    Opt82        MAC Addr
 ID    Insertion   Verification
------+----------+--------------
 50       Enabled      Enabled
 60       Enabled      Enabled
 100      Disabled     Enabled
 200      Enabled      Disabled
 1500     Disabled     Disabled
```

output definitions

VLAN ID	The VLAN identification number for the DHCP Snooping VLAN.
MAC Address Verification	Indicates whether or not MAC address verification is enabled for the VLAN (**Enabled** or **Disabled**). Configured through the **ip helper dhcp-snooping vlan** command.
Opt-82 Data Insertion	Indicates whether or not Option-82 data insertion is enabled for the VLAN (**Enabled** or **Disabled**). Configured through the **ip helper dhcp-snooping vlan** command.

Release History

Release 5.4.1; command was introduced.

Related Commands

show ip helper	Displays current DHCP Relay configuration information.
show ip helper dhcp-snooping port	Displays the trust mode and DHCP violation statistics for all switch ports that are filtered by DHCP Snooping.

MIB Objects

iphelperDhcpSnoopingVlanTable
```
iphelperDhcpSnoopingVlanNumber
iphelperDhcpSnoopingVlanMacVerificationStatus
iphelperDhcpSnoopingVlanOpt82DataInsertionStatus
```

show ip helper dhcp-snooping port

Displays the trust mode and DHCP Snooping violation statistics for all switch ports that are filtered by DHCP Snooping.

show ip helper dhcp-snooping port

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If DHCP Snooping is operating at the switch level, then information for all switch ports is displayed.
- If DHCP Snooping is operating at the VLAN level, then information for only those ports that are associated with a DHCP Snooping VLAN is displayed.
- The violation statistics displayed only apply to ports that are in the client only trust mode. When the trust mode for a port is changed from **client-only** to **trusted** or **blocked**, the violation counters are set to zero (0).

Examples

```
-> show ip helper dhcp-snooping port
Slot      Trust        Opt82       MAC      Server     Relay      Binding
Port      Mode       Violation  Violation  Violation  Violation  Violation
-----+-------------+----------+----------+----------+----------+----------
1/1        Blocked      0          0          0          0          0
1/2    Client-Only      0          0          0          0          0
1/3    Client-Only      0          0          0          0          0
1/4    Client-Only      0          0          0          0          0
1/5    Client-Only      0          0          0          0          0
1/6        Blocked      0          0          0          0          0
1/7    Client-Only      0          0          0          0          0
1/8    Client-Only      0          0          0          0          0
1/9    Client-Only      0          0          0          0          0
1/10       Trusted      0          0          0          0          0
1/11       Trusted      0          0          0          0          0
1/12       Trusted      0          0          0          0          0
```

output definitions

Slot/Port	The slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
Trust Mode	The DHCP Snooping trust mode for the port (**Blocked**, **Client-Only**, or **Trusted**). Configured through the **ip helper dhcp-snooping port** command.
Opt82 Violation	The number of DHCP packets dropped due to a DHCP Snooping Option-82 violation.
MAC Violation	The number of DHCP packets dropped due to a mismatch between the packet source MAC address and the client hardware address contained within the packet.
Server Violation	The number of DHCP server packets dropped because they originated from outside the network or firewall.
Relay Violation	The number of DHCP packets dropped because the packet included a relay agent IP address that was not 0.0.0.0.
Binding Violation	The number of DHCP packets dropped due to a mismatch between packets received and binding table information.

Release History

Release 5.4.1; command was introduced.

Related Commands

show ip helper	Displays current DHCP Relay configuration information.
show ip helper dhcp-snooping vlan	Displays a list of DHCP Snooping VLANs.

MIB Objects

```
iphelperDhcpSnoopingPortTable
   iphelperDhcpSnoopingPortIfIndex
   iphelperDhcpSnoopingPortTrustMode
   iphelperDhcpSnoopingPortOption82Violation
   iphelperDhcpSnoopingPortMacAddrViolation
   iphelperDhcpSnoopingPortDhcpServerViolation
   iphelperDhcpSnoopingPortRelayAgentViolation
   iphelperDhcpSnoopingPortBindingViolation
```

show ip helper dhcp-snooping binding

Displays the contents of the DHCP Snooping binding table (database).

show ip helper dhcp-snooping binding

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **ip helper dhcp-snooping binding** command to create a static entry in the binding table.
- Dynamic binding table entries are created when the relay agent receives a DHCPACK packet.

Examples

```
-> show ip helper dhcp-snooping binding
MAC Address        IP Address     VLAN ID  Slot/Port  Lease Time  Binding Type
-----------------+--------------+--------+----------+-----------+--------------
00:ae:22:e4:00:08  10.255.11.23      5        1/4       20000      Dynamic
10:fe:a2:e4:32:08  10.255.91.53      2        2/15      20000      Dynamic
```

output definitions

MAC Address	The MAC address of the client.
IP Address	The IP address offered by the DHCP server.
VLAN ID	The VLAN ID of the VLAN to which the client belongs.
Slot/Port	The slot/port designation for the switch port that received the DHCP request
Lease Time	The IP address lease time assigned by the DHCP server.
Binding Type	Indicates whether the binding table entry is **dynamic** or **static**. Static entries are created using the **ip helper dhcp-snooping binding** command.

Release History

Release 5.4.1; command was introduced.

Related Commands

show ip helper	Displays current DHCP Relay configuration information.
show ip helper dhcp-snooping vlan	Displays a list of DHCP Snooping VLANs.
show ip helper dhcp-snooping port	Displays the trust mode and DHCP violation statistics for all switch ports that are filtered by DHCP Snooping.

MIB Objects

```
iphelperDhcpSnoopingBindingStatus
iphelperDhcpSnoopingBindingTable
   iphelperDhcpSnoopingBindingMacAddress
   iphelperDhcpSnoopingBindingIfIndex
   iphelperDhcpSnoopingBindingIpAddress
   iphelperDhcpSnoopingBindingLeaseTime
   iphelperDhcpSnoopingBindingVlan
   iphelperDhcpSnoopingBindingType
```

show ip udp relay service

Displays current configuration for UDP services by service name or by service port number.

show ip udp relay service [BOOTP | NBDD | NBNSNBDD | DNS | TACACS | TFTP | NTP | *port***]**

Syntax Definitions

BOOTP	BOOTP/DHCP well-known ports 67/68.
NBDD	NBDD well-known port 138.
NBNSNBDD	NBNS/NBDD well-known ports 137/138.
DNS	DNS well-known port 53.
TACACS	TACACS well-known port 65.
TFTP	TFTP well-known port 69.
NTP	NTP well-known port 123.
port	A user-specified port that is not a well-known port.

Defaults

By default, the configuration for all UDP services is shown.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Enter a service name or port number with this command to display information about an individual service.
- When specifying a port number, do not specify a well-known port number. Instead, use the service name for the well-known port (i.e., NBNS/NBDD, DNS, etc.).

Examples

```
-> show ip udp relay service

Service    Port(s)  Description
---------+--------+-----------------
  1        67  68   BOOTP/DHCP
  4        53       DNS
  5        65       TACACS

-> show ip udp relay service dns

Service    Port(s)  Description
---------+--------+-----------------
   4       53       DNS
```

```
-> show ip udp relay service 1776

Service    Port(s)  Description
---------+--------+------------------
   9       1776     A UDP protocol
```

output definitions

Service	The UDP service number. (**1** through **7** for well-known service ports and **8** and above for user-defined service ports).
Port(s)	The UDP service port number.
Description	A description of the UDP service.

Release History

Release 5.1; command was introduced.

Related Commands

show ip udp relay statistics	Displays the current statistics for each UDP port relay service.
show ip udp relay destination	Displays the VLAN assignments to which the traffic received on the specified UDP service port is forwarded.

MIB Objects

```
iphelperxPropertiesTable
   iphelperxPropertiesService
   iphelperxPropertiesPort
   iphelperxPropertiesName
```

show ip udp relay statistics

Displays the current statistics for each UDP port relay service. These statistics include the name of the service, the forwarding VLAN(s) configured for that service, and the number of packets the service has sent and received.

show ip udp relay [BOOTP | NBDD | NBNSNBDD | DNS | TACACS | TFTP | NTP | *port***]**

Syntax Definitions

BOOTP	BOOTP/DHCP well-known ports 67/68.
NBDD	NBDD well-known port 138.
NBNSNBDD	NBNS/NBDD well-known ports 137/138.
DNS	DNS well-known port 53.
TACACS	TACACS well-known port 65.
TFTP	TFTP well-known port 69.
NTP	NTP well-known port 123.
port	A user-specified port that is not a well-known port.

Defaults

By default, the statistics for all UDP services is shown.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Enter a service name or port number with this command to display information about an individual service.
- When specifying a port number, do not specify a well-known port number. Instead, use the service name for the well-known port (i.e., NBNS/NBDD, DNS, etc.).

Examples

```
-> show ip udp relay statistics

Service          Vlan     Pkts Sent   Pkts Recvd
---------------+--------+------------+----------
BOOTP                        0           0
DNS              2          10          10
                 4          15          15
TACACS           3           0           0
```

```
-> show ip udp relay statistics tacacs

Service          Vlan     Pkts Sent   Pkts Recvd
---------------+--------+------------+-----------
TACACS            3        0            0

-> show ip udp relay statistics 1776

Service              Vlan     Pkts Sent   Pkts Recvd
-------------------+--------+-----------+-----------
A UDP Protocol       18       2           2
```

output definitions

Service	The active UDP service name.
VLAN	The VLAN assigned to the UDP service port that will forward traffic destined for that port. Use the **ip udp relay vlan** command to configure this value.
Pkts Sent	The number of packets sent from this service port to the server.
Pkts Recvd	The number of packets received by this service port from a client.

Release History

Release 5.1; command was introduced.

Related Commands

show ip udp relay service	Displays current configuration for UDP services by service name or by service port number.
show ip udp relay destination	Displays the VLAN assignments to which the traffic received on the specified UDP service port is forwarded.

MIB Objects

```
iphelperxStatTable
   iphelperxStatService
   iphelperxStatVlan
   iphelperxStatTxToServer
   iphelperxStatRxFromClient
```

show ip udp relay destination

Displays the VLAN assignments to which the traffic received on the specified UDP service port is forwarded.

show ip udp relay destination [BOOTP | NBDD | NBNSNBDD | DNS | TACACS | TFTP | NTP | *port***]**

Syntax Definitions

BOOTP	BOOTP/DHCP well-known ports 67/68.
NBDD	NBDD well-known port 138.
NBNSNBDD	NBNS/NBDD well-known ports 137/138.
DNS	DNS well-known port 53.
TACACS	TACACS well-known port 65.
TFTP	TFTP well-known port 69.
NTP	NTP well-known port 123.
port	A user-specified port that is not a well-known port.

Defaults

By default, the forwarding VLAN assignments for all UDP services is shown.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Enter a service name or port number with this command to display information about an individual service.
- When specifying a port number, do not specify a well-known port number. Instead, use the service name for the well-known port (i.e., NBNS/NBDD, DNS, etc.).

Examples

```
-> show ip udp relay destination

Service          Port     VLANs
---------------+--------+----------------
BOOTP            67
DNS              53       2  4
TACACS           65       3

-> show ip udp relay destination dns

Service          Port     VLANs
---------------+--------+----------------
DNS              53       2  4
```

```
-> show ip udp relay destination 1776

Service            Port     VLANs
-----------------+--------+----------------
A UDP Protocol     1776     18
```

output definitions

Service	The active UDP service name.
Port	The UDP service port number.
VLANs	The VLAN assigned to the UDP service port that will forward traffic destined for that port. Use the **ip udp relay vlan** command to configure this value.

Release History

Release 5.1; command was introduced.

Related Commands

show ip udp relay service	Displays current configuration for UDP services by service name or by service port number.
show ip udp relay statistics	Displays the current statistics for each UDP port relay service.

MIB Objects

```
iphelperTable
   iphelperService
   iphelperVlan
iphelperxPropertiesTable
   iphelperxPropertiesName
   iphelperxPropertiesPort
```

27 RIP Commands

Routing Information Protocol (RIP) is an Interior Gateway Protocol (IGP) that uses hop count as its routing metric. RIP-enabled switches update neighboring switches by transmitting a copy of their own routing table. The RIP routing table always uses the most efficient route to a destination, that is, the route with the fewest hops and longest matching prefix.

The switch supports RIP version 1 (RIPv1), RIP version 2 (RIPv2), and RIPv2 that is compatible with RIPv1. It also supports simple and MD5 authentication, on an interface basis, for RIPv2.

The RIP commands comply with the following RFCs: RFC1058, RFC2453, RFC1722, RFC1723, RFC1724.

MIB information for the RIP commands is as follows:

Filename: RIPv2.mib
Module: rip2

Filename: AlcatelIND1Rip.mib
Module: alaRipMIB

A summary of the available commands is listed here:

ip load rip
ip rip status
ip rip interface
ip rip interface status
ip rip interface metric
ip rip interface send-version
ip rip interface recv-version
ip rip force-holddowntimer
ip rip host-route
ip rip route-tag
ip rip redist status
ip rip redist
ip rip redist metric
ip rip redist-filter
ip rip redist-filter effect
ip rip redist-filter metric
ip rip redist-filter route-tag
ip rip redist-filter redist-control
ip rip interface auth-type
ip rip interface auth-key
ip rip debug-type
ip rip debug-level
show ip rip
show ip rip routes
show ip rip interface
show ip rip peer
show ip rip redist
show ip rip redist-filter
show ip rip debug

ip load rip

Loads RIP into memory. When the switch is initially configured, you must load RIP into memory before it can be enabled.

ip load rip

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- In simple networks where only IP forwarding is required, you may not want to use RIP. If you are not using RIP, it is best not to load it to save switch resources.
- To remove RIP from switch memory, you must manually edit the **boot.cfg** file. The **boot.cfg** file is an ASCII text-based file that controls many of the switch parameters. Open the file and delete all references to RIP. You must reboot the switch when this is complete.
- Use the **ip rip status** command to enable RIP on the switch.

Examples

```
-> ip load rip
```

Release History

Release 5.1; command was introduced.

Related Commands

ip rip status	Enables/disables RIP routing on the switch.
show ip rip	Displays RIP status and general configuration parameters.

MIB Objects

```
alaDrcTmConfig
   alaDrcTmIPRipStatus
```

ip rip status

Enables/disables RIP on the switch. RIP performs well in small networks. By default, RIP packets are broadcast every 30 seconds, even if no change has occurred anywhere in a route or service. Depending on the size and speed of the network, these periodic broadcasts can consume a significant amount of bandwidth.

ip rip status {enable | disable}

Syntax Definitions

enable	Enables RIP routing on the switch.
disable	Disables RIP routing on the switch.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- RIP must be loaded on the switch (**ip load rip**) to enable RIP on the switch.
- A RIP network can be no more than 15 hops (end-to-end). If there is a 16th hop, that network is identified as infinity and the packet is discarded.

Examples

```
-> ip rip status enable
```

Release History

Release 5.1; command was introduced.

Related Commands

ip load rip	Loads RIP into switch memory.
show ip rip	Displays RIP status and general configuration parameters.

MIB Objects

```
alaProtocolRip
   alaRipProtoStatus
```

ip rip interface

Creates/deletes a RIP interface. Routing is enabled on a VLAN when you create a router port. However, to enable RIP routing, you must also configure and enable a RIP routing interface on the VLAN's IP router port.

ip rip interface {*ip_address* | *interface_name***}**

no ip rip interface {*ip_address* | *interface_name***}**

Syntax Definitions

ip_address	32-bit IP address.
interface_name	The name of the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- By default, a RIP interface is created in the disabled state. To enable RIP routing on the interface, you must enable the interface using the **ip rip interface status** command.
- You can create a RIP interface even if an IP router port has not been configured. However, RIP will not function unless an IP router port is configured with the RIP interface.
- For more information on VLANs and router ports, see Chapter 21, "VLAN Management Commands".

Examples

```
-> ip rip interface 172.22.2.115
```

Release History

Release 5.1; command was introduced.
Release 5.1.6; *interface_name* parameter added.

Related Commands

ip load rip	Loads RIP into memory. When the switch is initially configured, you must load RIP into memory before it can be enabled.
ip rip status	Enables/disables RIP routing on the switch.
ip rip interface status	Enables/disables a RIP interface.

MIB Objects

```
rip2IfConfTable
   rip2IfConfAddress
   rip2IfConfStatus
```

ip rip interface status

Enables/disables a RIP interface. By default, a RIP interface is created in the disabled state. After creating a RIP interface, you must use this command to enable the interface.

ip rip interface *ip_address* **status {enable | disable}**

Syntax Definitions

ip_address	32-bit IP address.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- You must first create a RIP interface using the **ip rip interface** command before enabling the interface.
- You can create a RIP interface even if an IP router port has not been configured. However, RIP will not function unless an IP router port is configured with the RIP interface.
- For more information on VLANs and router ports, see Chapter 21, “VLAN Management Commands”.

Examples

```
-> ip rip interface status enable
```

Release History

Release 5.1; command was introduced.

Related Commands

ip load rip	Loads RIP into memory. When the switch is initially configured, you must load RIP into memory before it can be enabled.
ip rip status	Enables/disables RIP routing on the switch.
ip rip interface	Creates/deletes a RIP interface.

MIB Objects

```
rip2IfConfTable
   rip2IfConfAddress
   rip2IfConfStatus
```

ip rip interface metric

Configures the RIP metric or cost for a specified interface. You can set priorities for routes generated by a switch by assigning a metric value to routes generated by that switch's RIP interface. For example, routes generated by a neighboring switch may have a hop count of 1. However, you can lower the priority of routes generated by that switch by increasing the metric value for routes generated by the RIP interface.

ip rip interface *ip_address* **metric** *value*

Syntax Definitions

ip_address	32-bit IP address.
value	Metric value. Valid range is 1–15.

Defaults

parameter	default
value	1

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

When you configure a metric for a RIP interface, this metric cost is added to the metric of the incoming route.

Examples

```
-> ip rip interface 172.22.2.115 metric 2
```

Release History

Release 5.1; command was introduced.

Related Commands

ip rip interface	Enables/disables RIP on a specific interface.
show ip rip peer	Displays active RIP neighbors (peers). An active peer is a switch that has sent a RIP packet within the last 180 seconds.

MIB Objects

```
rip2IfConfTable
   rip2IfConfAddress
   rip2IfConfDefaultMetric
```

ip rip interface send-version

Configures the send option for a RIP interface. This defines the type(s) of RIP packets that the interface will send.

ip rip interface *ip_address* **send-version {none | v1 | v1compatible | v2}**

Syntax Definitions

ip_address	32-bit IP address.
none	RIP packets will not be sent by the interface.
v1	Only RIPv1 packets will be sent by the interface.
v1compatible	Only RIPv2 broadcast packets (not multicast) will be sent by the interface.
v2	Only RIPv2 packets will be sent by the interface.

Defaults

parameter	default
none | v1 | v2 | v1compatible	**v2**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Using this command will override RIP default behavior.
- Other devices must be able to interpret the information provided by this command or there will not be proper routing information exchanged between the switch and other devices on the network.

Examples

```
-> ip rip interface 172.22.2.115 send-version v1
```

Release History

Release 5.1; command was introduced.

Related Commands

ip rip interface recv-version	Configures the receive option for a RIP interface.

MIB Objects

```
rip2IfConfTable
   rip2IfConfAddress
   rip2IfConfSend
```

ip rip interface recv-version

Configures the receive option for a RIP interface. This defines the type(s) of RIP packets that the interface will accept.

ip rip interface *ip_address* **recv-version {v1 | v2 | both | none}**

Syntax Definitions

ip_address	32-bit IP address.
v1	Only RIPv1 packets will be received by the interface.
v2	Only RIPv2 packets will be received by the interface.
both	Both RIPv1 and RIPv2 packets will be received by the interface.
none	Interface ignores any RIP packets received.

Defaults

parameter	default
v1 | v2 | both | none	**both**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Using this command will override RIP default behavior.
- Other devices must be able to interpret the information provided by this command or there will not be proper routing information exchanged between the switch and other devices on the network.

Examples

```
-> ip rip interface 172.22.2.115 recv-version both
```

Release History

Release 5.1; command was introduced.

Related Commands

ip rip interface send-version	Configures the send option for a RIP interface.

MIB Objects

```
rip2IfConfTable
   rip2IfConfAddress
   rip2IfConfReceive
```

ip rip force-holddowntimer

Configures the forced hold-down timer value, in seconds, that defines an amount of time during which routing information regarding better paths is suppressed. A route enters into a forced holddown state when an update packet is received that indicates the route is unreachable and when this timer is set to a non-zero value. After this timer has expired and if the value is less that 120 seconds, the route enters a holddown state for the rest of the period until the remainder of the 120 seconds has also expired. During this time the switch will accept any advertisements for better paths that are received.

ip rip force-holddowntimer *seconds*

Syntax Definitions

seconds	Forced hold-down interval. Valid range is 0–120 seconds.

Defaults

parameter	default
seconds	0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The forced holddown timer is not the same as the RIP holddown timer. The RIP holddown timer is fixed at 120 seconds and is not configurable. The forced holddown timer defines a separate interval that overlaps the holddown state. During the forced holddown timer interval, the switch will not accept *better* routes from other gateways.
- The forced holddown timer interval can become a subset of the holddown timer (120 seconds) by using this command to set a value less than 120.
- To allow the routing switch to use better routes advertised during the entire hold-down time period, leave the forced holddown timer set to the default value of 0.

Examples

```
-> ip rip force-holddowntimer 10
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip rip	Displays RIP status and general configuration parameters (e.g., force holddown timer).

MIB Objects

```
alaProtocolRip
   alaRipForceHolddownTimer
```

ip rip host-route

Specifies whether or not RIP can add host routes (routes with a 32-bit mask) to the RIP table.

ip rip host-route

no ip rip host-route

Syntax Definitions

N/A

Defaults

The default is to enable a default host route.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to prevent RIP from adding host routes to the RIP table.
- When enabled, RIPv1 will interpret an incoming route announcement that contains any 1 bits in the host portion of the IP address as a host route, implying a mask of 255.255.255.255.

Examples

```
-> ip rip host-route
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip rip routes	Displays the RIP Routing Database.

MIB Objects

```
alaProtocolRip
   alaRipHostRouteSupport
```

ip rip route-tag

Configures the route tag value for RIP routes generated by the switch.

ip rip route-tag *value*

Syntax Definitions

value	Route tag value. Valid range is 0–2147483647.

Defaults

parameter	default
value	0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Only RIPv2 supports route tags.

Example

```
-> ip rip route-tag 0
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip rip	Displays RIP status and general configuration information (e.g., route tag value).

MIB Objects

```
alaRipRedistRouteTag
```

ip rip redist status

Enables/disables redistribution of routes learned through advanced routing protocols or static and local routes into RIP. Basically, redistribution makes a non-RIP route look like a RIP route.

ip rip redist status {enable | disable}

Syntax Definitions

enable	Enables RIP redistribution.
disable	Disables RIP redistribution.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

RIP routes can also be exported for use in other protocols.

Examples

```
-> ip rip redist status enable
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip rip	Displays RIP status and general configuration information (e.g., redistribution status).
show ip rip redist	Displays the route types/protocols that are configured for RIP redistribution.

MIB Objects

```
alaProtocolRip
   alaRipRedistAdminStatus
```

ip rip redist

Configures the route types that will be redistributed into RIP. To redistribute other route types into RIP, you must define the route types that will redistributed.

ip rip redist {local | static | ospf | bgp}

no ip rip redist {local | static | ospf | bgp}

Syntax Definitions

local	Redistributes local routes into RIP.
static	Redistributes static routes into RIP.
ospf	Redistributes routes learned through OSPF into RIP.
bgp	Redistributes routes learned through BGP into RIP. This option is not supported on OmniSwitch 6600 Family switches.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

In addition to configuring a redistribution type, you must also configure a redistribution filter (**ip rip redist-filter**).

Examples

```
-> ip rip redist ospf
```

Release History

Release 5.1; command was introduced.

Related Commands

ip rip redist status	Enables/disables redistribution of routes learned through advanced routing protocols or static and local routes.
show ip rip redist	Displays the route types/protocols that are configured for RIP redistribution.

MIB Objects

```
alaRipRedistProtoTable
   alaRipRedistProtoId
   alaRipRedistProtoStatus
```

ip rip redist metric

Configures the metric value for a given route type. When redistributing routes into RIP, the metric for the redistributed route is calculated as a summation of the route's metric and the corresponding metric in the redistribution type. This is the case when the matching filter metric is 0 (the default). However, if the matching redistribution filter metric is set to a non-zero value, the redistributed route's metric is set to the filter metric. This gives better control of the metric when redistributing non-RIP routes into RIP.

ip rip redist {local | static | ospf | bgp} metric *value*

Syntax Definitions

local	Redistributes local routes into RIP.
static	Redistributes static routes into RIP.
ospf	Redistributes routes learned through OSPF into RIP.
bgp	Redistributes routes learned through BGP into RIP. This option is not supported on OmniSwitch 6600 Family switches.
value	Metric value. Valid range is 0–15.

Defaults

parameter	default
value	0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- You must configure a redistribution type (**ip rip redist**) before configuring a redistribution metric for that type.
- If you are configuring a metric value for more than one route type/protocol, you must repeat the command for each one.
- Note that if the metric calculated for the redistributed route, as described above, is *greater* than 15 (RIP_UNREACHABLE) or *greater* than the metric of an existing pure RIP route, the new route is not redistributed.

Examples

```
-> ip rip redist ospf metric 2
```

Release History

Release 5.1; command was introduced.

Related Commands

ip rip redist	Configures the route types/protocols that will be redistributed into RIP.
show ip rip redist	Displays the route types/protocols that are configured for RIP redistribution.

MIB Objects

```
alaRipRedistProtoTable
   alaRipRedistProtoId
   alaRipRedistProtoMetric
```

ip rip redist-filter

Creates/deletes a RIP redistribution filter. After configuring a redistribution route type (e.g., OSPF), you must specify what routes will be redistributed by configuring a redistribution filter. Only the specified route types to the destination specified in the filter will be redistributed into RIP.

ip rip redist-filter {local | static | ospf | bgp} *ip_address ip_mask*

no ip rip redist-filter {local | static | ospf | bgp} *ip_address ip_mask*

Syntax Definitions

local	Redistributes local routes into RIP.
static	Redistributes static routes into RIP.
ospf	Redistributes routes learned through OSPF into RIP.
bgp	Redistributes routes learned through BGP into RIP. This option is not supported on OmniSwitch 6600 Family switches.
ip_address	The destination IP address of the routes to be redistributed.
ip_mask	The subnet mask corresponding to the IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to delete a RIP filter.
- In addition to configuring a redistribution filter, you must also configure a redistribution type (**ip rip redist**).
- A network/subnetwork of 0.0.0.0. 0.0.0.0. will redistribute all routes for the configured route type.

Examples

```
-> ip rip redist-filter ospf 172.22.0.0 255.255.0.0
```

Release History

Release 5.1; command was introduced.

Related Commands

ip rip redist-filter effect	Configures a redistribution filter action.
show ip rip redist-filter	Displays currently-configured RIP redistribution filters.

MIB Objects

```
alaRipRedistRouteTable
   alaRipRedistRouteProto
   alaRipRedistRouteDest
   alaRipRedistRouteMask
   alaRipRedistRouteStatus
```

ip rip redist-filter effect

Configures the redistribution filter action for route importation to RIP. You can use the redistribution filter action feature to “fine-tune” a filter. By default, the filter action is set to allow (permit) routes that match the criteria specified in the filter to be redistributed. However, you may want to redistribute all routes to a network except routes from a particular subnet. In this case, you would “allow” all routes from the network but “deny” routes from a particular subnet.

ip rip redist-filter {local | static | ospf | bgp} *ip_address ip_mask* **effect {permit | deny}**

Syntax Definitions

local	Redistributes local routes into RIP.
static	Redistributes static routes into RIP.
ospf	Redistributes routes learned through OSPF into RIP.
bgp	Redistributes routes learned through BGP into RIP. This option is not supported on OmniSwitch 6600 Family switches.
ip_address	The destination IP address of the routes to be redistributed.
ip_mask	The subnet mask corresponding to the IP address.
permit	Permits redistribution.
deny	Denies redistribution.

Defaults

parameter	default
permit | deny	permit

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- You must first configure a redistribution type (**ip rip redist**) before configuring a filter for that type.
- By default, the filter action is set to allow routes that match the criteria specified in the filter to be redistributed.

Examples

If you were using the 172.22.0.0 network and wanted to redistribute all routes from that network except routes from subnetwork 3 you would use the following commands:

```
-> ip rip redist-filter ospf 172.22.0.0 255.255.0.0 effect permit
-> ip rip redist-filter ospf 172.22.3.0 255.255.255.0 effect deny
```

Release History

Release 5.1; command was introduced.

Related Commands

ip rip redist-filter	Creates/deletes a RIP redistribution filter.
show ip rip redist-filter	Displays currently configured RIP redistribution filters.

MIB Objects

```
alaRipRedistRouteTable
   alaRipRedistRouteProto
   alaRipRedistRouteDest
   alaRipRedistRouteMask
   alaRipRedistRouteEffect
```

ip rip redist-filter metric

Configures a metric value for the redistribution filter.

Note. When redistributing routes into RIP, the metric for the redistributed route is calculated as a summation of the route's metric and the corresponding metric in the redistribution type. This is the case when the matching filter metric is 0 (the default). However, if the matching redistribution filter metric is set to a non-zero value, the redistributed route's metric is set to the filter metric. This gives better control of the metric when redistributing non-RIP routes into RIP.

ip rip redist-filter {local | static | ospf | bgp} *ip_address ip_mask* **metric** *value*

Syntax Definitions

local	Redistributes local routes into RIP.
static	Redistributes static routes into RIP.
ospf	Redistributes routes learned through OSPF into RIP.
bgp	Redistributes routes learned through BGP into RIP. This option is not supported on OmniSwitch 6600 Family switches.
ip_address	The destination IP address of the routes to be redistributed.
ip_mask	The subnet mask corresponding to the IP address.
value	Metric value. Valid range is 0–15.

Defaults

parameter	default
value	0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- You must first configure a redistribution type (**ip rip redist**) before configuring a filter for that type.
- If you are configuring a metric value for more than one route type/protocol, you must repeat the command for each one.
- Note that if the metric calculated for the redistributed route, as described above, is *greater* than 15 (RIP_UNREACHABLE) or *greater* than the metric of an existing pure RIP route, the new route is not redistributed.

Examples

```
-> ip rip redist-filter metric ospf 172.22.0.0 255.255.0.0 metric 2
```

Release History

Release 5.1; command was introduced.

Related Commands

ip rip redist-filter	Creates/deletes a RIP redistribution filter.
ip rip redist-filter effect	Configures the redistribution filter action.
show ip rip redist-filter	Displays currently configured RIP redistribution filters.

MIB Objects

```
alaRipRedistRouteTable
   alaRipRedistRouteProto
   alaRipRedistRouteDest
   alaRipRedistRouteMask
   alaRipRedistRouteMetric
```

ip rip redist-filter route-tag

Configures the route tag value for the redistribution filter. The redistribution route tag specifies the route tag with which routes matching a filter are redistributed into RIP.

ip rip redist-filter {local | static | osplf | bgp} *ip_address ip_mask* **route-tag** *value*

Syntax Definitions

local	Redistributes local routes into RIP.
static	Redistributes static routes into RIP.
ospf	Redistributes routes learned through OSPF into RIP.
bgp	Redistributes routes learned through BGP into RIP. This option is not supported on OmniSwitch 6600 Family switches.
ip_address	The destination IP address of the routes to be redistributed.
ip_mask	The mask corresponding to the IP address.
value	Route tag value.

Defaults

parameter	default
value	0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

The default value is zero (0), which means that the route tag used will be the one in the route, if specified.

Examples

```
-> ip rip redist-filter ospf 172.22.0.0 255.255.0.0 route-tag 1
```

Release History

Release 5.1; command was introduced.

Related Commands

ip rip redist-filter	Creates/deletes a RIP redistribution filter.
ip rip redist-filter effect	Configures the redistribution filter action.
show ip rip redist-filter	Displays currently-configured RIP redistribution filters.

MIB Objects

```
alaRipRedistRouteTagMatch
```

ip rip redist-filter redist-control

Configures the route control action for a redistribution filter. This controls the manner in which routes are redistributed into RIP. In certain cases, the specified route to be filtered will be either an aggregate route or a subnet. In these cases, the route may be comprised of several routes. It is possible to redistribute these routes separately or not using this command.

ip rip redist-filter {local | static | ospf | bgp} *ip_address ip_mask* **redist-control {all-subnets | aggregate | no-subnets}**

Syntax Definitions

local	Redistributes local routes into RIP.
static	Redistributes static routes into RIP.
ospf	Redistributes routes learned through OSPF into RIP.
bgp	Redistributes routes learned through BGP into RIP. This option is not supported on OmniSwitch 6600 Family switches.
ip_address	The destination IP address of the routes to be redistributed.
ip_mask	The subnet mask corresponding to the IP address.
all-subnets	Redistributes all subnet routes that match this filter, if permitted.
aggregate	Redistributes an aggregate route if there are one or more routes that match this filter.
no-subnets	Redistributes only those routes that exactly match the redistribution filter.

Defaults

parameter	default
all-subnets | aggregate | no-subnets	all-subnets

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- You must first configure a redistribution type (**ip rip redist**) before configuring a filter for that type.
- By default, filters are set to allow subnet routes to be advertised. If this is the filter action desired, it is not necessary to set an action for the filter.

Examples

```
-> ip rip redist-filter ospf 172.22.0.0 255.255.0.0 redist-control aggregate
```

Release History

Release 5.1; command was introduced.

Related Commands

ip rip redist-filter	Creates/deletes a RIP redistribution filter.
ip rip redist-filter effect	Configures the redistribution filter action.
show ip rip redist-filter	Displays currently configured RIP redistribution filters.

MIB Objects

```
alaRipRedistRouteTable
   alaRipRedistRouteProto
   alaRipRedistRouteDest
   alaRipRedistRouteMask
   alaRipRedistRouteControl
```

ip rip interface auth-type

Configures the type of authentication that will be used for the RIP interface. By default, there is no authentication used for RIP. However, you can configure a password for a RIP interface. To configure a password, you must first select the authentication type (simple or MD5), then configure a password.

ip rip interface *ip_address* **auth-type {none | simple | md5}**

Syntax Definitions

ip_address	32-bit IP address.
none	No authentication will be used.
simple	Simple authentication will be used.
md5	MD5 authentication will be used.

Defaults

parameter	default
none | simple	**none**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Regardless of which authentication type is used (simple or MD5), both switches on either end of a link must share the same password.

Examples

```
-> ip rip interface 172.22.2.115 auth-type none
```

Release History

Release 5.1; command was introduced.

Related Commands

ip rip interface auth-key	Configures the text string that will be used as the password for the RIP interface.

MIB Objects

```
rip2IfConfTable
   rip2IfConfAddress
   rip2IfConfAuthType
```

ip rip interface auth-key

Configures the text string that will be used as the password for the RIP interface. If you configure simple or MD5 authentication, you must configure a text string that will be used as the password for the RIP interface.

ip rip interface *ip_address* **auth-key** *string*

Syntax Definitions

ip_address	32-bit IP address.
string	16-byte text string.

Defaults

The default authentication string is a null string.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Regardless of which authentication type is used (simple or MD5), both switches on either end of a link must share the same password.

Examples

```
-> ip rip interface 172.22.2.115 auth-key nms
```

Release History

Release 5.1; command was introduced.

Related Commands

ip rip interface auth-type	Configures the type of authentication that will be used for the RIP interface.

MIB Objects

```
rip2IfConfTable
   rip2IfConfAddress
   rip2IfConfAuthKey
```

ip rip debug-type

Configures the type of RIP messages to debug. The debug feature on the switch is generally used only under the direction of a field engineer. Use this command to configure the type of RIP debug warnings (e.g., errors, warning) that will be logged.

ip rip debug-type [error] [warning] [recv] [send] [rdb] [age] [redist] [info] [setup] [time] [tm] [all]

no ip rip debug-type [error] [warning] [recv] [send] [rdb] [age] [redist] [info] [setup] [time] [tm] [all]

Syntax Definitions

error	Includes error conditions, failures, processing errors, etc.
warning	Includes general warnings, non-fatal conditions.
recv	Enables debugging in the receive flow path of the code.
send	Enables debugging in the send flow path of the code.
rdb	Debugs RIP database handling.
age	Debugs code handling database entry aging/timeouts.
redist	Debugs redistribution code.
info	Provides general information.
setup	Provides information during initialization.
time	Debugs timeout handler.
all	Enables all debug options.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to delete a debug type.
- To configure more than one debug type, you must repeat the command for each type.
- Use the **ip rip debug-level** command to set the debug level for the configured type(s).

Examples

```
-> ip rip debug-type all
```

Release History

Release 5.1; command was introduced.

Related Commands

ip rip debug-type	Configures RIP debugging level.
show ip rip debug	Displays the current RIP debug levels and types.

MIB Objects

```
alaRipLogTable
   alaRipDebugType
```

ip rip debug-level

Configures RIP debug level. You can set the level of information displayed using the **ip rip debug level** command. The lower the level, the more significant the event. For example, a level of 1 will display only the most critical problems. A level of 99 would display all of the available information for the specified debug type. It is best to use the default level of 1 unless instructed to increase the level by a field engineer. If more information is needed to debug a problem, a higher level can be selected.

ip rip debug-level *level*

Syntax Definitions

level	Debug level. Valid range is 0–255.

Defaults

parameter	default
level	1

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The debug level applies to all debug types that are configured. You cannot set different levels for each debug type.
- When the debug level is set to 0, the log is turned off.

Examples

```
-> ip rip debug-level 3
```

Release History

Release 5.1; command was introduced.

Related Commands

ip rip debug-type	Configures the type of RIP messages to debug.
show ip rip debug	Displays the current RIP debug levels and types.

MIB Objects

```
alaRipLogTable
   alaRipDebugLevel
```

show ip rip

Displays RIP status and general configuration parameters (e.g., force holddown timer).

show ip rip

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show ip rip

Status                    = Enabled
Host Route Support        = Disabled
Redistribution status     = Disabled
Route Tag                 = 0
Hold Down Timer           = 40
Log level                 = 0
```

output definitions

Status	RIP status (enabled or disabled).
Host Route Support	Host route status (enabled or disabled). Indicates whether or not RIP can add host routes (routes with a 32-bit mask) to the RIP table.
Redistribution status	Redistribution status (enabled or disabled). If enabled, routes learned through advanced routing protocols or static and local routes are redistributed into RIP routes.
Route Tag	Route tag value for RIP routes generated by the switch. Valid values are 0–2147483647.
Hold Down Timer	Holddown timer value, in seconds. Valid range is 0–120. Default is 0.
Log Level	RIP debugging level. Valid range is 0–255. Default is 0 (off).

Release History

Release 5.1; command was introduced.

Related Commands

ip rip status	Enables/disables RIP routing on the switch.
ip rip force-holddowntimer	Configures the interval during which a RIP route remains in a hold-down state.

MIB Objects

```
dispDrcRipGlobal
```

show ip rip routes

Displays the RIP routing database. The routing database contains all of the routes learned through RIP.

show ip rip routes [*ip_address ip_mask*]

Syntax Definitions

ip_address	32-bit IP address.
ip_mask	The mask corresponding to the IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

To view all rip routes, enter the basic command syntax (**show ip rip routes**). To view a specific route, enter the destination IP address and mask.

Examples

```
-> show ip rip routes

Destination      Mask            Gateway       Metric
-------------------------------------------------------
11.0.0.0        255.0.0.0       11.11.11.1      1
11.11.11.0      255.255.255.0   11.11.11.1      1
12.0.0.0        255.0.0.0       12.12.12.1      1
12.12.12.0      255.255.255.0   12.12.12.1      1
```

output definitions

Destination	Destination network IP address.
Mask	Destination network IP subnet mask.
Gateway	Gateway IP address (switch from which the destination address was learned).
Metric	Metric associated with this network. Generally, this is the RIP hop count (the number of hops from this switch to the destination switch).

Release History

Release 5.1; command was introduced.

Related Commands

ip rip host-route	Enables/disables a host route to an individual host on a network.

MIB Objects

```
dispDrcRipRoutes
```

show ip rip interface

Displays RIP interface status and configuration.

show ip rip interface [*ip_address*]

Syntax Definitions

ip_address	32-bit IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Enter an IP address to view a specific interface. Enter the basic **show ip rip interface** command to show status for all interfaces.

Examples

```
-> show ip rip interface 11.11.11.1

Interface IP Address                    = 11.11.11.1/24
Interface IP Broadcast Address          = 11.11.11.255
IP Interface Number (VLANId)            = 4
IP Interface Status                     = Up
Interface Config AuthType               = None
Interface Config AuthKey                =
Interface Config Send-Version           = v2
Interface Config Receive-Version        = both
Interface Config Default Metric         = 1
RIP Config Status                       = Active
Received Bad Packets                    = 0
Received Bad Routes                     = 0
Sent Updates                            = 8
```

output definitions

Interface IP Address	Interface IP address.
Interface IP Broadcast Address	Interface broadcast address.
IP Interface Number	Interface VLAN ID number.
IP Interface Status	Interface status (up/down).
Interface Config AuthType	The type of authentication that will be used for the RIP interface (None or Simple).
Interface Config AuthKey	If Simple authentication is used, the authentication string is displayed. If no authentication is used, the field is blank.

output definitions (continued)

Interface Config Send-Version	Interface send option (none, v1, v2, v1 compatible). Default is v2.
Interface Config Receive-Version	Interface receive option (none, v1, v2, both). Default is both.
Interface Config Default Metric	Default redistribution metric. Default is 1.
RIP Config Status	RIP status (active/inactive).
Received Bad Packets	Number of bad packets received and discarded. Normally this value is zero (0).
Received Bad Routes	Number of bad routes received and discarded. Normally this value is zero (0).
Sent Updates	Number of RIP routing table updates sent.

Release History

Release 5.1; command was introduced.

Related Commands

ip rip interface	Enables/disables RIP for a specific interface.

MIB Objects

```
dispDrcRipInterface
```

show ip rip peer

Displays active RIP neighbors (peers). An active peer is a switch that has sent a RIP packet within the last 180 seconds. If a peer does not send a RIP packet (request or response) within 180 seconds, it is aged out and will not be displayed.

show ip rip peer [*ip_address*]

Syntax Definitions

ip_address	32-bit IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show ip rip peer

                Total   Bad     Bad             Secs since
    IP Address   Recvd  Packets Routes Version  last update
----------------+------+-------+------+-------+-----------
  100.10.10.1      1      0       0      2       3
```

output definitions

IP Address	Peer IP address.
Total recvd	Total number of RIP packets received from the peer.
Bad Packets	Number of bad packets received from peer.
Bad Routes	Number of bad routes received from peer.
Version	Peer's RIP version as seen on the last packet received.
Secs since last update	Number of seconds since the last packet was received from the peer.

Release History

Release 5.1; command was introduced.

Related Commands

show ip rip interface	Displays RIP interface status and configuration.

MIB Objects

```
dispDrcRipPeer
```

show ip rip redist

Displays the route types/protocols that are configured for RIP redistribution.

show ip rip redist [local] [static] [ospf] [bgp]

Syntax Definitions

local	Displays redistribution configuration for local routes.
static	Displays redistribution configuration for static routes.
ospf	Displays redistribution configuration for OSPF routes.
bgp	Displays redistribution configuration for BGP routes. This option is not supported on OmniSwitch 6600 Family switches.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

To view all redistribution information for all protocols, enter the basic command syntax (**show ip rip redist**). To view a specific protocol type, enter the filter type.

Examples

```
-> show ip rip redist

Status:  ACT - Active    NIS - Not In Service

Protocol      Metric      Route-Tag  Status
--------------+-----------+----------+------
OSPF          4           0          ACT
```

output definitions

Protocol	Protocol from which routes are redistributed into RIP (e.g., OSPF).
Metric	Metric value. Valid range is **0–15**. Default is **0**.
Route-Tag	Route tag value. Default is **0**.
Status	Redistribution status (active/not in service).

Release History

Release 5.1; command was introduced.

Related Commands

ip rip redist status	Enables/disables redistribution of routes learned through advanced routing protocols or static and local routes
ip rip redist	Configures the route types/protocols that will be redistributed into RIP.

MIB Objects

```
alaRipRedistProtoEntry
```

show ip rip redist-filter

Displays currently configured RIP redistribution filters.

show ip rip redist-filter [local] [static] [ospf] [bgp]

Syntax Definitions

local	Displays filters configured for local routes.
static	Displays filters configured for static routes.
ospf	Displays filters configured for OSPF routes.
bgp	Displays filters configured for BGP routes. This option is not supported on OmniSwitch 6600 Family switches.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

To view redistribution filter information for all protocols, enter the basic command syntax (**show ip rip redist-filter**). To view information for a specific protocol, enter the protocol type.

Examples

```
-> show ip rip redist-filter

Control:    All-Sub - All Subnets     No-Sub - No Subnets Aggreg  - Aggregate
Permit:     Perm    - Permit          Deny   - Deny
Status:     ACT     - Active          NIS    - Not In Service

Proto   Destination           Control Permit Metric Tag   Status
-------+--------------------+-------+------+------+-----+------
OSPF    100.1.2.3/16         All-Sub  Perm    0     0     ACT
```

output definitions

Proto	Protocol from which routes are redistributed into RIP (e.g., OSPF).
Destination	Destination network.
Control	Route control action (all subnets, aggregate, no subnets).
Permit	Filter effect (permit or deny redistribution).
Metric	Metric value. Valid range is **0–15**. Default is **0**.
Tag	Route tag value. Default is **0**.
Status	Redistribution status (active/not in service).

Release History

Release 5.1; command was introduced.

Related Commands

ip rip redist-filter	Creates/deletes a RIP redistribution filter.
ip rip redist-filter effect	Configures the redistribution filter action for route importation to RIP.
ip rip redist-filter metric	Configures a metric value for the redistribution filter.
ip rip redist-filter redist-control	Configures the route control action for a redistribution filter.

MIB Objects

```
dispDrcRipRedistFilter
```

show ip rip debug

Displays the current RIP debug levels and types.

show ip rip debug

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show ip rip debug

Debug Level       = 3
Types/Sections
error             = on
warning           = on
recv              = on
send              = on
rdb               = on
age               = on
config            = on
redist            = on
info              = on
setup             = on
time              = on
```

output definitions

Debug Level	Debug level. The valid range 0–255. The default level is 0.
Types/Selections	The status of each debug type is shown here (on/off). See page 27-33 for a description of debug types.

Release History

Release 5.1; command was introduced.

Related Commands

ip rip debug-level	Configures RIP debugging level.
ip rip debug-type	Configures the type of RIP messages to debug.

MIB Objects

```
dispDrcRipDebug
```

28 IPX Commands

The Internet Packet Exchange (IPX) protocol, developed by Novell for NetWare, is a protocol used to route packets through IPX networks. IPX specifies a connectionless datagram similar to the IP packet of TCP/IP networks. An IPX network address consists of two parts: a network number and a node number. The IPX network number is assigned by the network administrator. The node number is the Media Access Control (MAC) address for a network interface in the end node.

IPX exchanges information using its own Routing Information Protocol (RIP), which sends updates every 60 seconds. NetWare also supports a Service Advertising Protocol (SAP) to allow network resources, including file and print servers, to advertise their network addresses and the services they provide. The user can also define a specific route. These routes, called static routes, have higher priority than routes learned through RIP.

IPX supports multiple encapsulation types for Ethernet:. 802.3 Raw, 802.3, Ethernet v2, and SNAP.

MIB information for the IPX commands is as follows:

Filename: AlcatelIND1IPX.mib
Module: alaIPXMIB

A summary of the available commands is listed here:

ipx routing
ipx default-route
ipx route
clear ipx route
ping ipx
ipx filter rip
ipx filter sap
ipx filter gns
ipx type-20-propagation
ipx packet-extension
ipx timers
show ipx interface
show ipx traffic
show ipx default-route
show ipx route
show ipx servers
show ipx filter
show ipx type-20-propagation
show ipx packet-extension
show ipx timers

ipx routing

Enables/disables IPX routing on the switch. When IPX routing is enabled and an IPX router port has been created for a VLAN on the switch, the switch is able to exchange routing information with external IPX routers; and hosts connected to VLANs with IPX router ports are able to communicate.

ipx routing

no ipx routing

Syntax Definitions

N/A

Defaults

IPX routing is enabled by default.

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Use the no form of the command to disable IPX routing.
- You must configure an IPX router port on a VLAN for the switch to communicate with other VLAN router ports. You can only create one IPX router port per VLAN. VLAN router ports are not active until at least one active physical port is assigned to the VLAN. See Chapter 21, "VLAN Management Commands."

Examples

```
-> ipx routing
```

Release History

Release 5.1; command was introduced.

Related Commands

show ipx route	Displays IPX routing table information.

MIB Objects

```
ipxBasicSysTable
   ipxBasicSysInstance
   ipxBasicSysExistState
```

ipx default-route

Creates/deletes an IPX default route. A default IPX route can be configured for packets destined for networks that are unknown to the switch. If RIP messages are disabled, packets can still be forwarded to a router that knows where to send them.

ipx default-route [*vlan*] *network_number* [*network_node*]

no ipx default-route [*vlan*]

Syntax Definitions

vlan	VLAN number of the destination node for the default route (valid range 0–4094).
network_number	IPX network number of the router used to reach the first hop in the default route.
network_node	IPX node number of the router used to reach the first hop in the default route in hexadecimal format (xx:xx:xx:xx:xx:xx). This is only required if the network number is directly connected to the switch.

Defaults

parameter	default
network_number	00000000
network_node	00:00:00:00:00:00

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- To delete a default route, use the **no** form of the command. To delete a default route to specific VLAN, enter the VLAN number. To delete a default route to a specific network, enter the network number.
- If fewer than eight hex digits are entered for an IPX network number, the entry is automatically prefixed with zeros to equal eight digits. For example, if you enter IPX network number 222, the leading zeros are automatically added to the number (e.g., 00000222).
- To create a default route to a specific VLAN, enter the VLAN number (e.g., **ipx default-route 10**).
- The network node number is the physical address assigned to the interface board that connects the device to the network.
- IPX requires the node number to be unique only within the same IPX network. For example, a node on network FEDCBA98 can use the number 1A2B3C5D7E9F, and a node on network 1234567D can also use the number 1A2B3C5D7E9F. Because each node has a different network number, IPX recognizes each node as having a legitimate, unique address.

Examples

```
-> ipx default-route 222 00:20:da:99:88:77
```

Release History

Release 5.1; command was introduced.

Related Commands

show ipx default-route	Displays IPX default route(s).

MIB Objects

```
alaIpxDefRouteTable
   alaIpxDefRouteVlanId
   alaIpxDefRouteNet
   alaIpxDefRouteNode
   alaIpxDefRouteRowStatus
```

ipx route

Creates/deletes an IPX static route. A static route enables you to send traffic to a router other than those learned through routing protocols. Static routes have higher priority than routes learned through RIP.

ipx route *network_number next_hop_network next_hop_node* [*hop_count*] [*delay*]

no ipx route *network_number*

Syntax Definitions

network_number	IPX network number of the static route's destination.
next_hop_network	IPX network number of the router used to reach the first hop in the static route.
next_hop_node	IPX node number of the router used to reach the first hop in the static route in hexadecimal format (xx:xx:xx:xx:xx:xx).
hop_count	Number of hops to the destination node.
delay	Delay, in ticks, to reach the route's destination. One clock tick is the equivalent to 1/18 of a second (approximately 55 ms).

Defaults

parameter	default
next_hop_network	00000000
next_hop_node	00:00:00:00:00:00
hop-count	0
delay	0

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- If fewer than eight hex digits are entered for an IPX network number, the entry is automatically prefixed with zeros to equal eight digits. For example, if you enter IPX network number 222, the leading zeros are automatically added to the number (e.g., 00000222).
- The amount of time is takes a packet to arrive at another IPX network segment is expressed, in ticks, as the static route's path cost. Path cost refers to the network path preference assigned to the static route. This parameter is used to advertise the static route to other RIP routers.
- Static routes do not age out of the routing tables; however, they can be deleted.
- To delete a static route you only need to enter the network number of the destination node.
- The network node number is the physical address assigned to the interface board that connects the device to the network.

- IPX requires the node number to be unique only within the same IPX network. For example, a node on network FEDCBA98 can use the number 1A2B3C5D7E9F, and a node on network 1234567D can also use the number 1A2B3C5D7E9F. Because each node has a different network number, IPX recognizes each node as having a legitimate, unique address.

Examples

```
-> no ipx route 222
```

Release History

Release 5.1; command was introduced.

Related Commands

show ipx route	Displays IPX routing table information.

MIB Objects

```
alaIpxStaticRouteTable
   alaIpxStaticRouteNetNum
   alaIpxStaticRouteNextHopNet
   alaIpxStaticRouteNextHopNode
   alaIpxStaticRouteHopCount
   alaIpxStaticRouteTicks
   alaIpxStaticRouteRowStatus
```

clear ipx route

Flushes the IPX Routing Information Protocol (RIP) Routing and/or Service Address Protocol (SAP) Bindary Tables. RIP Routing Tables are used to keep track of optimal destinations to remote IPX networks. The SAP Bindary Table contains information about available network services. NetWare workstations use SAP to obtain the network addresses of NetWare servers. IPX routers use SAP to gather service information and then share it with other IPX routers. The RIP Table and SAP Bindery Table can contain a maximum of 2,000 entries each. This number includes configured VLAN routes.

clear ipx route {rip | sap | all}

Syntax Definitions

rip	Flushes all RIP routes from the RIP Routing Table.
sap	Flushes all SAP routes from the SAP Bindary Table.
all	Flushes both the RIP Routing and SAP Bindary Tables.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- When you flush the table(s) only routes learned by RIP and SAP are deleted. Static routes are not removed. Use the **no** form of the **ipx route** command to delete a static route.
- After the routes are cleared, the switch begins soliciting RIPs and SAPs from adjacent routers and RIP and SAP information is re-learned.

Examples

```
-> clear ipx route all
```

Release History

Release 5.1; command was introduced.

Related Commands

show ipx route	Displays IPX routing table information.
show ipx servers	Displays the servers in the SAP Bindary Table, sorted by server name.

MIB Objects

```
alaIpxRoutingGroup
   alaIpxFlush
```

ping ipx

Pings an IPX node to test its reachability. The software supports two different types of IPX pings: Novell— used to test the reachability of NetWare servers currently running the NetWare Loadable Module called IPXRTR.NLM; and **alcatel**—used to test the reachability of Alcatel switches on which IPX routing has been enabled.

ping ipx *network_number network_node* [**count** *packets*] [**size** *bytes*] [**timeout** *seconds*] [**type** *packet_type*]

Syntax Definitions

network_number	Network of the node you want to ping.
network_node	Node you want to ping in hexadecimal format (xx:xx:xx:xx:xx:xx).
packets	Number of ping messages (packets) to send.
bytes	Message packet size, in bytes. Valid range is 1–8192 (1–1492 for Ethernet)
seconds	Number of seconds in which a response must be returned (0 = infinite).
packet_type	Packet type (**novell** or **alcatel**).

Defaults

parameter	default
packets	5
bytes	64
seconds	1
packet_type	novell

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- When entering the network number you only need to enter the necessary characters and the system will backfill the remainder of the number format.
- Use the basic command to send a default packet. The packet will use the default parameters for count, size, timeout, and type.
- Use the **novell** packet type to test the reachability of NetWare servers running the NetWare Loadable Module (IPXRTR.NLM). This type cannot be used to reach NetWare workstations running IPXODI. Novell uses a unique type of ping for this purpose (implemented by their IPXPNG.EXE program) which is not currently supported by the switch software. Other vendors' switches may respond to this type of ping.

- Use the **alcatel** packet type to test the reachability of Alcatel switches on which IPX routing is enabled.
- Alcatel switches respond to either ping type.

Examples

```
-> ping ipx 304 00:20:da:05:16:94
```

Release History

Release 5.1; command was introduced.

Related Commands

show ipx servers	Displays the servers in the SAP Bindary Table, sorted by server name.

MIB Objects

```
alaIpxDefRouteTable
   alaIpxDefRouteNode
alaIpxStaticRouteTable
   alaIpxStaticRouteNextHopNode
```

ipx filter rip

Creates/deletes an IPX RIP filter. IPX RIP filters allow you to minimize the number of entries put in the IPX RIP Routing Table. RIP filters work only on switches running the RIP protocol. They do not work for routers running the NLSP protocol.

ipx filter [*vlan*] **rip {in | out} {allow | block}** [*network_number* [**mask** *network_mask*]]

no ipx filter [*vlan*] **rip {in | out} {allow | block}** [*network_number* [**mask** *network_mask*]]

Syntax Definitions

vlan	To apply the filter to a specific VLAN or delete a filter from a specific VLAN, enter the VLAN number.
in	Filters incoming RIP updates.
out	Filters outgoing RIP updates.
allow	Allows the traffic specified in the filter.
block	Blocks the traffic specified in the filter.
network_number	To apply the filter to a specific network or delete a filter from a specific network, enter the IPX network number.
network_mask	If you are configuring a specific network as described above, enter the network mask.

Defaults

parameter	default
vlan	0
allow | block	allow
network_number	00000000
network_mask	ffffffff

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to delete a RIP filter.
- To apply a global filter, use only the basic command syntax (e.g., **ipx filter rip in allow**). Do not enter the optional *vlan*, *network*, or *network_mask* parameters.
- If you do not enter a network number, the filter will be applied to all networks.
- Use RIP filters with care because they can partition a physical network into two or more segments.

- The default setting for all filters is to allow traffic. Therefore, you will typically only have to define a filter to block traffic. However, defining a filter to allow certain traffic may be useful in situations where a more generic filter has been defined to block the majority of the traffic.

Examples

```
-> ipx filter rip in block
```

Release History

Release 5.1; command was introduced.

Related Commands

show ipx filter	Displays the current IPX RIP, SAP, and GNS filters.

MIB Objects

```
alaIpxRipSapFilterTable
   alaIpxRipSapFilterVlanId
   alaIpxRipSapFilterType
   alaIpxRipSapFilterNet
   alaIpxRipSapFilterNetMask
   alaIpxRipSapFilterNode
   alaIpxRipSapFilterNodeMask
   alaIpxRipSapFilterSvcType
   alaIpxRipSapFilterMode
   alaIpxRipSapFilterRowStatus
```

ipx filter sap

Creates/deletes an IPX SAP filter. IPX SAP filters allow you to minimize the number of entries put in the IPX SAP Bindery Table. SAP input filters control the SAP updates received by the switch prior to a switch accepting information about a service. The switch will filter all incoming service advertisements received before accepting information about a service. SAP output filters control which services are included in SAP updates sent by the switch.

ipx filter [*vlan*] **sap {all |** *sap_type***} {in | out} {allow | block}** [*network_number* [**mask** *network_mask*] [*network_node* [**mask** *node_mask*]]]

no ipx filter [*vlan*] **sap {all |** *sap_type***} {in | out} {allow | block}** [*network_number* [**mask** *network_mask*] [*network_node* [**mask** *node_mask*]]]

Syntax Definitions

vlan	To apply the filter to a specific VLAN or delete a filter from a specific VLAN, enter the VLAN number.
all	Enter **all** to include all SAP filters.
sap_type	To configure a specific SAP filter, enter the 4-digit hex SAP filter type as defined by NetWare.
in	Filters incoming traffic.
out	Filters outgoing traffic.
allow	Allows the traffic specified in the filter.
block	Blocks the traffic specified in the filter.
network_number	To apply the filter to a specific network or delete a filter from a specific network, enter the IPX network number.
network_mask	If you are configuring a specific network, enter the network mask.
network_node	To apply the filter to a specific network node or delete a filter from a specific network node, enter the network node number. (You must also enter a network number and network mask as described above.)
node_mask	If you are configuring a specific node, enter the node mask.

Defaults

parameter	default
vlan	0
allow | block	allow
network_number	00000000
network_mask	ffffffff
network_node	00:00:00:00:00:00
node_mask	00:00:00:00:00:00

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to delete a SAP filter.
- To apply a global filter, use only the basic command syntax (e.g., **ipx filter sap all in allow**). Do not enter the optional *vlan*, *network*, *network_mask*, *network_node*, or *node_mask* parameters.
- If you do not enter a network number, the filter will be applied to all networks.
- If you do not enter a node number, the filter will be applied to all nodes of the specified network.
- The network node number is the physical address assigned to the interface board that connects the device to the network.

Examples

```
-> ipx filter sap 0004 in block
```

Release History

Release 5.1; command was introduced.

Related Commands

show ipx filter	Displays the current IPX RIP, SAP, and GNS filters.

MIB Objects

```
alaIpxRipSapFilterTable
   alaIpxRipSapFilterVlanId
   alaIpxRipSapFilterType
   alaIpxRipSapFilterNet
   alaIpxRipSapFilterNetMask
   alaIpxRipSapFilterNode
   alaIpxRipSapFilterNodeMask
   alaIpxRipSapFilterSvcType
   alaIpxRipSapFilterMode
   alaIpxRipSapFilterRowStatus
```

ipx filter gns

Creates/deletes an IPX Get Next Server (GNS) filter. GNS output filters control which servers are included in the GNS responses sent by the router. GNS supports output filters only.

ipx filter [*vlan*] **gns {all |** *gns_type***} out {allow | block}** [*network_number* [**mask** *network_mask*] [*network_node* [**mask** *node_mask*]]]

no ipx filter [*vlan*] **gns {all |** *gns_type***} out {allow | block}** [*network_number* [**mask** *network_mask*] [*network_node* [**mask** *node_mask*]]]

Syntax Definitions

vlan	To apply the filter to a specific VLAN or delete a filter from a specific VLAN, enter the VLAN number.
all	Enter **all** to include all GNS filters.
gns_type	To configure a specific SAP filter, enter the 4-digit hex GNS filter type as defined by NetWare.
out	Optional command syntax. GNS supports output filters only.
allow	Allows the traffic specified in the filter.
block	Blocks the traffic specified in the filter.
network_number	To apply the filter to a specific network or delete a filter from a specific network, enter the IPX network number.
network_mask	If you are configuring a specific network, enter the network mask.
network_node	To apply the filter to a specific network node or delete a filter from a specific network node, enter the network node number. (You must also enter a network number and network mask as described above.)
node_mask	If you are configuring a specific node, enter the node mask.

Defaults

parameter	default
vlan	0
allow | block	allow
network_number	00000000
network_mask	ffffffff
network_node	00:00:00:00:00:00
node_mask	00:00:00:00:00:00

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to delete a GNS filter.
- To apply a global filter, use only the basic command syntax (e.g., **ipx filter gns all allow**). Do not enter the optional *vlan*, *network*, *network_mask*, *network_node*, or *node_mask* parameters.
- If you do not enter a network number, the filter will be applied to all networks.
- If you do not enter a node number, the filter will be applied to all nodes of the specified network.
- The network node number is the physical address assigned to the interface board that connects the device to the network.

Examples

```
-> ipx filter gns all block
```

Release History

Release 5.1; command was introduced.

Related Commands

show ipx filter	Displays the current IPX RIP and SAP filters.

MIB Objects

```
alaIpxRipSapFilterTable
   alaIpxRipSapFilterVlanId
   alaIpxRipSapFilterType
   alaIpxRipSapFilterNet
   alaIpxRipSapFilterNetMask
   alaIpxRipSapFilterNode
   alaIpxRipSapFilterNodeMask
   alaIpxRipSapFilterSvcType
   alaIpxRipSapFilterMode
   alaIpxRipSapFilterRowStatus
```

ipx type-20-propagation

Enables/disables Type 20 packet forwarding. Type 20 is an IPX packet type that refers to any propagated packet. If Type 20 packet forwarding is enabled on the switch, the switch receives and propagates type 20 packets through all its interfaces. If Type 20 packet forwarding is disabled on the switch, the switch discards, rather than propagates, any Type 20 packet it receives.

ipx type-20-propagation [*vlan*] **{enable | disable}**

no ipx type-20-propagation [*vlan*]

Syntax Definitions

vlan	To enable/disable Type 20 packet forwarding on a specific VLAN, enter the VLAN number.
enable	Enables Type 20 packet forwarding.
disable	Disables Type 20 packet forwarding.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to disable Type 20 packet forwarding.
- To enable/disable Type 20 packet forwarding on all VLANs, use only the basic command syntax (e.g., **ipx type-20-propagation enable**). Do not enter the optional *vlan* parameter.
- If Type 20 packet forwarding is enabled it may cause problems with highly redundant IPX networks by causing what appears to be a broadcast storm.

Examples

```
-> ipx type-20-propagation enable
```

Release History

Release 5.1; command was introduced.

Related Commands

show ipx type-20-propagation	Displays the current status of Type 20 packet forwarding.

MIB Objects

```
alaIpxType20Table
   alaIpxType20VlanId
   alaIpxType20Mode
   alaIpxType20RowStatus
```

ipx packet-extension

Enables/disables extended RIP/SAP packets. Larger RIP and SAP packets can be transmitted to reduce network congestion. RIP packets can contain up to 68 network entries. SAP packets can contain up to 8 network entries. Extended RIP and SAP packets are disabled by default.

ipx packet-extension [*vlan*] **{enable | disable}**

no ipx packet-extension [*vlan*]

Syntax Definitions

vlan	To enable/disable extended RIP/SAP packets on a specific VLAN, enter the VLAN number.
enable	Enables extended RIP/SAP packets.
disable	Disables extended RIP/SAP packets.

Defaults

parameter	default
enable | **disable**	disable

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to disable extended RIP/SAP packets.
- To enable/disable extended RIP/SAP packets on all VLANs, use only the basic command syntax (e.g., **ipx packet-extension enable**). Do not enter the optional *vlan* parameter.
- Transmitting larger RIP and SAP packets reduces network congestion; however, other switches and routers in the network must support a larger, or extended, packet sizes if this feature is configured on the switch.

Examples

```
-> ipx packet-extension
```

Release History

Release 5.1; command was introduced.

Related Commands

show ipx packet-extension	Displays the current status of extended RIP and SAP packets.

MIB Objects

```
alaIpxExtMsgTable
   alaIpxExtMsgVlanId
   alaIpxExtMsgMode
   alaIpxExtMsgRowStatus
```

ipx timers

Configures the frequency of RIP/SAP updates. RIP and SAP are the routing and service advertising protocols traditionally used by NetWare systems to exchange route and service information on an IPX network. By default, RIP and SAP packets are broadcast every 60 seconds, even if no change has occurred anywhere in a route or service. This command allows you to control how often a router broadcasts these updates.

ipx timers [*vlan*] *rip_timer sap_timer*

no ipx timers [*vlan*]

Syntax Definitions

vlan	To configure the IPX timer on a specific VLAN, enter the VLAN number.
rip_timer	RIP timer value, in seconds (valid range 1–180).
sap_timer	SAP timer value, in seconds (valid range 1–180).

Defaults

parameter	default
rip_timer	60
sap_timer	60

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to return the timers to the default value of 60.
- To configure the IPX timer on all VLANs, use only the basic command syntax (e.g., **ipx timers 60 60**). Do not enter the optional *vlan* parameter.
- You must set both timer values at the same time (e.g., **ipx timers 120 60**).
- A reduced interval may impact switch performance.

Examples

```
-> ipx timers 120 60
```

Release History

Release 5.1; command was introduced.

Related Commands

show ipx timers	Displays the current RIP and SAP timer values.

MIB Objects

```
alaIpxTimerTable
   alaIpxTimerVlanId
   alaIpxTimerSap
   alaIpxTimerRip
   alaIpxTimerRowStatus
```

show ipx interface

Displays current IPX configuration information.

show ipx interface [*vlan*]

Syntax Definitions

vlan	VLAN that you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- To display IPX information for all VLANs use only the basic command syntax (e.g., **show ipx interface**). Do not enter the optional *vlan* parameter.
- This command is only functional if RIP is enabled on an IPX VLAN interface.

Examples

```
-> show ipx interface

VLAN  State         Address                    Encapsulation
----  ------------ -------------------------- -------------
   4  active       00000020.00d0956a7ca2      ETHERNET2
   5  active       00000040.00d0956a7ca2      NOVELL
```

output definitions

VLAN	VLAN number.
State	VLAN status (up/down, active/inactive).
Address	Interface IPX address.
Encapsulation	Type of port encapsulation used for the interface (Ethernet, FDDI, Token Ring).

```
-> show ipx interface 4

VLAN 4 is up, line is inactive
IPX address is 00000020.00d0956a7ca2
Encapsulation ETHERNET2
Delay of this Novell network, in ticks is 1
WAN processing not enabled on this interface.
IPX RIP update interval is 60 seconds
IPX SAP update interval is 60 seconds
RIP/SAP mode is active
RIP Input filter list is not set
RIP Output filter list is not set
SAP Input filter list is not set
SAP Output filter list is not set
SAP GNS filter list is not set
Extended packets is not set
Type 20 packets is not set
Default route is not set
state changes    = 1    CMM Routed pkts = 0
Type 20 pkts rcvd = 0    Broadcast pkts rcvd = 0
RIP is ON: sent = 0  rcvd = 999, update interval = 60 secs.
SAP is ON: sent = 0  rcvd = 1, update interval = 60 secs.
```

output definitions

VLAN	Displays VLAN status (Up/Down).
IPX address	IPX address of the interface (network and node).
Encapsulation	Type of port encapsulation used for the interface (e.g., Ethernet, FDDI, Token Ring, SNAP, Ethernet 2).
Delay	Delay, in ticks, to reach the route's destination.
WAN processing	WAN processing is not available.
IPX RIP update interval	RIP update timer interval for the interface.
IPX SAP update interval	SAP update timer interval for the interface.
RIP/SAP mode	RIP/SAP state (active/inactive).
RIP input filter list	Indicates whether or not RIP input filters are configured (**set** indicates that RIP input filters are configured; **not set** indicates RIP input filters are not configured).
RIP output filter list	Indicates whether or not RIP output filters are configured (**set** indicates that RIP output filters are configured; **not set** indicates RIP output filters are not configured).
SAP input filter list	Indicates whether or not SAP input filters are configured (**set** indicates that SAP input filters are configured; **not set** indicates SAP input filters are not configured).
SAP output filter list	Indicates whether or not SAP output filters are configured (**set** indicates that SAP output filters are configured; **not set** indicates SAP output filters are not configured).
SAP GNS filter list	Indicates whether or GNS filters are configured (**set**).
Extended packets	State of IPX packet extension feature (**set** indicates that packet extension is enabled, **not set** indicates packet extension is disabled).
Type 20 packets	State of IPX Type 20 propagation (**set** indicates that Type 20 propagation is enabled; **not set** indicates Type 20 propagation is not enabled).

output definitions (continued)

Default route	IPX default route. If a default route is configured for the interface, the route number will appear. If not, the status is “not set”.
state changes	Number of state changes that have occurred on this interface (up to down, down to up).
CMM routed packets	Number of packets routed by the CMM(s).
Type 20 pkts rcvd	Number of Type 20 packets received.
Broadcast pkts rcvd	Number of RIP/SAP broadcast packets received.
RIP	RIP state (ON or OFF) and number of RIP packets sent/received.
sent	Number of RIP packets sent.
rcvd	Number of RIP packets received.
update interval	Frequency of RIP updates (default is 60 seconds).
SAP	SAP state (ON or OFF) and number of SAP packets sent/received.
sent	Number of SAP packets sent.
rcvd	Number of SAP packets received.
update interval	Frequency of SAP updates (default is 60 seconds).

Release History

Release 5.1; command was introduced.

Related Commands

ipx filter rip	Creates/deletes an IPX RIP filter.
ipx filter sap	Creates/deletes an IPX SAP filter.
ipx filter gns	Creates/deletes an IPX GNS filter.
ipx type-20-propagation	Enables/disables Type 20 packet forwarding.
ipx packet-extension	Enables/disables extended RIP/SAP packets.
ipx timers	Configures the frequency of RIP/SAP updates.

MIB Objects

```
alaIpxType20Table
   alaIpxType20VlanId
   alaIpxType20Mode
   alaIpxType20RowStatus
alaIpxTimerTable
   alaIpxTimerVlanId
   alaIpxTimerRip
   alaIpxTimerSap
   alaIpxTimerRowStatus
alaIpxRipSapFilterTable
   alaIpxRipSapFilterVlanId
   alaIpxRipSapFilterType
   alaIpxRipSapFilterNet
   alaIpxRipSapFilterNetMask
   alaIpxRipSapFilterNode
   alaIpxRipSapFilterNodeMask
   alaIpxRipSapFilterSvcType
   alaIpxRipSapFilterMode
   alaIpxRipSapFilterRowStatus
```

show ipx traffic

Displays IPX routing statistics and errors.

show ipx traffic [*vlan*]

Syntax Definitions

vlan	VLAN that you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

To display IPX routing statistics and errors for all VLANs use only the basic command syntax (e.g., **show ipx traffic**). Do not enter the optional *vlan* parameter.

Examples

```
-> show ipx traffic

IPX Routing is ON                      Total     Since Last - 644
seconds
IPX Input Statistics:
  pkts rcv                    =            0              0
  pkts delivered locally      =            0              0
  pkts discarded              =            0              0
  input header errors         =            0              0
IPX Output Statistics:
  pkts generated locally      =            0              0
  pkts discarded              =            0              0
  pkts with no route found    =            0              0
  pkts with a bad checksum    =            0              0
  pkts with too many hops     =            0              0
  NETBIOS packets             =            0              0
  Forwarded packets           =            0              0
  RIP bad packets             =            0              0
  SAP bad packets             =            0              0
2 VLANs active

VLAN 4     Network 00000020  Statistics and Errors:
state changes    = 1    Software Routed pkts = 0/0
Type 20 pkts rcvd = 0/0    Broadcast pkts rcvd = 0/0
RIP is ON: sent = 1000/11  rcvd = 0/0, update interval = 60 secs.
SAP is ON: sent = 1/0  rcvd = 0/0, update interval = 60 secs.
```

```
VLAN 5     Network 00000040  Statistics and Errors:
state changes    = 1    Software Routed pkts = 0/0
Type 20 pkts rcvd = 0/0    Broadcast pkts rcvd = 0/0
RIP is ON: sent = 999/11  rcvd = 0/0, update interval = 60 secs.
SAP is ON: sent = 1/0  rcvd = 0/0, update interval = 60 secs.
```

output definitions

IPX Input Statistics	
pkts rcvd	Number of packets received.
pkts delivered locally	Number of received packets delivered to local IPX applications (RIP and SAP).
pkts discarded	Number of discarded packets.
input header errors	Number of packets discarded due to IPX packet header errors.
IPX Output Statistics	
pkts generated locally	Number of received packets forwarded that were generated by local IPX applications (RIP and SAP).
pkts discarded	Number of discarded packets.
pkts with no route found	Number of packets that could not be forwarded because a route to the destination IPX network could not be found.
pkts with a bad checksum	Number of IPX packets received with incorrect checksums.
pkts with too many hops	Number of IPX packets discarded because they exceeded the maximum hop count.
NETBIOS packets	Number of NETBIOS packets received.
Forwarded packets	Number of IPX packets forwarded.
RIP bad packets	Number incorrectly formatted RIP packets received.
SAP bad packets	Number incorrectly formatted SAP packets received.
VLANs active	Number of active IPX VLANs.
VLAN Statistics and Errors	
state changes	Number of state changes that have occurred on this interface (up to down, down to up).
Software Routed pkts	Number of packets routed through software.
Type 20 packets rcvd	Number of Type 20 packets received.
broadcast pkts rcvd	Number of RIP/SAP broadcast packets received.
RIP	RIP state (ON/OFF).
sent	Number of RIP packets sent.
rcvd	Number of RIP packets received.
update interval	Frequency of RIP updates (default is 60 seconds).
SAP	SAP state (ON/OFF).
sent	Number of SAP packets sent.
rcvd	Number of SAP packets received.
update interval	Frequency of SAP updates (default is 60 seconds).

Release History

Release 5.1; command was introduced.

Related Commands

ipx filter rip	Creates/deletes an IPX RIP filter.
ipx filter sap	Creates/deletes an IPX SAP filter.
ipx filter gns	Creates/deletes an IPX GNS filter.
ipx type-20-propagation	Enables/disables Type 20 packet forwarding.

MIB Objects

```
ipxCircTable
   ipxCircSysInstance
   ipxCircIndex
   ipxCircExistState
   ipxCircOperState
   ipxCircIfIndex
   ipxCircName
   ipxCircType
   ipxCircDialName
   ipxCircLocalMaxPacketSize
   ipxCircCompressState
   ipxCircCompressSlots
   ipxCircStaticStatus
   ipxCircCompressedSent
   ipxCircCompressedInitSent
   ipxCircCompressedRejectsSent
   ipxCircUncompressedSent
   ipxCircCompressedReceived
   ipxCircCompressedInitReceived
   ipxCircCompressedRejectsReceived
   ipxCircUncompressedReceived
   ipxCircMediaType
   ipxCircNetNumber
   ipxCircStateChanges
   ipxCircInitFails
   ipxCircDelay
   ipxCircThroughput
   ipxCircNeighRouterName
   ipxCircNeighInternalNetNum
ipxBasicSysTable
   ipxBasicSysInstance
   ipxBasicSysExistState
```

```
ipxAdvSysTable
   ipxAdvSysInstance
   ipxAdvSysMaxPathSplits
   ipxAdvSysMaxHops
   ipxAdvSysInTooManyHops
   ipxAdvSysInFiltered
   ipxAdvSysInCompressDiscards
   ipxAdvSysNETBIOSPackets
   ipxAdvSysForwPackets
   ipxAdvSysOutFiltered
   ipxAdvSysOutCompressDiscards
   ipxAdvSysCircCount
   ipxAdvSysDestCount
   ipxAdvSysServCount
```

show ipx default-route

Displays IPX default route(s).

show ipx default-route

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show ipx default-route

VLAN      Default Route
------    --------------------
110       00000120.000c45786420
global    00000010
```

output definitions

VLAN	VLAN associated with the default route.
Default Route	IPX default route number and MAC address, if applicable.

Release History

Release 5.1; command was introduced.

Related Commands

ipx default-route	Creates/deletes an IPX default route.

MIB Objects

```
alaIpxDefRouteTable
   alaIpxDefRouteVlanId
   alaIpxDefRouteNet
   alaIpxDefRouteNode
   alaIpxDefRouteRowStatus
ipxCircTable
   ipxCircSysInstance
   ipxCircIndex
   ipxCircExistState
   ipxCircOperState
   ipxCircIfIndex
   ipxCircName
   ipxCircType
   ipxCircDialName
   ipxCircLocalMaxPacketSize
   ipxCircCompressState
   ipxCircCompressSlots
   ipxCircStaticStatus
   ipxCircCompressedSent
   ipxCircCompressedInitSent
   ipxCircCompressedRejectsSent
   ipxCircUncompressedSent
   ipxCircCompressedReceived
   ipxCircCompressedInitReceived
   ipxCircCompressedRejectsReceived
   ipxCircUncompressedReceived
   ipxCircMediaType
   ipxCircNetNumber
   ipxCircStateChanges
   ipxCircInitFails
   ipxCircDelay
   ipxCircThroughput
   ipxCircNeighRouterName
   ipxCircNeighInternalNetNum
```

show ipx route

Displays IPX routing table information.

show ipx route {*network_number* | **vlan** *vlan***}**

Syntax Definitions

network_number	IPX network number.
vlan	VLAN that you want to display. Displays information on the specified VLAN only.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- When entering the network number, you only need to enter the necessary characters and the system will backfill the remainder of the number format.
- To display IPX routing table information for all networks/VLANs use only the basic command syntax (e.g., **show ipx route**).

Examples

```
-> show ipx route

Codes: C - Connected network, S - Static, R - RIP
    4 routes
Type Network   Next Hop [hops/delay]    Next Hop               VLAN
---- -------- ----------------------- ---------------------- ----
C          20 [0/1](ETHERNET_802.3),         20.00d0956a7ca2,    5
C          40 [0/1](ETHERNET_II),            40.00d0956a7ca2,    4
R        eeee [1/2]    via                   20.0020daec9e7c,    4
R    55555555 [1/3]    via                   40.0000391b790c,    5
```

output definitions

Type	Network type (connected, static, RIP).
Network	IPX network number.
Next Hop (hops/delay)	The first number in brackets is the hop count (the number of routers between this node and the destination network). The second number is the tick count (the number of ticks between this node and the destination network). If the route is directly connected, the media type is shown in parenthesis. If the route was learned through routing protocols the media type is not shown.

output definitions (continued)

Next Hop	Network node of the next hop.
VLAN	VLAN number of the next hop.

Release History

Release 5.1; command was introduced.

Related Commands

ipx route	Creates/deletes an IPX static route.
clear ipx route	Flushes the IPX RIP Routing and/or SAP Bindary Tables.

MIB Objects

```
alaIpxStaticRouteTable
   alaIpxStaticRouteNetNum
   alaIpxStaticRouteNextHopNet
   alaIpxStaticRouteNextHopNode
   alaIpxStaticRouteTicks
   alaIpxStaticRouteHopCount
   alaIpxStaticRouteRowStatus
alaIpxDefRouteTable
   alaIpxDefRouteVlanId
   alaIpxDefRouteNet
   alaIpxDefRouteNode
   alaIpxDefRouteRowStatus
```

show ipx servers

Displays the servers in the SAP Bindary Table, sorted by server name.

show ipx servers {vlan *vlan* | *server_name* | *server_type***}**

Syntax Definitions

vlan	VLAN that you want to display. Displays all servers on the specified VLAN.
server_name	Server name. Displays information on the specified server only.
server_type	Server type. Displays information on all servers of the specified type.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

To display all servers in the SAP Bindary Table, use only the basic command syntax (e.g., **show ipx servers**).

Examples

```
-> show ipx servers

7 servers
Svc  Name                            Net Address           Port Route Hops VLAN
---- ------------------------------- --------------------- ---- ----- ---- ----
0640 NMS-TEST-18                          222.00b0d062faa6:e885 [0/1]   1     1
0640 NMS-TEST-4                           222.0090271c8b5c:e885 [0/1]   1     1
0640 NMSTEST17                            222.006008c1d7c2:e885 [0/1]   1     1
044f NMSTEST17                            222.006008c1d7c2:85d8 [0/1]   1     1
044f NMSTEST28                            222.00b0d0427fe2:85d8 [0/1]   1     1
0640 NMSTEST28                            222.00b0d0427fe2:e885 [0/1]   1     1
8001 SERVER1                              222.00b0d062faf1:1329 [0/1]   1     1
```

output definitions

Svc	IPX server type as defined by Novell (e.g., 0047 is an advertising print server, 0004 is a file server).
Name	Server name.
Net Address	Server IPX network address.
Port	Port number.

output definitions (continued)

Route	Hop and tick counts. The first number is the hop count (the number of routers between this node and the destination network). The second number is the tick count (the number of ticks between this node and the destination network).
Hops	Number of routers between this node and the destination network.
VLAN	VLAN number.

Release History

Release 5.1; command was introduced.

Related Commands

ping ipx	Pings an IPX node to test its reachability.

MIB Objects

```
ipxServTable
   ipxServSysInstance
   ipxServType
   ipxServName
   ipxServProtocol
   ipxServNetNum
   ipxServNode
   ipxServSocket
   ipxServHopCount
```

show ipx filter

Displays the current IPX RIP, SAP, and GNS filters.

show ipx filter {*vlan* **| rip in | rip out | sap in | sap out | gns out | global}**

Syntax Definitions

vlan	VLAN that you want to display. Displays information on the specified VLAN only.
rip in	Displays only RIP input filters.
rip out	Displays only RIP output filters.
sap in	Displays only SAP input filters.
sap out	Displays only SAP output filters.
gns out	Displays only GNS output filters.
global	Displays only global filters.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

To display all RIP and SAP filters, use only the basic command syntax (e.g., **show ipx filter**).

Examples

```
-> show ipx filter

Vlan         Type         Net/Mask              Node/Mask         Svc Md
------------ -------- ---------------- ------------------------- ----- -
global       SAP OUT       ALL Networks                 ALL Nodes  0020 A
global       GNS OUT  00000005/ffffffff  112233445566/ffffffffffff 0007 A
```

output definitions

Vlan	VLAN that is being filtered, if applicable. Global indicates a global filter.
Type	Filter type (RIP input filter, SAP output filter).
Net/Mask	Network and corresponding mask that is being filtered. ALL Networks indicates a global filter.
Node/Mask	Node and corresponding mask that is being filtered. ALL Nodes indicates a global filter.

output definitions (continued)

Svc	Filter type (SAP and GNS filters only).
Md	Filter Mode—allow (A) or block (B).

Release History

Release 5.1; command was introduced.

Related Commands

ipx filter rip	Creates/deletes an IPX RIP filter.
ipx filter sap	Creates/deletes an IPX SAP filter.
ipx filter gns	Creates/deletes an IPX GNS filter.

MIB Objects

```
alaIpxRipSapFilterTable
   alaIpxRipSapFilterVlanId
   alaIpxRipSapFilterType
   alaIpxRipSapFilterNet
   alaIpxRipSapFilterNetMask
   alaIpxRipSapFilterNode
   alaIpxRipSapFilterNodeMask
   alaIpxRipSapFilterSvcType
   alaIpxRipSapFilterMode
   alaIpxRipSapFilterRowStatus
```

show ipx type-20-propagation

Displays the current status of Type 20 packet forwarding.

show ipx type-20-propagation

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show ipx type-20-propagation

VLAN     Type 20 Packet Forwarding
-------  -------------------------
110      Enabled
120      Enabled
```

output definitions

VLAN	VLAN on which Type 20 packet forwarding is enabled/disabled. Global indicates a global filter.
Type 20 Packet Forwarding	Type 20 packet forwarding status.

Release History

Release 5.1; command was introduced.

Related Commands

ipx type-20-propagation	Enables/disables Type 20 packet forwarding.

MIB Objects

```
alaIpxType20Table
   alaIpxType20VlanId
   alaIpxType20Mode
   alaIpxType20RowStatus
```

show ipx packet-extension

Displays the current status of extended RIP/SAP packet feature.

show ipx packet-extension

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show ipx packet-extension

VLAN   Extended RIP/SAP Packets
-----  ------------------------
110    Disabled
120    Enabled
```

output definitions

VLAN	VLAN on which packet extension is enabled/disabled. Global indicates a global filter.
Extended RIP/SAP Packets	Packet extension status.

Release History

Release 5.1; command was introduced.

Related Commands

ipx packet-extension	Enables/disables extended RIP/SAP packets.

MIB Objects

```
alaIpxExtMsgTable
   alaIpxExtMsgVlanId
   alaIpxExtMsgMode
   alaIpxExtMsgRowStatus
```

show ipx timers

Displays the current RIP and SAP timer values.

show ipx timers

Syntax Definitions

N/A

Defaults

N/A

Usage Guidelines

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Examples

```
-> show ipx timers

VLAN       RIP Timer(secs) SAP Timer(secs)
-------    --------------- ---------------
global            60             60
110               45             120
```

output definitions

VLAN	VLAN on which RIP/SAP timer is set. Global indicates a global timer setting.
RIP Timer	RIP timer value, in seconds (default is 60).
SAP Timer	SAP timer value, in seconds (default is 60).

Release History

Release 5.1; command was introduced.

Related Commands

ipx timers	Configures the frequency of RIP/SAP updates.

MIB Objects

```
alaIpxTimerTable
   alaIpxTimerVlanId
   alaIpxTimerSap
   alaIpxTimerRip
   alaIpxTimerRowStatus
```

29 VRRP Commands

The Virtual Router Redundancy Protocol (VRRP) eliminates the single point of failure in a default route environment. VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on the LAN. The VRRP router controlling the IP address associated with a virtual router is called the master router and forwards packets to that IP address. If the master router becomes unavailable, the highest priority backup router will transition to the master state.

The VRRP commands comply with RFC 2787.

MIB information is as follows:

Filename: IETF-VRRP.MIB
Module: VRRP-MIB

The VRRP CLI commands are listed here:

vrrp
vrrp ip
vrrp trap
vrrp delay
vrrp track
vrrp track-association
show vrrp
show vrrp statistics
show vrrp track
show vrrp track-association

vrrp

Configures a new VRRP virtual router or modifies an existing one. Used to enable or disable a virtual router.

vrrp *vrid vlan_id* **[enable | disable | on | off] [priority** *priority***] [preempt | no preempt] [[advertising] interval** *seconds***] [authenticate** *password* **| no authenticate]**

no vrrp *vrid vlan_id*

Syntax Definitions

vrid	The virtual router ID, in the range from 1–255 (OmniSwitch 7700, 7800, or 8800) or 1–7 (OmniSwitch 6600).
vlan_id	The VLAN on which the virtual router is configured. The VLAN must already be created and available on the switch.
enable	Enables the virtual router. A virtual router may only be enabled if an IP address is configured for the virtual router.
disable	Disables the virtual router. Cannot be combined on the same line with other parameters.
on	Alternate syntax for enabling the virtual router.
off	Alternate syntax for disabling the virtual router.
priority	The priority for this virtual router to become the master router. The range is 1 (lowest priority) to 255 (highest priority). The priority should be set to 255 only if this router is the actual owner of the virtual router's IP address.
preempt	Specifies that a higher priority router may preempt a lower priority master router.
no preempt	Specifies that a higher priority router may not preempt a lower priority master router.
seconds	The interval in seconds after which the master router will send VRRP advertisements. The advertising interval must be same for all VRRP routers configured with the same VRID.
password	A 16-character password to be used for simple text authentication of VRRP packets. The password must be same for all VRRP routers configured for this VRID. *Not supported on the OmniSwitch 6600, 7700/7800, or 8800.*
no authenticate	Specifies that VRRP packets should not be authenticated. If authentication is enabled for this virtual router, it must enabled for all VRRP routers configured with this VRID. *Not supported on the OmniSwitch 6600, 7700/7800, or 8800.*

Defaults

By default, VRRP advertisements are *not* authenticated.

parameter	default
enable | disable | on | off	**disable** (off)
priority	100
preempt | no preempt	**preempt**
seconds	1

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a virtual router from the configuration.
- Use the **vrrp ip** command to configure an IP address for the virtual router. This must be done first before the virtual router can be enabled.
- To disable the virtual router, rather than remove it, use the **disable** or **off** option. Note that **disable** or **off** cannot be used with any other optional parameter.
- A virtual router must be disabled before it may be modified.

Important information about configuring priority:

- A value of 255 indicates that the VRRP router owns the IP address, that is, that the router contains the real physical interface to which the IP address is assigned. The system automatically sets this value to 255 if it detects that this router is the IP address owner. The IP address owner will always be the master router if it is available.
- VRRP routers backing up a virtual router must use priority values from 1 to 254. The default priority value for VRRP routers backing up a virtual router is 100. If you configure more than one backup, their priority values should be different. The **preempt** or **no preempt** setting specifies whether or not a higher priority router may preempt a lower priority master router.

Examples

```
-> vrrp 23 1 priority 75
-> vrrp 23 1 enable
```

Release History

Release 5.1; command was introduced.
Release 5.1.6; authenticate parameters deprecated on the OmniSwitch 6600, 7700/7800, and 8800.

Related Commands

vrrp ip	Configures an IP address for a virtual router.
show vrrp	Displays the virtual router configuration for all virtual routers or for a particular virtual router.

MIB Objects

```
vrrpOperTable
   vrrpOperAdminState
   vrrpOperPriority
   vrrpOperPreemptMode
   vrrpOperAdvertisementinterval
   vrrpOperAuthType
   vrrpOperAuthKey
```

vrrp ip

Configures an IP address for a virtual router.

vrrp *vrid vlan_id* **ip** *ip_address*

vrrp *vrid vlan_id* **no ip** *ip_address*

Syntax Definitions

vrid	The virtual router ID, in the range from 1–255 (OmniSwitch 7700, 7800, or 8800) or 1–7 (OmniSwitch 6600).
vlan_id	The VLAN on which the virtual router is configured.
ip_address	The virtual IP address associated with the specified virtual router.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

A virtual router IP address must be configured before the virtual router can be enabled.

Examples

```
-> vrrp 1 3 ip 10.10.3.2
-> vrrp 1 3 no ip 10.10.3.2
```

Release History

Release 5.1; command was introduced.

Related Commands

vrrp	Configures a new VRRP virtual router or modifies an existing one. Used to enable to disable a virtual router.
show vrrp statistics	Displays statistics for all virtual routers configured on the switch or for a particular virtual router.

MIB Objects

```
vrrpAssoIpAddrTable
   vrrpAssoIpAddrRowStatus
```

vrrp trap

Enables or disables SNMP traps for VRRP.

vrrp trap

no vrrp trap

Syntax Definitions

N/A

Defaults

By default, SNMP traps for VRRP are enabled.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

SNMP traps must be enabled globally on the switch for VRRP traps to actually be sent.

Examples

```
-> vrrp trap
-> no vrrp trap
```

Release History

Release 5.1; command was introduced.

Related Commands

snmp trap filter	SNMP traps must be enabled with this command.

MIB Objects

```
vrrpOperations
   vrrpNotificationCntl
```

vrrp delay

Configures the amount of time allowed for routing tables to stabilize before virtual routers are started.

vrrp delay *seconds*

Syntax Definitions

seconds	The amount of time after a reboot that virtual routers will wait before they go active; the range is 0 to 180 seconds.

Defaults

parameter	default
seconds	45 seconds

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use this command to prevent loss of workstation connectivity before a virtual router becomes master.

Examples

```
-> vrrp delay 50
```

Release History

Release 5.1; command was introduced.

Related Commands

vrrp	Configures a new VRRP virtual router or modifies an existing one. Used to enable or disable a virtual router.
show vrrp	Displays the virtual router configuration for all virtual routers or for a particular virtual router.

MIB Objects

```
alaVRRPStartDelay
```

vrrp track

Creates a new tracking policy or modifies an existing tracking policy.

vrrp track *track_id* **[enable | disable] [priority** *value***] {interface** *name***} {vlan** *vlan_id* **| port** *slot/port* **| ip** *ip_address***}**

no vrrp track *track_id*

Syntax Definitions

track_id	The ID of the tracking policy; the range is 1 to 255.
enable	Enables the tracking policy.
disable	Disables the tracking policy.
value	The value to be decremented from the priority value of the virtual router monitoring this tracking policy when the operational state of the tracking policy is down.
name	The name of the IP interface that this policy will track.
vlan_id	The VLAN ID of the VLAN that this policy will track. *Not supported on the OmniSwitch 6600, 7700/7800 or* 8800.
slot/port	The slot/port number that this policy will track.
ip_address	The remote IP address that this policy will track.

Defaults

parameter	default
enable | disable	**enable**
value	25

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a tracking policy.
- Use the **disable** option to disable the tracking policy rather than remove it from the switch.

Examples

The following examples apply to configuring a tracking policy on an OmniSwitch 6600, 7700/7800, and 8800 (IP interface name is specified instead of a VLAN ID):

```
-> vrrp track 2 enable priority 50 interface Marketing
-> no vrrp track 2
```

Release History

Release 5.1; command was introduced.
Release 5.1.6; *vlan_id* parameter replaced with *name* parameter on the OmniSwitch 6600, 7700/7800, and 8800.

Related Commands

vrrp track-association	Associates a VRRP tracking policy with a virtual router.
show vrrp track	Displays information about tracking policies on the switch.

MIB Objects

```
alaVRRPTrackTable
   alaVrrpTrackId
   alaVrrpTrackState
   alaVrrpTrackAdminState
   alaVrrpTrackEntityType
   alaVrrpTrackEntityVlan
   alaVrrpTrackEntityPort
   alaVrrpTrackEntityIpAddress
   alaVrrpTrackEntityInterface
   alaVrrpTrackPriority
```

vrrp track-association

Associates a VRRP tracking policy with a virtual router.

vrrp *vrid vlan_id* **track-association** *track_id*

vrrp *vrid vlan_id* **no track-association** *track_id*

Syntax Definitions

vrid	The virtual router ID, in the range from 1–255 (OmniSwitch 7700, 7800, or 8800) or 1–7 (OmniSwitch 6600).
vlan_id	The VLAN ID of the virtual router.
track_id	The ID of the tracking policy associated with the virtual router; the range is 1 to 255.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **no** form of the command to remove a tracking policy from a virtual router.

Examples

```
-> vrrp 2 4 track-association 1
-> vrrp 2 4 no track-association 1
```

Release History

Release 5.1; command was introduced.

Related Commands

vrrp	Configures a new VRRP virtual router or modifies an existing one.
show vrrp track-association	Displays the tracking policies associated with virtual routers.

MIB Objects

```
alaVrrpAssoTrackTable
   alaVrrpAssoTrackId
```

show vrrp

Displays the virtual router configuration for all virtual routers or for a particular virtual router.

show vrrp [*vrid***]**

Syntax Definitions

vrid	The virtual router ID, in the range from 1–255 (OmniSwitch 7700, 7800, or 8800) or 1–7 (OmniSwitch 6600).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **show vrrp** command to display information about configuration parameters, which may be set through the **vrrp** command. Use the **show vrrp statistics** command to get information about VRRP packets.

Examples

```
-> show vrrp
VRRP trap generation: Enabled
VRRP startup delay: 75
                IP           Admin                                    Adv
VRID  VLAN   Address(es)    Status    Priority  AuthType  Preempt  Interval
----+ ----+ -------------+----------+----------+----------+--------+---------
  1    1   192.168.170.1   Enabled     255    SimpleText  Yes         1
           192.168.170.2
  2   15   10.2.25.254     Disabled    100    None        No          1


-> show vrrp 1
Virtual Router VRID = 1 on VLAN = 1
   Admin Status       = Enabled
   Priority           = 255
   AuthType           = SimpleText
   Preempt            = 1
   Virtual MAC        = 00-00-5E-00-01-01
   IP Address(es)
      192.168.170.1
      192.168.170.2
```

output definitions

VRRP trap generation	Whether or not VRRP trap generation is enabled or disabled; configured through the **vrrp trap** command.
VRRP startup delay	The amount of time after a reboot that virtual routers will wait before they go active; allows time for routing tables to stabilize. Configured through the **vrrp delay** command.
VRID	Virtual router identifier. Configured through the **vrrp** command.
VLAN	The VLAN associated with the VRRP instance. Configured through the **vrrp** command.
IP Address(es)	The assigned IP addresses. Configured through the **vrrp ip** command.
Admin Status	The administrative status of this virtual router instance; **enabled** allows the virtual router instance to operate; **disabled** disables the virtual router instance without deleting it.
Priority	Indicates the VRRP router's priority for the virtual router. For more information about priority, see the **vrrp** command description on page 29-2.
AuthType	Indicates the type of authentication used for VRRP exchanges between virtual routers, **SimpleText** or **None**.
Preempt	Controls whether a higher priority virtual router will preempt a lower priority master: preempt indicates that a higher priority virtual router will preempt a lower priority master; no preempt indicates that the first backup router to take over for the master will not be preempted by a virtual router with a higher priority. In either case the IP address owner will always take over it if is available.
Virtual MAC	Displays the virtual MAC address for the virtual router when the router is in the **master** state. The first 5 bytes are always 00-00-5E-00-01. The last byte indicates the VRID. This field displays N/A when the virtual router is in the **backup** or **initialize** state.
Adv Interval	Indicates the time interval, in seconds, between sending advertisement messages. Only the master router sends advertisements.

Release History

Release 5.1; command was introduced.

Related Commands

vrrp	Configures a new VRRP virtual router or modifies an existing one. Used to enable to disable a virtual router.
vrrp ip	Configures an IP address for a virtual router.
show vrrp statistics	Displays statistics for all virtual routers configured on the switch or for a particular virtual router.

MIB Objects

```
vrrpOperTable
   vrrpOperAdminState
   vrrpOperPriority
   vrrpOperPreemptMode
   vrrpOperAdvertisementinterval
   vrrpOperAuthType
   vrrpOperAuthKey
```

show vrrp statistics

Displays statistics about VRRP packets for all virtual routers configured on the switch or for a particular virtual router.

show vrrp [*vrid***] statistics**

Syntax Definitions

vrid	The virtual router ID, in the range from 1–255 (OmniSwitch 7700, 7800, or 8800) or 1–7 (OmniSwitch 6600).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **show vrrp statistics** command to display information about VRRP packets. Use the **show vrrp** command to display information about the virtual router configuration.

Examples

```
-> show vrrp statistics
Checksum   Version      VRID
 Errors     Errors      Errors
----------+-----------+---------
         0          0         0

VRID  VLAN   State          UpTime   Become Master   Adv. Rcvd
----+ ----+ -------------+----------+--------------+------------
  1      1  master           378890             1              0
  2     15  backup             4483             0          64783
  7      2  initialize            0             0              0
```

output definitions

Checksum Errors	The total number of VRRP packets received with an invalid checksum value.
Version Errors	The total number of VRRP packets received with an invalid version number.
VRID Errors	The total number of VRRP packets received with invalid VRIDs.
VRID	The virtual router identifier.
VLAN	The VLAN associated with the VRRP instance.

output definitions (continued)

State	The administrative state of the VRRP instance; **initialize** means that this instance is either disabled or a reboot occurred and the startup delay timer has not expired; **backup** means that this instance is monitoring the availability of the master router; **master** means that this instance is functioning as the master router.
UpTime	Time interval (in hundredths of a second) since this virtual router was last initialized.
Become Master	The total number of times this virtual router's state has transitioned from backup to master.
Adv. Rcvd	The total number of VRRP advertisements received by this instance.

```
-> show vrrp 1 statistics
Virtual Router VRID = 1 on VLAN = 1
   State                                = master
   UpTime (1/100th second)              = 378890
   Become master                        = 1
   Advertisement interval errors        = 0
   Password errors                      = 0
   Authentication errors                = 0
   Authentication type errors           = 0
   IP TTL errors                        = 0
   IP address list errors               = 0
   Zero priority advertisements sent    = 0
   Zero priority advertisements received  = 0
```

output definitions

VRID	The virtual router identifier.
VLAN	The VLAN associated with the VRRP instance.
State	The administrative state of the VRRP instance; **initialize** means that this instance is either disabled or a reboot occurred and the startup delay timer has not expired; **backup** means that this instance is monitoring the availability of the master router; **master** means that this instance is functioning as the master router.
UpTime	Time interval (in hundredths of a second) since this virtual router was last initialized.
Become master	The total number of times this virtual router's state has transitioned from backup to master.
Advertisements received	The total number of VRRP advertisements received by this instance.
Type errors	The total number of VRRP packets received with an invalid value in the VRRP type field.
Advertisement interval errors	The total number of VRRP packets received in which the advertisement interval was different than the one configured for the virtual router.
Password errors	The total number of VRRP packets received that did not pass the simple text password authentication check.
Authentication errors	The total number of VRRP packets received with an unknown or invalid authentication type.

output definitions (continued)

Authentication type errors	The total number of VRRP packets received in which the AuthType value was different than the one configured for the virtual router.
IP TTL errors	The total number of VRRP packets received in which the IP address list does not match the configured list for the virtual router.
IP address list errors	The total number of VRRP packets in which the IP address list does not match the configured list for the virtual router.
Zero priority advertisements sent	The total number of VRRP advertisements with a priority of 0 sent by the virtual router.
Zero priority advertisements received	The total number of VRRP advertisements with a priority of 0 received by the virtual router.

Release History

Release 5.1; command was introduced.

Related Commands

vrrp	Configures a new VRRP virtual router or modifies an existing one. Used to enable to disable a virtual router.
show vrrp	Displays the virtual router configuration for all virtual routers or for a particular virtual router.

MIB Objects

```
vrrpRouterStatsTable
   vrrpRouterChecksumErrors
   vrrpRouterVersionErrors
   vrrpRouterVrIdErrors
   vrrpStatsBecomeMaster
   vrrpStatusAuthFailures
   vrrpStatsIpTtlErrors
   vrrpStatsPriorityZeroPktsRcvd
   vrrpStatsPriorityZeroPktsSent
   vrrpStatsInvalidTypePktsRcvd
   vrrpStatsAddressListErrors
   vrrpStatsInvalidAuthType
   vrrpStatsAuthTypeMismatch
   vrrpStatsPacketLengthErrors
```

show vrrp track

Displays information about tracking policies on the switch.

show vrrp track [*track_id***]**

Syntax Definitions

track_id	The ID of the tracking policy for which you want to display information.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Enter the tracking ID to display information about a particular policy; if no tracking policy ID is entered, information for all tracking policies is displayed.

Examples

```
-> show vrrp track
Track                      Admin    Oper
 ID         Policy         State    State  Pri
-----+-----------------+----------+------+-----
   1  PORT 1/1           Enabled    Up      25
   2    192.10.150.42    Enabled    Down    25
```

output definitions

Track ID	The ID of the tracking policy.
Policy	The slot/port, IP address, or VLAN tracked by the policy.
Admin State	Whether the tracking policy is administratively enabled or disabled.
Oper State	Whether the operating state of the tracking policy is up or down.
Pri	The value to be decremented from the priority value of the virtual router monitoring this tracking policy when the operational state of the tracking policy is down.

Release History

Release 5.1; command was introduced.

Related Commands

vrrp track	Creates a new tracking policy or modifies an existing tracking policy.

MIB Objects

```
alaVRRPTrackTable
   alaVrrpTrackId
   alaVrrpTrackState
   alaVrrpTrackAdminState
   alaVrrpTrackEntityType
   alaVrrpTrackEntityVlan
   alaVrrpTrackEntityPort
   alaVrrpTrackEntityIpAddress
   alaVrrpTrackPriority
```

show vrrp track-association

Displays the tracking policies associated with virtual routers.

show vrrp [*vrid***] track-association [***track_id***]**

Syntax Definitions

vrid	The virtual router ID, in the range from 1–255 (OmniSwitch 7700, 7800, or 8800) or 1–7 (OmniSwitch 6600).
track_id	The ID of the tracking policy for which you want to display information.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

If a track ID is specified, only information about that track ID is displayed. If the virtual router ID and track ID are not specified, information about all virtual routers and their associated tracking policies is displayed.

Examples

```
-> show vrrp 2 track-association
           Conf  Cur  Track                      Admin   Oper  Track
VRID VLAN  Pri   Pri   ID        Policy          State   State  Pri
----+----+-----+-----+-----+-----------------+----------+-----+------
   2    1  100   100     1  VLAN    1           Enabled  Up       25
                         2    10.255.11.101     Enabled  Up       25
```

output definitions

VRID	The virtual router identifier.
VLAN	The VLAN ID associated with the virtual router.
Conf Pri	The priority configured for the virtual router through the **vrrp** command.
Cur Pri	The priority currently being used for the virtual router. If the tracking policy is in effect because the tracked entity is down, the current priority will be equal to the configured priority (Conf Pri) minus the tracking priority (Track Pri). Otherwise the current priority will be equal to the configured priority.
Track ID	The ID of the tracking policy.
Policy	The VLAN, IP address, or slot/port being tracked by this policy.

output definitions (continued)

Admin State	The administrative state of the tracking policy configured through the **vrrp track** command.
Oper State	Whether the tracking policy is operational (Up) or not (Down).
Track Pri	The amount to be decremented from the configured virtual router priority when the tracking policy is applied.

Release History

Release 5.1; command was introduced.

Related Commands

vrrp track-association	Associates a VRRP tracking policy with a virtual router.
vrrp track	Creates a new tracking policy or modifies an existing tracking policy.

MIB Objects

```
alaVRRPTrackTable
   alaVrrpTrackId
   alaVrrpTrackState
   alaVrrpTrackAdminState
   alaVrrpTrackEntityType
   alaVrrpTrackEntityVlan
   alaVrrpTrackEntityPort
   alaVrrpTrackEntityIpAddress
   alaVrrpTrackPriority
```

30 OSPF Commands

Open Shortest Path First routing (OSPF) is a shortest path first (SPF) or link-state protocol. OSPF is an interior gateway protocol (IGP) that distributes routing information between routers in a single autonomous system (AS). OSPF chooses the least-cost path as the best path.

Each participating router distributes its local state (i.e., the router's usable interfaces and reachable neighbors) throughout the AS by flooding. In a link-state protocol, each router maintains a database describing the entire AS topology. This database is built from the collected link state advertisements of all routers. Each multi-access network that has at least two attached routers has a designated router and a backup designated router. The designated router floods a link state advertisement for the multi-access network and has other special responsibilities.

OSPF allows collections of contiguous networks and hosts to be grouped together. A group, together with the routers having interfaces to any one of the included networks, is called an *are*a. Each area runs a separate copy of the basic link-state routing algorithm. This means that each area has its own topological database, as explained in the previous section.

Alcatel's version of OSPF complies with RFCs 1370, 1850, 2328, 2370, 3101, and 3623.

MIB information for OSPF is as follows:

Filename: AlcatelIND1DrcTm.mib
Module: ALCATEL-IND1-DRCTM-MIB

Filename: AlcatelIND1Ospf.mib
Module: ALCATEL-IND1-OSPF-MIB

Filename: IETF_OSPF.MIB
Module: OSPF-MIB

The following is a list of the commands for configuring OSPF:

Global OSPF Commands	**ip ospf status** **ip load ospf** **ip ospf asbr** **ip ospf exit-overflow-interval** **ip ospf extlsdb-limit** **ip ospf host** **ip ospf mtu-checking** **ip ospf redist-filter** **ip ospf redist status** **ip ospf redist** **ip ospf route-tag** **ip ospf spf-timer** **ip ospf virtual-link** **ip ospf neighbor** **ip ospf debug-level** **ip ospf debug-type** **show ip ospf** **show ip ospf border-routers** **show ip ospf ext-lsdb** **show ip ospf host** **show ip ospf lsdb** **show ip ospf neighbor** **show ip ospf redist-filter** **show ip ospf redist** **show ip ospf routes** **show ip ospf virtual-link** **show ip ospf virtual-neighbor** **show ip ospf debug**
OSPF Area Commands	**ip ospf area** **ip ospf area status** **ip ospf area default-metric** **ip ospf area range** **show ip ospf area** **show ip ospf area range** **show ip ospf area stub**
OSPF Interface Commands	**ip ospf interface** **ip ospf interface status** **ip ospf interface area** **ip ospf interface auth-key** **ip ospf interface auth-type** **ip ospf interface dead-interval** **ip ospf interface hello-interval** **ip ospf interface md5** **ip ospf interface md5 key** **ip ospf interface type** **ip ospf interface cost** **ip ospf interface poll-interval** **ip ospf interface priority** **ip ospf interface retrans-interval** **ip ospf interface transit-delay** **show ip ospf interface**
OSPF Graceful Restart Commands	**ip ospf restart-support** **ip ospf restart-interval** **ip ospf restart-helper status** **ip ospf restart-helper strict-lsa-checking-status** **ip ospf restart initiate** **show ip ospf restart**

ip ospf status

Enables or disables the administration status of OSPF on the router.

ip ospf status {enable | disable}

Syntax Definitions

enable	Enables OSPF.
disable	Disables OSPF.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

The OSPF protocol must be enabled for it to route traffic.

Examples

```
-> ip ospf status enable
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip ospf	Displays OSPF status and general configuration parameters.

MIB Objects

```
ospfGeneralGroup
   ospfAdminStat
```

ip load ospf

This command is used to load the OSPF software on the router.

ip load ospf

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> ip load ospf
```

Release History

Release 5.1; command was introduced.

Related Commands

N/A

MIB Objects

```
ALADRCTMCONFIG
   alaDrcTmIPOspfStatus
```

ip ospf asbr

Configures the router as an Autonomous System Border Router (ASBR). A router running multiple protocols or acting as a gateway to other exterior routers is an ASBR.

ip ospf asbr

no ip ospf asbr

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Autonomous System Border Routers (ASBRs) are routers that exchange information with routers from another autonomous system (AS).
- The **no** variant of this command removes the ASBR classification of the selected router.

Examples

```
-> ip ospf asbr
-> no ip ospf asbr
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip ospf	Displays OSPF status and general configuration parameters.

MIB Objects

```
alaProtocolOspf
   alaOspfAsBdRtr
```

ip ospf exit-overflow-interval

This command sets the overflow interval value.

ip ospf exit-overflow-interval *seconds*

Syntax Definitions

seconds	The number of seconds the router waits before attempting to leave the overflow state.

Defaults

parameter	default
seconds	0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The overflow interval is the time whereby the routing router will wait before attempting to leave the database overflow state; the interval begins upon the routing router's arrival into this state.
- When the routing router leaves the overflow state, it can once again create non-default and external link state advertisements (LSAs) for autonomous systems (AS).
- Note that the router will not leave the overflow state (until it is restarted) when the overflow interval value is set to 0.

Examples

```
-> ip ospf exit-overflow-interval 10
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip ospf	Displays OSPF status and general configuration parameters.

MIB Objects

```
ospfGeneralGroup
  ospfExitOverflowInterval
```

ip ospf extlsdb-limit

Assigns a limit to the number of External Link-State Database (LSDB) entries that can be learned.

ip ospf extlsdb-limit *limit*

Syntax Definitions

limit	The maximum number of LSDB entries allowed on the router. The accepted value is any number greater than or equal to 1. If 0 is entered, there is no limit.

Defaults

parameter	default
limit	-1

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command allows you to set a limit to the number of external LSDBs learned by the router. An external LSDB is created when the router learns a link address that exists outside of its Autonomous System (AS).
- When the limit is set, and it is exceeded, older addresses that were previously learned are removed from the routing table to make room for the new external LSDB.

Examples

```
-> ip ospf extlsdb-limit 25
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip ospf	Displays OSPF status and general configuration parameters.

MIB Objects

```
ospfGeneralGroup
   ospfExtLsdbLimit
```

ip ospf host

Creates and deletes an OSPF entry for directly attached hosts. Allows for the modification of the host parameters of Type of Service (ToS) and metric.

ip ospf host *ip_address* **tos** *tos* **[metric** *metric***]**

no ip ospf host *ip_address* **tos** *tos*

Syntax Definitions

ip_address	The 32-bit IP address in dotted decimal format of the OSPF host. See the example below for more information.
tos	The type of service (ToS) of the specified OSPF host. The valid range is 0- 15. Only ToS value 0 is supported at this time.
metric	The cost metric value assigned to the specified host. The valid range is 0 and up.

Defaults

parameter	default
metric	0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use this command when multiple paths exist to a host. The specified host must be directly attached to the router. ToS routing is the ability to make a forwarding decision based on a destination address and a desired Quality of Service (QoS). ToS routing allows link selection based on QoS when more than one path exists between a source and a destination.A metric value is the cost of all the hops necessary for a packet to reach its destination. Routers use the metric to determine the best possible path
- The **no** variant of this command removes the record of the OSPF host.

Examples

```
-> ip ospf host 172.22.2.115 tos 1 metric 10
-> no ip ospf host 172.22.2.115 tos 1
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip ospf host	Displays information on configured OSPF hosts.

MIB Objects

```
ospfHostTable
   ospfHostStatus
   ospfHostIpAddress
   ospfHostTOS
   ospfHostMetric
```

ip ospf mtu-checking

Enables or disables the use of Maximum Transfer Unit (MTU) checking. The MTU limits the size of a transmitted or received packet.

ip ospf mtu-checking

no ip ospf mtu-checking

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command is used to disable the checking for mismatch of the interface MTU while establishing a neighbor adjacency with a router MTU mismatch occurs when a router receives packets that contain a larger MTU value than that of the interface on which adjacency is being established. The interface MTU is the largest IP datagram size (in bytes) that the interface can accept.
- The **no** variant of this command disables MTU checking.

Examples

```
-> ip ospf mtu-checking
-> no ip ospf mtu-checking
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip ospf	Displays OSPF status and general configuration parameters.

MIB Objects

```
alaProtocolOspf
   alaOspfMTUCheck
```

ip ospf redist-filter

Creates or deletes an OSPF redistribution filter. Allows for modifying several preset defaults in an OSPF redistribution filter.

ip ospf redist-filter {local | static | rip | bgp} *ip_address subnet_mask* **[{[effect {permit | deny}] | [metric** *value***] | [route-tag** *tag***] | [redist-control {all-subnets | aggregate | no-subnets}]}]**

no ip ospf redist-filter {local | static | rip | bgp} *ip_address subnet_mask*

Syntax Definitions

local	Redistributes local routes into OSPF.
static	Redistributes static routes into OSPF.
rip	Redistributes routes learned through RIP into OSPF.
bgp	Redistributes routes learned through BGP into OSPF. (BGP is not supported on OmniSwitch 6600 Family switches.)
ip_address	The IP address of the filter.
subnet_mask	The mask corresponding to the IP address.
permit	Allows routes to be redistributed.
deny	Disallows routes to be redistributed.
metric	The metric value. The valid range is 1–65535.
tag	The route tag value for the redistribution filter. The assigned route tag value.
all-subnets	Redistributes all subnet routes which match this filter, if permitted.
aggregate	Redistributes an aggregate route if there are one or more routes that match this filter.
no-subnets	Redistributes only those routes that exactly match the redistribution filter.

Defaults

parameter	default
permit | deny	**permit**
metric	0
tag	0
all-subnets | aggregate | no-subnets	**all-subnets**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command sets up a filter to redistribute routes from one routing domain to another routing domain. The selected route or protocol type and an IP address/mask are the parameters of the filter. For example, if RIP and IP address 1.0.0.0 with a mask of 255.0.0.0 is the specified filter, all routes learned from RIP with an address of 1.0.0.0 and mask of 255.0.0.0 would be filtered into OSPF domain.
- The **bgp** parameter is not supported on OmniSwitch 6600 Family switches.
- By default, the filter action is set to allow routes that match the criteria specified in the filter to be redistributed. The filter can be set to deny redistribution to routes obtained from the specified learning source and IP address/mask.
- This command specifies the metric value with which routes matching this filter are redistributed into OSPF. The default value is zero (0), which means that the metric used for the redistributed route is the value specified by the OSPF redistribution metric variable.
- This command specifies the route tag with which routes matching this filter are redistributed into OSPF. The default value is zero (0), which means that the route tag used will be the one in the route, if specified.
- This command is used to control the manner in which routes are redistributed into OSPF.
- The **no** variant of this command deletes the redistribution filter previously created.

Examples

```
-> ip ospf redist-filter local 172.22.2.0 255.255.255.0
-> ip ospf redist-filter local 172.22.2.0 255.255.255.0 effect deny
-> ip ospf redist-filter local 172.22.2.0 255.255.255.0 metric 5
-> ip ospf redist-filter local 172.22.2.0 255.255.255.0 route-tag 5555
-> ip ospf redist-filter local 172.22.2.0 255.255.255.0 redist-control subnet
-> no ip ospf redist-filter local 172.22.2.0 255.255.255.0
```

Release History

Release 5.1; command was introduced.

Related Commands

ip ospf redist	Creates and deletes a redistribution instance that allows routes to be redistributed into OSPF.
ip ospf redist status	Enables or disables OSPF redistribution.
show ip ospf redist-filter	Displays OSPF redistribution filter attributes.

MIB Objects

```
alaOspfRedistRouteTable
   alaOspfRedistRouteProto
   alaOspfRedistRouteDest
   alaOspfRedistRouteMask
   alaOspfRedistRouteStatus
   alaOspfRedistRouteEffect
   alaOspfRedistRouteMetric
   alaOspfRedistRouteTagMatch
```

ip ospf redist status

Enables or disables OSPF redistribution.

ip ospf redist status {enable | disable}

Syntax Definitions

enable	Enables OSPF redistribution.
disable	Disables OSPF redistribution.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

OSPF can redistribute routes from outside the OSPF domain into OSPF by using the **ip ospf redist** command and the **ip ospf redist-filter**.

Examples

```
-> ip ospf redist status enable
```

Release History

Release 5.1; command was introduced.

Related Commands

ip ospf redist-filter	Creates/deletes a redistribution filters that allows routes to be redistributed into OSPF.
ip ospf redist	Creates/deletes a redistribution instance that allows routes to be redistributed into OSPF.
show ip ospf	Displays OSPF status and general configuration parameters.

MIB Objects

```
alaProtocolOspf
   alaOspfRedistAdminStatus
```

ip ospf redist

Creates and deletes a redistribution instance that allows routes to be redistributed into OSPF. Allows for the modification of various parameters of a redistribution instance.

ip ospf redist {local | static | rip | bgp} [metric *metric***] [metric-type {type1 | type2}] [subnets {enable | disable}]**

no ip ospf redist {local | static | rip | bgp}

Syntax Definitions

local	Redistributes local routes into OSPF.
static	Redistributes static routes into OSPF.
rip	Redistributes routes learned through RIP into OSPF.
bgp	Redistributes routes learned through BGP into OSPF. (BGP is not supported on OmniSwitch 6600 Family switches.)
metric	Configures the metric value that will be assumed on receipt of external routes. The valid range is 1–65535.
type 1	Sets the redistribution metric as Type 1 (non-OSPF).
type 2	Sets the redistribution metric as Type 2 (calculated weight value from non-OSPF protocol).
enable	Enables subnet route redistribution
disable	Disables subnet route redistribution.

Defaults

parameter	default
metric	0
type1 | type2	**type2**
enable | disable	**enable**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- When a redistribution instance for a specified non-OSPF protocol is created, it is automatically enabled.
- The **bgp** parameter is not supported on OmniSwitch 6600 Family switches.
- Creating a route distribution entry automatically enables the **ip ospf redist subnets** and **ip ospf redist metric-type** features.

- Use the **ip ospf redist status** command and the **ip ospf redist-filter** command to initiate redistribution of routes into OSPF.

Examples

```
-> ip ospf redist rip metric 15 metric-type type2 subnets disable
-> no ip ospf redist rip
```

Release History

Release 5.1; command was introduced.

Related Commands

ip ospf redist-filter	Creates/deletes a redistribution filters that allows routes to be redistributed into OSPF.
ip ospf redist status	Enables/disables OSPF redistribution.
show ip ospf redist	Displays the specified redistribution instance that allows routes to be redistributed into OSPF.

MIB Objects

```
alaOspfRedistProtoTable
   alaOspfRedistProtoId
   alaOspfRedistProtoStatus
   alaOspfRedistProtoMetric
   alaOspfRedistProtoMetricType
   alaOspfRedistProtoSubnets
```

ip ospf route-tag

Configures a tag value for Autonomous System External (ASE) routes created.

ip ospf route-tag *tag*

Syntax Definitions

tag	The set tag value. The valid range is 0–2,147,483,647.

Defaults

parameter	default
tag	0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command allows you to set a tag value for ASE routes that are learned by this OSPF router. The tag value allows for quick identification.
- OSPF ASE route advertisements contain a tag value field. This field allows the exchange of information between autonomous system border routers (ASBRs).

Examples

```
-> ip ospf route-tag 2
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip ospf	Displays OSPF status and general configuration parameters.

MIB Objects

```
alaProtocolOspf
   alaOspfRedistRouteTag
```

ip ospf spf-timer

Configures timers for Shortest Path First (SPF) calculation.

ip ospf spf-timer [delay *delay_seconds***] [hold** *hold_seconds***]**

Syntax Definitions

delay_seconds	Specifies time (from 0 to 65535 seconds) between the reception of an OSPF topology change and the start of a SPF calculation.
hold_seconds	Specifies the minimum time (from 0 to 65535 seconds) between consecutive SPF calculations.

Defaults

parameter	default
delay_seconds	5
hold_seconds	10

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command allows you to configure the time between SPF calculations. Using the delay timer, you can determine how much time to postpone an SPF calculation after the router receives a topology change. Using the hold timer, you can configure the amount of time that must elapse between consecutive SPF calculations.
- Note that if either of these values is set to 0, there will be no delay in SPF calculation. This means that SPF calculations will occur immediately upon the reception of a topology change and/or that back-to back SPF calculations can take place with no break in-between the two.

Examples

```
-> ip ospf spf-timer delay 20 hold 35
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip ospf	Displays OSPF status and general configuration parameters.

MIB Objects

```
alaProtocolOspf
   alaOspfTimerSpfDelay
   alaOspfTimerSpfHold
```

ip ospf virtual-link

Creates or deletes a virtual link. A virtual link is used to restore backbone connectivity if the backbone is not physically contiguous.

ip ospf virtual-link *area_id router_id* **[auth-type {none | simple | md5}] [auth-key** *key_string***] [dead-interval** *seconds***] [hello-interval** *seconds***] [retrans-interval** *seconds***] [transit-delay** *seconds***]**

no ip ospf virtual-link *area_id router_id*

Syntax Definitions

area_id	A unique 32-bit value in IP address format.
router_id	A unique 32-bit value, such as an IP address, that identifies a neighboring router in the Autonomous System.
none	Sets the virtual link authorization type to no authentication.
simple	Sets the virtual link authorization type to simple authentication. If **simple** is selected, a key must be specified as well.
md5	Sets the virtual link authorization type to MD5 authentication.
key_string	Sets the virtual link authorization key. The key can be up to 8 ASCII characters. See the example for more details.
dead-interval *seconds*	Sets the virtual link dead interval. If no hello packets on this link for the set number of seconds have been received, the virtual neighbor is declared dead. The valid range is 1–2147483647.
hello-interval *seconds*	Sets the virtual link hello interval, which is the time interval between OSPF hellos sent on this virtual link. The valid range is 1–65535.
retrans-interval *seconds*	Sets the virtual link retransmit interval. The router waits the set number of seconds before retransmitting OSPF packets. The valid range is 0–3600.
transit-delay *seconds*	Sets the virtual link transit delay, which is the number of seconds to transmit OSPF packets over this link. The valid range is 0–3600.

Defaults

parameter	default
none | simple | md5	none
key_string	null string
dead-interval *seconds*	40
hello-interval *seconds*	10
retrans-interval *seconds*	5
transit-delay *seconds*	1

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- It is possible to define areas in such a way that the backbone is no longer contiguous. In this case the system administrator can ensure backbone connectivity physically.
- Virtual links can be configured between any two backbone routers that have an interface to a common non-backbone area. Virtual links belong to the backbone. The protocol treats two routers joined by a virtual link as if they were connected by an unnumbered point-to-point network. The routing protocol traffic that flows along the virtual link uses intra-area routing only.
- If authentication is enabled, both routers at either end of the virtual link must share the same password. Simple authentication refers to the use of only clear-text passwords as an authentication method. MD5 authentication refers to the usage of message digests.
- The **dead-interval** value should be the same for all routers on the same network. This value should be some multiple of the value given for the hello interval.
- The **no** form of the command deletes the virtual link.

Examples

```
-> ip ospf virtual-link 0.0.0.1 172.22.2.115
-> ip ospf virtual-link 0.0.0.1 172.22.2.115 auth-key "techpubs"
-> ip ospf virtual-link 0.0.0.1 172.22.2.115 auth-type simple
-> ip ospf virtual-link 0.0.0.1 172.22.2.115 dead-interval 50
-> ip ospf virtual-link 0.0.0.1 172.22.2.115 hello-interval 20
-> ip ospf virtual-link 0.0.0.1 172.22.2.115 retrans-interval 20
-> ip ospf virtual-link 0.0.0.1 172.22.2.115 transit-delay 50
-> no ip ospf virtual-link 0.0.0.1 172.22.2.115
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip ospf virtual-link	Displays virtual link information.

MIB Objects

```
ospfVirtIfTable
   ospfVirtIfAreaId
   ospfVirtIfNeighbor
   ospfVirtIfAuthKey
   ospfVirtIfStatus
   ospfVirtIfAuthType
   ospfVirtIfRtrDeadInterval
   ospfVirtIfHelloInterval
   ospfVirtIfRetransInterval
   ospfVirtIfTransitDelay
```

ip ospf neighbor

Creates a static neighbor on a non-broadcast interface.

ip ospf neighbor *neighbor_id* **{eligible | non-eligible}**

no ip ospf neighbor *neighbor_id*

Syntax Definitions

neighbor_id	A unique 32-bit IP address identical to the neighbor's interface address.
eligible	Sets this router as eligible to be the DR.
non-eligible	Sets this router as not eligible to be the DR.

Defaults

parameter	default
eligible | non-eligible	**eligible**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- NBMA (Non Broadcast Multi Access), PMP (Point-to-Multipoint) and P2P (Point-to-Point) OSPF non-broadcast modes are supported over Ethernet interfaces (broadcast media).
- Neighboring routers on non-broadcast OSPF networks must be statically configured, because lack of OSPF multicast capabilities prevents using normal OSPF Hello protocol discovery.
- In the case of NBMA interface the static neighbor eligibility for becoming a DR can be configured while it is not necessary for point-to-multipoint and point-to-point interfaces.
- An interface connected to this neighbor must also be configured as a non-broadcast interface, which can be either point-to-multipoint or point-to-point, using the **ip ospf interface type** command.
- For the correct working of an OSPF NBMA network, a fully meshed network is mandatory. Also, the neighbor eligibility configuration for a router on every other router should match the routers interface priority configuration.

Examples

```
-> ip ospf neighbor 1.1.1.1 non-eligible
-> no ip ospf neighbor 1.1.1.1
```

Release History

Release 5.1; command was introduced.

Related Commands

ip ospf interface type	Configures the OSPF interface type.
show ip ospf neighbor	Displays information on OSPF non-virtual neighbor routers.

MIB Objects

```
ospfNbrTable
   ospfNbrPriority
   ospfNbmaNbrStatus
```

ip ospf debug-level

Configures OSPF debugging level. The level refers to the granularity of the information provided. Generally, the higher the number, the more specific the information.

ip ospf debug-level *level*

Syntax Definitions

level	The debugging level. The valid range 0–255.

Defaults

parameter	default
level	0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This command allows you to select the granularity at which you wish to view debugging information. Currently, in OSPF, there are three levels available:

- **10**–Only critical errors and warnings.
- **50**–Most errors, warnings, and events.
- **99**–All errors, warnings and events.

Examples

```
-> ip ospf debug-level 10
```

Release History

Release 5.1; command was introduced.

Related Commands

ip ospf debug-type	Configures type of OSPF functionality to debug.
show ip ospf debug	Displays current OSPF debug level and types.

MIB Objects

```
alaOspfDebugConfig
   alaOspfDebugLevel
```

ip ospf debug-type

Configures type of OSPF traffic to debug.

ip ospf debug-type [error] [warning] [state] [recv] [send] [flood] [spf] [lsdb] [rdb] [age] [vlink] [redist] [summary] [dbexch] [hello] [auth] [area] [intf] [mip] [info] [setup] [time] [tm] [restart] [helper] [all]

no ip ospf debug-type [error] [warning] [state] [recv] [send] [flood] [spf] [lsdb] [rdb] [age] [vlink] [redist] [summary] [dbexch] [hello] [auth] [area] [intf] [mip] [info] [setup] [time] [tm] [restart] [helper] [all]

Syntax Definitions

error	Administratively enables/disables debugging error messages. Error messages provide information of program faults.
warning	Administratively enables/disables debugging warning messages.
state	Administratively enables/disables debugging OSPF state messages. State messages show the switch state in relation to its neighbors.
recv	Administratively enables/disables debugging messages for packets received by OSPF.
send	Administratively enables/disables debugging messages for packets sent by OSPF.
flood	Administratively enables/disables debugging messages for the flooding of Link State Advertisements (LSAs) in OSPF.
spf	Administratively enables/disables debugging messages for OSPF's Shortest Path First (SPF) calculations.
lsdb	Administratively enables/disables debugging messages for OSPF's Link State Database (LSDB) related operations.
rdb	Administratively enables/disables debugging messages for OSPF's routing database (RDB) related operations.
age	Administratively enables/disables debugging messages for OSPF's aging process of LSAs.
vlink	Administratively enables/disables debugging messages for OSPF's virtual links operations.
redist	Administratively enables/disables debugging messages for OSPF's route redistribution process.
summary	Administratively enables/disables debugging messages for all OSPF's summarizations.
dbexch	Administratively enables/disables debugging messages for OSPF neighbors' database exchange.
hello	Administratively enables/disables debugging messages for OSPF's hello handshaking process.

auth	Administratively enables/disables debugging messages for OSPF's authentication process.
area	Administratively enables/disables debugging messages for OSPF's area events.
intf	Administratively enables/disables debugging messages for OSPF's interface operations.
mip	Administratively enables/disables debugging messages for MIP processing of OSPF specific commands.
info	Administratively enables/disables debugging messages for purpose to provide OSPF information.
setup	Administratively enables/disables debugging messages for OSPF's initialization setup.
time	Administratively enables/disables debugging messages for OSPF's time related events.
tm	Administratively enables/disables debugging messages for DRC's Task Manager communication events.
restart	Administratively enables/disables debugging messages for graceful restart events.
helper	Administratively enables/disables debugging messages for graceful helper events.
all	Administratively enables/disables all debugging listed above for OSPF.

Defaults

parameter	default
error | warning | state | recv | send | flood | spf | lsdb | rdb | age | vlink | redist | summary | dbexch | hello| auth | area | intf | mip | info | setup | time | tm | restart | helper | all	**error**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The debug command allows you to enable debugging on various OSPF functions. These messages can be highly detailed, or very general, depending upon the debug level set.
- Use the **no** form of the command to turn off the selected debugging type.

Examples

```
-> ip ospf debug-type all
-> no ip ospf debug-type all
```

Release History

Release 5.1; command was introduced.

Related Commands

ip ospf debug-level	Configures OSPF debugging level.
show ip ospf debug	Displays current OSPF debug level and types.

MIB Objects

```
alaOspfDebugConfig
   alaOspfDebugError
   alaOspfDebugWarning
   alaOspfDebugState
   alaOspfDebugRecv
   alaOspfDebugSend
   alaOspfDebugFlood
   alaOspfDebugSPF
   alaOspfDebugLsdb
   alaOspfDebugRdb
   alaOspfDebugAge
   alaOspfDebugVlink
   alaOspfDebugRedist
   alaOspfDebugSummary
   alaOspfDebugDbexch
   alaOspfDebugHello
   alaOspfDebugAuth
   alaOspfDebugArea
   alaOspfDebugIntf
   alaOspfDebugMip
   alaOspfDebugInfo
   alaOspfDebugSetup
   alaOspfDebugTime
   alaOspfDebugTm
   alaOspfDebugRestart
   alaOspfDebugHelper
   alaOspfDebugAll
```

ip ospf area

Assigns an OSPF interface to a specified area.

ip ospf area *area_id* **[summary {enable | disable}] | [type {normal | stub | nssa}]**

no ip ospf area *area_id*

Syntax Definitions

area_id	A unique 32-bit value in IP address format.
enable	Enables summarization.
disable	Disables summarization.
normal	Sets the area as a regular OSPF area.
stub	Configures an OSPF area as a stub area.
nssa	Configures an OSPF area as a Not So Stubby Area (NSSA)

Defaults

parameter	default
enable | disable	**enable**
normal | stub | nssa	**normal**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The **summary** options are used to enable or disable route summarization for stub and NSSA areas. Stub and NSSA areas will not receive LSA type 3 unless summary is enabled.
- The **type** command allows you to chose what type of area this is going to be.
- The **no** variant deletes the area.

Examples

```
-> ip ospf area 0.0.0.1
-> ip ospf area 0.0.0.1 stub
-> ip ospf area 0.0.0.1 type normal
-> no ip ospf area 0.0.0.1
```

Release History

Release 5.1; command was introduced.

Related Commands

ip ospf area default-metric	Creates or deletes an OSPF default metric.
ip ospf area range	Creates a route summarization instance whereby a range of addresses will be advertised as a single route.
show ip ospf area	Displays either all OSPF areas, or a specified OSPF area.

MIB Objects

```
ospfAreaTable
   ospfImportAsExtern
   ospfAreaSummary
   ospfAreaId
```

ip ospf area status

Enables or disables the administration status of the OSPF area.

ip ospf area *area_id* **status {enable | disable}**

Syntax Definitions

area_id	A unique 32-bit value in IP address format.
enable	Enables the OSPF area.
disable	Disables the OSPF area.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

The OSPF area must be enabled for it to perform routing. This command enables or disables the specified OSPF area.

Examples

```
-> ip ospf area 1.1.1.1 status enable
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip ospf area	Displays the status and statistics of an OSPF area.

MIB Objects

```
ospfAreaTable
  ospfAreaStatus
```

ip ospf area default-metric

Creates or deletes a default metric for stub or Not So Stubby Area (NSSA) areas. The default metric configures the type of cost metric that a default area border router (ABR) will advertise in the default summary Link State Advertisement (LSA).

ip ospf area *area_id* **default-metric** *tos* **[[cost** *cost***] | [type {ospf | type 1 | type 2}]**

no ip ospf area *area_id* **default-metric** *tos*

Syntax Definitions

area_id	A unique 32-bit value in IP address format.
tos	Type of service. The valid range is 0–15. Only ToS value 0 is supported at this time.
cost	The numerical cost of this area and ToS. Only 0 is supported in the current release.
ospf	Advertises external routes as OSPF autonomous system external (ASE) routes.
type1	Advertises external routes as a Type 1 (non-OSPF) metric.
type2	Advertises external routes as a Type 2 (calculated weight value from non-OSPF protocol) metric.

Defaults

parameter	default
tos	0
ospf | type 1 | type 2	**ospf**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The **type** command configures the type of cost metric for the specified ToS.To ensure that internal routers receiving external route advertisements choose the correct route, all border routers advertising a particular external network should be configured to advertise the route using the same metric type. That is, they must all advertise the route using an OSPF, Type 1 or Type 2 metric.
- The **no** variant deletes the default metric from the specified area.

Examples

```
-> ip ospf area 1.1.1.1 default-metric 0
-> no ip ospf area 1.1.1.1 default-metric 0
```

Release History

Release 5.1; command was introduced.

Related Commands

ip ospf area	Creates or deletes an OSPF area.
ip ospf area range	Creates a route summarization instance whereby a range of addresses will be advertised as a single route.
show ip ospf area	Displays either all OSPF areas, or a specified OSPF area.

MIB Objects

```
ospfStubAreaTable
   ospfStubAreaId
   ospfStubTOS
   ospfStubStatus
   ospfStubMetric
   ospfStubMetricType
```

ip ospf area range

Creates a route summarization instance whereby a range of addresses assigned for the route at the area border router will be advertised.

ip ospf area *area_id* **range {summary | nssa}** *ip_address subnet_mask*
[effect {admatching | noMatching}]

no ip ospf area *area_id* **range {summary | nssa}** *ip_address subnet_mask*

Syntax Definitions

area_id	A unique 32-bit value in IP address format.
summary	Advertises the address range as a summary link state advertisement (LSA).
nssa	Advertises the address range of Not So Stubby Area (NSSA) routes as a Type 5 advertisement.
ip_address	A 32-bit IP address for the range's area.
subnet_mask	A 32-bit subnet mask that determines how many bits of the IP address denote the network number.
admatching	Determines that routes specified falling within the specified range will be advertised.
noMatching	Determines that any route falling within the specified range will not be advertised.

Defaults

parameter	default
summary | nssa	**summary**
admatching | noMatching	**admatching**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Route summarization is the consolidation of addresses within an area which are advertised as a single route. When network numbers in an area are assigned consecutively, the area border router can be configured, using this command, to advertise a route that aggregates all the individual networks within the range.
- Using this command causes a single route to be advertised, for an address range in the specified area, to other areas.

- An NSSA (Not So Stubby Area) is similar to a stub area. However, where autonomous system (AS) external routes cannot be imported into a stub area, an NSSA will allow the importing of some AS external routes.
- Area ranges, once created, are enabled by default. Classless Inter-Domain Routing (CIDR) can work with OSPF to make route summarization more efficient. This is especially true for the summarization of routes in the global database. OSPF area address ranges can be configured on area border routers

Examples

```
-> ip ospf area 1.1.1.1 range summary 172.22.2.0 255.255.255.0
-> no ip ospf area 1.1.1.1 range summary 172.22.2.0 255.255.255.0
```

Release History

Release 5.1; command was introduced.

Related Commands

ip ospf area	Creates or deletes an OSPF area.
ip ospf area default-metric	Creates or deletes an OSPF default metric.
show ip ospf area range	Displays all or specified route summaries in a given area.

MIB Objects

```
ospfAreaAggregateTable
   ospfAreaAggregateAreaId
   ospfAreaAggregateLsdbType
   ospfAreaAggregateNet
   ospfAreaAggregateMask
   ospfAreaAggregateEffect
   ospfAreaAggregateStatus
```

ip ospf interface

Creates and deletes an OSPF interface.

ip ospf interface {*ip_address* | *interface_name***}**

no ip ospf interface {*ip_address* | *interface_name***}**

Syntax Definitions

ip_address	A 32-bit IP address for the interface.
interface_name	The name of the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to delete an OSPF interface.
- The interface name cannot contain spaces.

Examples

```
-> ip ospf interface 172.22.2.115
-> ip ospf interface vlan-101
-> no ip ospf interface 172.22.2.115
-> no ip ospf interface vlan-101
```

Release History

Release 5.1; command was introduced.
Release 5.1.6; *interface_name* parameter added.

Related Commands

show ip ospf interface	Displays the status and statistics of an OSPF interface.

MIB Objects

```
ospfIfTable
   ospfIfIpAddress
alaOspfIfAugTable
   alaOspfIfIntfName
```

ip ospf interface status

Enables or disables the administration status on an OSPF interface.

ip ospf interface {*ip_address* | *interface_name***} status {enable | disable}**

no ip ospf interface {*ip_address* | *interface_name***} status {enable | disable}**

Syntax Definitions

ip_address	A 32-bit IP address for the interface.
interface_name	The name of the interface.
enable	Enables the OSPF interface.
disable	Disables the OSPF interface.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The OSPF interface must be enabled for it to participate in the OSPF protocol.
- Use the **no** form of the command to delete an OSPF interface.

Examples

```
-> ip ospf interface vlan-101 status enable
-> no ip ospf interface vlan-101 status enable
-> ip ospf interface 1.1.1.1 status enable
-> no ip ospf interface 1.1.1.1 status enable
```

Release History

Release 5.1; command was introduced.
Release 5.1.6; *interface_name* parameter added.

Related Commands

show ip ospf interface	Displays the status and statistics of an OSPF interface.

MIB Objects

```
ospfIfTable
   ospfIfAdminStat
```

ip ospf interface area

Configures an OSPF area identifier for this interface.

ip ospf interface {*ip_address* | *interface_name***} area** *area_id*

Syntax Definitions

ip_address	The 32-bit IP address for the interface.
interface_name	The name of the interface.
area_id	A unique 32-bit value in IP address format.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

An interface must be assigned to an area to become operational.

Examples

```
-> ip ospf interface 172.22.2.115 area 0.0.0.1
-> ip ospf interface vlan-101 area 0.0.0.1
```

Release History

Release 5.1; command was introduced.
Release 5.1.6; *interface_name* parameter added.

Related Commands

show ip ospf area	Displays either all OSPF areas, or a specified OSPF area.
show ip ospf interface	Displays the status and statistics of an OSPF interface.

MIB Objects

```
ospfIfTable
   ospfIfAreaId
```

ip ospf interface auth-key

Configures OSPF authentication key for simple authentication on an interface.

ip ospf interface {*ip_address* | *interface_name***} auth-key** *key_string*

Syntax Definitions

ip_address	The 32-bit IP address for the interface.
interface_name	The name of the interface.
key_string	An authentication key (8 characters maximum).

Defaults

The default for the authentication key string is a null string.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Sets a password as a simple text string of 8 ASCII characters.
- Must be used in conjunction with the **auth-type** command, described on page 30-40, set to **simple**.

Examples

```
-> ip ospf interface 172.22.2.115 auth-key pass
-> ip ospf interface vlan-101 auth-key pass
```

Release History

Release 5.1; command was introduced.
Release 5.1.6; *interface_name* parameter added.

Related Commands

ip ospf interface auth-type	Sets the authentication type.
show ip ospf interface	Displays the status and statistics of an OSPF interface.

MIB Objects

```
ospfIfTable
  ospfIfAuthKey
```

ip ospf interface auth-type

Sets the OSPF interface authentication type. Authentication allows the router to only respond to other routers that have the correct authentication information.

ip ospf interface {*ip_address* | *interface_name***} auth-type [none | simple | md5]**

Syntax Definitions

ip_address	The 32-bit IP address for the router interface.
interface_name	The name of the interface.
none	No authentication.
simple	Simple, clear text authentication.
md5	MD5 encrypted authentication.

Defaults

parameter	default
none | simple | md5	**none**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use this command to set the type of authentication that the OSPF interface uses to validate requests for route information from other OSPF neighbors on this interface.
- Simple authentication is authentication that uses only a text string as the password. The authentication type **simple** is used in conjunction with the **auth-key** keyword described, on page 30-39.
- MD5 authentication is encrypted authentication that uses an encryption key string and a key identification number. Both of these are necessary as the password. The authentication type **md5** is used in conduction with the commands described on page 30-45 and 30-47. One command enables MD5 and the other sets the key identification number.

Examples

```
-> ip ospf interface 172.22.2.115 auth-type simple
-> ip ospf interface vlan-101 auth-type-simple
```

Release History

Release 5.1; command was introduced.
Release 5.1.6; *interface_name* parameter added.

Related Commands

ip ospf interface auth-key	Sets the password for simple authentication.
show ip ospf interface	Displays the status and statistics of an OSPF interface.

MIB Objects

```
ospfIfTable
   ospfIfAuthType
```

ip ospf interface dead-interval

Configures the OSPF interface dead interval.

ip ospf interface {*ip_address* | *interface_name***} dead-interval** *seconds*

Syntax Definitions

ip_address	A 32-bit IP address assigned to the interface.
interface_name	The name of the interface.
seconds	The dead interval, in seconds. The valid range is 1–65535.

Defaults

parameter	default
seconds (broadcast and point-to-point)	40
seconds (NBMA and point-to-multi-point)	120

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This is the interval, in seconds, after which a neighbor on this interface is considered dead if no hello packets have been received from this neighbor.
- This interval should be greater than the hello interval or the multiple of the hello interval.

Examples

```
-> ip ospf interface 172.22.2.115 dead-interval 50
-> ip ospf interface vlan-101 dead-interval 50
```

Release History

Release 5.1; command was introduced.
Release 5.1.6; *interface_name* parameter added.

Related Commands

ip ospf interface hello-interval	Configures the OSPF interface hello interval.
show ip ospf interface	Displays the status and statistics of an OSPF interface.

MIB Objects

```
ospfIfTable
   ospfIfRtrDeadInterval
```

ip ospf interface hello-interval

Configures the OSPF interface hello interval.

ip ospf interface {*ip_address* | *interface_name***} hello-interval** *seconds*

Syntax Definitions

ip_address	The 32-bit IP address assigned to the interface.
interface_name	The name of the interface.
seconds	The hello interval, in seconds. The valid range is 1–65535.

Defaults

parameter	default
seconds (broadcast and point-to-point)	10
seconds (NBMA and point-to-multi-point)	30

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This is the interval between two consecutive hello packets sent out on this interface.

Examples

```
-> ip ospf interface 172.22.2.115 hello-interval 50
-> ip ospf interface vlan-101 hello-interval 50
```

Release History

Release 5.1; command was introduced.
Release 5.1.6; *interface_name* parameter added.

Related Commands

show ip ospf interface	Displays the status and statistics of an OSPF interface.

MIB Objects

```
ospfIfTable
   ospfIfHelloInterval
```

ip ospf interface md5

Creates and deletes the OSPF interface MD5 key identification number.

ip ospf interface {*ip_address* | *interface_name***} md5** *key_id* **[enable | disable]**

Syntax Definitions

ip_address	A 32-bit IP address.
interface_name	The name of the interface.
key_id	A key identification number. The key identification number specifies a number that allows MD5 encrypted routers to communicate. Both routers must use the same key ID. The valid range is 1–255.
enable	Enables the interface key.
disable	Disables the interface key.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- MD5 authentication can be used to encrypt information sent over the network. MD5 authentication works by using shared secret keys. Keys are used to sign the packets with an MD5 checksum, and they cannot be forged or tampered with. Since the keys are not included in the packet, snooping the key is not possible.
- This command is used in conjunction with the commands described on pages 30-40 and 30-47.
- The **no** variant deletes the key ID number.

Examples

```
-> ip ospf interface 172.22.2.115 md5 100
-> ip ospf interface 172.22.2.115 md5 100 enable
-> ip ospf interface vlan-101 md5 100
-> ip ospf interface vlan-101 md5 10 disable0
```

Release History

Release 5.1; command was introduced.
Release 5.1.6; *interface_name* parameter added.

Related Commands

ip ospf interface auth-type	Sets the OSPF interface authentication type.
ip ospf interface md5 key	Configures the OSPF key ID and key.
show ip ospf interface	Displays the status and statistics of an OSPF interface.

MIB Objects

```
alaOspfIfMd5Table
   alaOspfIfMd5IpAddress
   alaOspfIfMd5KeyId
```

ip ospf interface md5 key

Configures the OSPF key string. This interface MD5 string, along with the key identification number, enables the interface to encode MD5 encryption.

ip ospf interface {*ip_address* | *interface_name***} md5** *key_id* **key** *key_string*

Syntax Definitions

ip_address	A 32-bit IP address assigned to the interface.
interface_name	The name of the interface.
key_id	The key ID. The valid range is 1–255.
key_string	A key string.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command is used in conjunction with the commands described above on pages 30-45 and 30-40.
- For MD5 authentication to function properly the same key string must be configured on the neighboring router for that interface.

Examples

```
-> ip ospf interface 172.22.2.115 md5 100 key 1
-> ip ospf interface vlan-101 md5 100 key 1
```

Release History

Release 5.1; command was introduced.
Release 5.1.6; *interface_name* parameter added.

Related Commands

ip ospf interface auth-type	Sets the OSPF interface authentication type.
ip ospf interface md5	Creates and deletes the OSPF interface MD5 key identification number.
show ip ospf interface	Displays the status and statistics of an OSPF interface.

MIB Objects

```
alaOspfIfMd5Table
   alaOspfIfMd5IpAddress
   alaOspfIfMd5KeyId
   alaOspfIfMd5Key
```

ip ospf interface type

Configures the OSPF interface type.

ip ospf interface {*ip_address* | *interface_name***} type {point-to-point | point-to-multipoint | broadcast | non-broadcast}**

Syntax Definitions

ip_address	The 32-bit IP address of the interface.
interface_name	The name of the interface.
broadcast	Sets the interface to be a broadcast OSPF interface.
non-broadcast	Sets the interface to be NBMA (Non Broadcast Multi Access) OSPF interface.
point-to-point	Sets the interface to be a point-to-point OSPF interface.
point-to-multipoint	Sets the interface to be a point-to-multipoint OSPF interface.

Defaults

parameter	default
broadcast | non-broadcast | point-to-point| point-to-multipoint	**broadcast**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command sets an interface to be broadcast, non-broadcast, point-to-point, or point-to-multipoint.
- If the type is non broadcast or point-to-multipoint static neighbors should be configured.

Examples

```
-> ip ospf interface 172.22.2.115 type non-broadcast
-> ip ospf interface vlan-101 type non-broadcast
```

Release History

Release 5.1; command was introduced.
Release 5.1.6; *interface_name* parameter added.

Related Commands

ip ospf neighbor	Creates a static neighbor on a Non Broadcast Multi Access (NBMA) interface.
show ip ospf interface	Displays the status and statistics of an OSPF interface.

MIB Objects

```
ospfIfTable
   ospfIfType
```

ip ospf interface cost

Configures the OSPF interface cost.

ip ospf interface {*ip_address* | *interface_name***} cost** *cost*

Syntax Definitions

ip_address	The 32-bit IP address.
interface_name	The name of the interface.
cost	The interface cost. The valid range is 0 to 65535.

Defaults

parameter	default
cost	1

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

The configured interface cost, if any, is used during OSPF route calculations.

Examples

```
-> ip ospf interface 172.22.2.115 cost 10
-> ip ospf interface vlan-101 cost 10
```

Release History

Release 5.1; command was introduced.
Release 5.1.6; *interface_name* parameter added.

Related Commands

show ip ospf interface	Displays the status and statistics of an OSPF interface.

MIB Objects

```
ospfIfMetricTable
   ospfIfMetricIpAddress
   ospfIfMetricValue
```

ip ospf interface poll-interval

Configures the OSPF poll interval for a Non Broadcast Multi Access (NBMA) interface.

ip ospf interface {*ip_address* | *interface_name***} poll-interval** *seconds*

Syntax Definitions

ip_address	The 32-bit IP address for the interface.
interface_name	The name of the interface.
seconds	The poll interval, in seconds. The valid range is 1–2147483647.

Defaults

parameter	default
seconds	120

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This parameter configures the larger time interval, in seconds, between hello packets sent to an inactive neighbor.

Examples

```
-> ip ospf interface 172.22.2.115 poll-interval 500
-> ip ospf interface vlan-101 poll-interval 500
```

Release History

Release 5.1; command was introduced.
Release 5.1.6; *interface_name* parameter added.

Related Commands

show ip ospf interface	Displays the status and statistics of an OSPF interface.

MIB Objects

```
ospfIfTable
   ospfIfPollInterval
```

ip ospf interface priority

Configures the OSPF interface priority. The priority number helps determine the eligibility of this router to become the designated router on the network.

ip ospf interface {*ip_address* | *interface_name***} priority** *priority*

Syntax Definitions

ip_address	The 32-bit IP address for the interface.
interface_name	The name of the interface.
priority	The interface priority. The valid range is 0–255.

Defaults

parameter	default
priority	1

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

When two routers attached to a network both attempt to become the designated router, the one with the highest priority becomes the designated router. A router whose router priority is set to 0 is ineligible to become the designated router.

Examples

```
-> ip ospf interface 172.22.2.115 priority 100
-> ip ospf interface vlan-101 priority 100
```

Release History

Release 5.1; command was introduced.
Release 5.1.6; *interface_name* parameter added.

Related Commands

show ip ospf interface	Displays the status and statistics of an OSPF interface.

MIB Objects

```
ospfIfTable
   ospfIfRtrPriority
```

ip ospf interface retrans-interval

Configures the OSPF interface retransmit interval.

ip ospf interface {*ip_address* | *interface_name***} retrans-interval** *seconds*

Syntax Definitions

ip_address	The 32-bit IP address for the interface.
interface_name	The name of the interface.
seconds	The retransmit interval, in seconds. The valid range 0–3600.

Defaults

parameter	default
seconds	5

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

The number of seconds between link retransmission of OSPF packets on this interface.

Examples

```
-> ip ospf interface 172.22.2.115 retrans-interval 500
-> ip ospf interface vlan-101 retrans-interval 500
```

Release History

Release 5.1; command was introduced.
Release 5.1.6; *interface_name* parameter added.

Related Commands

show ip ospf interface	Displays the status and statistics of an OSPF interface.

MIB Objects

```
ospfIfTable
   ospfIfRetransInterval
```

ip ospf interface transit-delay

Configures the OSPF interface transit delay.

ip ospf interface {*ip_address* | *interface_name***} transit-delay** *seconds*

Syntax Definitions

ip_address	The 32-bit IP address for the interface.
interface_name	The name of the interface.
seconds	The transit delay, in seconds. The valid range is 0–3600.

Defaults

parameter	default
seconds	1

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

The estimated number of seconds required to transmit a link state update over this interface. This command takes into account transmission and propagation delays and must be greater than 0.

Examples

```
-> ip ospf interface 172.22.2.115 transit-delay 100
-> ip ospf interface vlan-101 transit-delay 100
```

Release History

Release 5.1; command was introduced.
Release 5.1.6; *interface_name* parameter added.

Related Commands

show ip ospf interface	Displays the status and statistics of an OSPF interface.

MIB Objects

```
ospfIfTable
   ospfIfTransitDelay
```

ip ospf restart-support

Configures support for the graceful restart feature on an OSPF router.

ip ospf restart-support {planned-unplanned | planned-only}

no ip ospf restart-support

Syntax Definitions

planned-unplanned	Specifies support for planned and unplanned restarts.
planned-only	Specifies support for planned restarts only.

Defaults

Graceful restart is disabled be default.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The minimum hardware configuration for this command is a redundant CMM configuration. This command is not supported on OmniSwitch 7700/7800/8800 switches with a single CMM or OmniSwitch 6600 Family switches in a standalone configuration.
- On OmniSwitch 6600 Family switches, a graceful restart is only supported only on active ports (i.e., interfaces), which are on the secondary or idle modules in a stack during a takeover. It is not supported on ports on a primary switch in a stack.
- Use the **no** form of the command to disable support for the graceful restart feature on an OSPF router.

Examples

```
-> ip ospf restart-support planned-unplanned
-> no ip ospf restart-support
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip ospf restart	Displays the OSPF graceful restart related configuration and status.

MIB Objects

```
alaProtocolOspf
   alaOspfRestartSupport
```

ip ospf restart-interval

Configures the grace period for achieving a graceful OSPF restart.

ip ospf restart-interval [*seconds***]**

Syntax Definitions

seconds	The hitless restart timeout interval, in seconds. The valid range is 0–1800.

Defaults

parameter	default
seconds	120

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The minimum hardware configuration for this command is a redundant CMM configuration. This command is not supported on OmniSwitch 7700/7800/8800 switches with a single CMM or OmniSwitch 6600 Family switches in a standalone configuration.
- On OmniSwitch 6600 Family switches, a graceful restart is only supported only on active ports (i.e., interfaces), which are on the secondary or idle modules in a stack during a takeover. It is not supported on ports on a primary switch in a stack.

Examples

```
-> ip ospf restart-interval 600
```

Release History

Release 5.1; command was introduced.

Related Commands

ip ospf restart-support	Administratively enables and disables support for the graceful restart feature on an OSPF router.
show ip ospf restart	Displays the OSPF graceful restart related configuration and status.

MIB Objects

```
alaProtocolOspf
   alaOspfRestartInterval
```

ip ospf restart-helper status

Administratively enables and disables the capability of an OSPF router to operate in helper mode in response to a router performing a graceful restart.

ip ospf restart-helper [status {enable | disable}]

Syntax Definitions

enable	Enables the capability of an OSPF router to operate in helper mode.
disable	Disables the capability of an OSPF router to operate in helper mode.

Defaults

parameter	default
enable | disable	enable

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The minimum hardware configuration for this command is a redundant CMM configuration. This command is not supported on OmniSwitch 7700/7800/8800 switches with a single CMM or OmniSwitch 6600 Family switches in a standalone configuration.
- On OmniSwitch 6600 Family switches, a graceful restart is only supported only on active ports (i.e., interfaces), which are on the secondary or idle modules in a stack during a takeover. It is not supported on ports on a primary switch in a stack.

Examples

```
-> ip ospf restart-helper status disable
-> ip ospf restart-helper enable
```

Release History

Release 5.1; command was introduced.

Related Commands

ip ospf restart-support	Administratively enables and disables support for the graceful restart feature on an OSPF router.
ip ospf restart-helper strict-lsa-checking-status	Administratively enables and disables whether or not a changed Link State Advertisement (LSA) will result in termination of graceful restart by a helping router.
show ip ospf restart	Displays the OSPF graceful restart related configuration and status.

MIB Objects

```
alaProtocolOspf
   alaOspfRestartHelperSupport
```

ip ospf restart-helper strict-lsa-checking-status

Administratively enables and disables whether or not a changed Link State Advertisement (LSA) will result in termination of graceful restart by a helping router.

ip ospf restart-helper strict-lsa-checking-status {enable | disable}

Syntax Definitions

enable	Enables whether or not a changed LSA will result in termination of graceful restart by a helping router.
disable	Disables whether or not a changed LSA will result in termination of graceful restart by a helping router.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The minimum hardware configuration for this command is a redundant CMM configuration. This command is not supported on OmniSwitch 7700/7800/8800 switches with a single CMM or OmniSwitch 6600 Family switches in a standalone configuration.
- On OmniSwitch 6600 Family switches, a graceful restart is only supported only on active ports (i.e., interfaces), which are on the secondary or idle modules in a stack during a takeover. It is not supported on ports on a primary switch in a stack.

Examples

```
-> ip ospf restart-helper strict-lsa-checking-status disable
```

Release History

Release 5.1; command was introduced.

Related Commands

ip ospf restart-support	Administratively enables and disables support for the graceful restart feature on an OSPF router.
ip ospf restart-helper status	Administratively enables and disables the capability of an OSPF router to operate in helper mode in response to a router performing a graceful restart.
show ip ospf restart	Displays the OSPF graceful restart related configuration and status.

MIB Objects

```
alaProtocolOspf
   alaOspfRestartHelperSupport
```

ip ospf restart initiate

Initiates a planned graceful restart.

ip ospf restart initiate

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- You must execute this command on the primary CMM before executing a **takeover** command.
- The minimum hardware configuration for this command is a redundant CMM configuration. This command is not supported on OmniSwitch 7700/7800/8800 switches with a single CMM or OmniSwitch 6600 Family switches in a standalone configuration.
- On OmniSwitch 6600 Family switches, a graceful restart is only supported only on active ports (i.e., interfaces), which are on the secondary or idle modules in a stack during a takeover. It is not supported on ports on a primary switch in a stack.

Examples

```
-> ip ospf restart initiate
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip ospf restart	Displays the OSPF graceful restart related configuration and status.

MIB Objects

```
alaProtocolOspf
   alaOspfRestartInitiate
```

show ip ospf

Displays OSPF status and general configuration parameters.

show ip ospf

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command is used to display the general configuration parameters of the OSPF router.
- See the Related Commands section below to modify the displayed parameters.

Examples

```
-> show ip ospf

Router Id                        = 10.255.11.242,
OSPF Version Number              = 2,
Admin Status                     = Enabled,
Area Border Router?             = No,
AS Border Router Status          = Disabled,
Route Redistribution Status      = Disabled,
Route Tag                        = 0,
SPF Hold  Time (in seconds)      = 10,
SPF Delay Time (in seconds)     = 5,
MTU Checking                     = Disabled,
# of Routes                      = 0,
# of AS-External LSAs            = 0,
# of self-originated LSAs        = 0,
# of LSAs received               = 0,
External LSDB Limit              = -1,
Exit Overflow Interval           = 0,
# of SPF calculations done       = 0,
# of Incr SPF calculations done  = 0,
# of Init State Nbrs             = 0,
# of 2-Way State Nbrs            = 0,
# of Exchange State Nbrs         = 0,
# of Full State Nbrs             = 0,
# of attached areas              = 1,
# of Active areas                = 0,
# of Transit areas               = 0,
# of attached NSSAs              = 0
```

output definitions

Router Id	The unique identification for the router.
OSPF Version Number	The version of OSPF the router is running.
Admin Status	Whether OSPF is currently enabled or disabled on the router.
Area Border Router?	Whether the router status is an area router or not.
AS Border Router Status	Whether the area Autonomous System Border Router status of this router is enabled or disabled.
Route Redistribution Status	Whether route redistribution is enabled or disabled on the router. This is set using the **ip ospf redist status** command
Route Tag	Shows the route tag for this router.
SPF Hold Time	Shows the time in seconds between the reception of an OSPF topology change and the start of a SPF calculation.
SPF Delay Time	Shows the time in seconds between consecutive SPF calculations.
MTU Checking	Shows whether Maximum Transfer Unit checking is enabled or disabled. This is set using the **ip ospf mtu-checking** command.
# of routes	The total number of OSPF routes known to this router.
# of AS-External LSAs	The number of external routes learned from outside the router's Autonomous System (AS).
# of self-originated LSAs	The number of times a new Link State Advertisement has been sent from this router.
# of LSAs received	The number of times a new Link State Advertisement has been received by this router.
External LSDB Limit	The maximum number of entries allowed in the external Link State Database.
Exit Overflow Interval	The number of seconds the router remains in the overflow state before attempting to leave it. This is set using the **ip ospf exit-overflow-interval** command.
# of SPF calculations done	The number of SPF calculations that have occurred.
# of Incr SPF calculations done	The number of incremental SPF calculations done.
# of Init State Nbrs	The number of neighbors in the initialization state.
# of 2-Way State Nbrs	The number of OSPF 2-way state neighbors on this router.
# of Exchange State Nbrs	The number of neighbors in the exchange state.
# of Full State Nbrs	The number of neighbors in the full state.
# of attached areas	The number of areas that are configured on the router.
# of Active areas	The number of areas that are active.
# of Transit areas	The number of transit areas that are configured on the router.
# of attached NSSAs	The number of Not So Stubby Areas that are configured on the router.

Release History

Release 5.1; command was introduced.

Related Commands

ip ospf status	Enables or disables the administration of OSPF on the router.
ip ospf mtu-checking	Enables or disables the use of Maximum Transfer Unit (MTU) checking.
ip ospf spf-timer	Configures timers for SPF calculation.
ip ospf redist status	Enables or disables OSPF redistribution
ip ospf asbr	Configures the router as an Autonomous System Border Router (ASBR).
ip ospf extlsdb-limit	Assigns a limit to the number of External Link-State Database (LSDB) entries that can be learned.
ip ospf exit-overflow-interval	This command sets the overflow interval value.
ip ospf route-tag	Configures a tag value for Autonomous System External (ASE) routes created.
ip router router-id	Configures the router ID for the router.

MIB Objects

```
ospfGeneralGroup
   ospfRouterId
   ospfAdminStat
   ospfVersionNumber
   ospfAreaBdrRtrStatus
   ospfASBdrRtrStatus
   ospfExternLsaCount
   ospfExternLsaCksumSum
   ospfTOSSupport
   ospfOriginateNewLsas
   ospfRxNewLsas
   ospfExtLsdbLimit
   ospfExitOverflowInterval
alcatelIND1Ospf
   alaOspfRedistAdminStatus
   alaOspfRedistRouteTag
   alaOspfTimerSpfDelay
   alaOspfTimerSpfHold
   alaOspfRouteNumber
   alaOspfMTUCheck
```

show ip ospf border-routers

Displays information regarding all or specified border routers.

show ip ospf border-routers [*area_id***] [***router_id***] [***tos***] [***gateway***]**

Syntax Definitions

area_id	A unique 32-bit value in IP address format.
router_id	A unique 32-bit value, such as an IP address, that identifies a neighboring router in the Autonomous System.
tos	The Type of Service. The valid range is 0–15. Only ToS value 0 is supported at this time.
gateway	The 32-bit IP address of the gateway for the border router being displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command is used to display a list of border routers known by this OSPF router.
- By using the optional parameters, you can display the border routers using the specified parameter. For example, to find a router using a router ID of 1.1.1.1, enter the command using the router ID of 1.1.1.1 as a search criteria.
- See the related commands sections below to modify the list.

Examples

```
-> show ip ospf border-routers 10.0.0.0

Router Id              Area Id            Gateway         TOS    Metric
-----------------+-----------------+--------------------+------+--------
10.0.0.0           1.0.0.1            143.209.92.71       1       1
```

output definitions

Router ID	The unique identification for the router.
Area ID	A unique 32-bit value, such as an IP address, that identifies a neighboring router in the Autonomous System.
Gateway	The next hop interface on which the border router has been learned.

output definitions (continued)

ToS	The Type of Service. Only ToS value 0 is supported at this time.
Metric	The cost to the border router.

Release History

Release 5.1; command was introduced.

Related Commands

ip ospf asbr	Configures the router as an Autonomous System Border Router (ASBR).

MIB Objects

```
alaOspfBdrRouterAreaId
alaOspfBdrRouterId
alaOspfBdrRouterTos
alaOspfBdrRouterMetric
```

show ip ospf ext-lsdb

Displays external Link State Advertisements known by this router.

show ip ospf ext-lsdb [linkstate-id *ls_id***] [router-id** *router_id***]**

Syntax Definitions

ls_id	The Link state ID. The ID is a unique 32-bit value such as an IP address. This number is used as a record in the link state database.
router_id	The Router ID. The ID is a unique 32-bit value such as an IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command is used to display the external link state database (LSDB) for the OSPF router.
- This command can be used for OSPF debugging purposes, specifically to narrow down sections of attached areas to determine which sections are receiving the specified external LSAs. You may specify only the parameters from the area LSDB in which you are interested using the optional command parameters.
- See the Related Commands section below to modify the list.

Examples

```
-> show ip ospf ext-lsdb

      LS Id         Orig Router-Id     SeqNo      Age     Protocol
-----------------+-----------------+----------+--------+----------
  198.168.100.100    198.168.100.100      10      100     STATIC
```

output definitions

LS Id	The Link state ID. The ID is a unique 32-bit value such as an IP address. This number is used as a record in the link state database.
Orig Router-Id	The router ID of the router that originated the external LSDB.
SeqNo	The advertisement sequence number (i.e., a value used to identify old and duplicate link state advertisements).
Age	The age of the LSA in seconds. That is, the duration for which this entry has existed in the external database.
Protocol	The type of protocol, if any.

Release History

Release 5.1; command was introduced.

Related Commands

ip ospf extlsdb-limit	Assigns a limit to the number of External Link-State Database (LSDB) entries that can be learned.

MIB Objects

```
ospfExtLsdbTable
   ospfExtLsdbLsid
   ospfExtLsdbRouterId
   ospfExtLsdbSequence
   ospfExtLsdbAge
   ospfExtLsdbType
```

show ip ospf host

Displays information on configured OSPF hosts.

show ip ospf host [*ip_address***]**

Syntax Definitions

ip_address	A 32-bit IP address for a directly attached host.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command is used to display general information for OSPF hosts directly attached to this router.
- See the Related Commands section below to modify the list.

Examples

```
-> show ip ospf host 172.22.2.115

   Host Address     TOS     Metric     Status       AreaId
-----------------+-------+-----------+--------+-----------------
 143.209.92.12       1            0      Up     0.0.0.0
```

output definitions

Host Address	A 32-bit IP address for a directly attached host. This can be set using the **ip ospf host** command.
ToS	The Type of Service traffic from the host is labeled as. ToS is set using the **ip ospf host** command.
Metric	The metric assigned to the host. Metric is set using the **ip ospf host** command.
Status	Whether the host is enabled or disabled.
AreaId	The area identification for the host's area.

Release History

Release 5.1; command was introduced.

Related Commands

ip ospf host	Creates and deletes an OSPF entry for directly attached hosts.

MIB Objects

```
ospfHostTable
   ospfHostIpAddress
   ospfHostTOS
   ospfHostMetric
   ospfHostStatus
   ospfHostAreaID
```

show ip ospf lsdb

Displays LSAs in the Link State Database associated with each area.

show ip ospf lsdb [*area_id*] **[rtr | net | netsum | asbrsum] [linkstate-id** *ls_id***] [router-id** *router_id***]**

Syntax Definitions

area_id	A unique 32-bit value in IP address format.
rtr	Specifies router LSAs.
net	Specifies network LSAs.
netsum	Specifies network summary LSAs.
asbrsum	Specifies Autonomous System Border Router summary LSAs.
ls_id	The Link state ID. The ID is a unique 32-bit value such as an IP address. This number is used as a record in the link state database.
router_id	The Router ID. The ID is a unique 32-bit value such as an IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command is used to display the Link State Database (LSDB) of the OSPF router. This command can be used for OSPF debugging purposes, specifically to narrow down sections of an area to determine which sections are receiving the specified link state advertisements. You may specify only the parameters from the area LSDB in which you are interested using the optional command parameters.
- You can view link state advertisements by specifying either a link state identifier or a router identifier. However, when specifying a router ID, you must also supply a valid link state ID.

Examples

```
-> show ip ospf lsdb
    Area Id       Type        LS Id        Orig Router-Id     SeqNo      Age
---------------+-------+---------------+---------------+------------+-----
0.0.0.1          OSPF   198.168.100.100  198.168.100.100     1         100
```

output definitions

Area Id	The area identification for the area to which the record belongs.
Type	The protocol type from where the route was learned.
LS Id	The Link state ID. The ID is a unique 32-bit value such as an IP address. This number is used as a record in the link state database.

output definitions (continued)

Orig Router-Id	The router ID of the router that originated the external LSDB.
SeqNo	The advertisement sequence number (i.e., a value used to identify old and duplicate link state advertisements).
Age	The age of the LSA in seconds. That is, the duration for which this entry has existed in the external database.

Release History

Release 5.1; command was introduced.

Related Commands

show ip ospf	Displays OSPF status and general configuration parameters.

MIB Objects

```
ospfLsdbTable
   ospfLsdbAreaId
   ospfLsdbType
   ospfLsdbLsid
   ospfLsdbRouterId
   ospfLsdbSequence
   ospfLsdbAge
```

show ip ospf neighbor

Displays information on OSPF non-virtual neighbor routers.

show ip ospf neighbor [*ip_address*]

Syntax Definitions

ip_address	A 32-bit IP address of the neighboring router.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command is used to display all non-virtual neighbors of the OSPF router.
- See the Related Commands section below to modify the list.

Examples

```
-> show ip ospf neighbor

IP Address        Area Id          Router Id      Vlan  State  Mode
----------------+----------------+----------------+----+-------+--------
1.1.1.1          255.255.255.255  0.0.0.0        0     Down   Static
```

output definitions

IP Address	The IP address of the neighbor
Area Id	A unique 32-bit value, such as an IP address, that identifies the neighboring router in the Autonomous System.
Router Id	The unique identification for the neighboring router.
VlanId	The VLAN corresponding to this interface on which the neighbor is reachable.
State	The state of the OSPF neighbor adjacency.
Mode	What type of neighbor, either **Dynamic** (learned) or **Static**.

```
-> show ip ospf neighbor 1.1.1.1
Neighbor's IP Address                = 1.1.1.1,
Neighbor's Router Id                 = 0.0.0.0,
Neighbor's Area Id                   = 255.255.255.255,
Neighbor's DR Address                = 0.0.0.0,
Neighbor's BDR Address               = 0.0.0.0,
Neighbor's Priority                  = 1,
Neighbor's State                     = Down,
Hello Suppressed ?                   = No,
Neighbor's type                      = Static,
DR Eligible                          = Yes,
# of State Events                    = 0,
Mode                                 = Slave,
MD5 Sequence Number                  = 0,
Time since Last Hello                = 0 sec,
# of Outstanding LS Requests         = 0,
# of Outstanding LS Acknowledgements = 0,
# of Outstanding LS Retransmissions  = 0,
Restart Helper Status               = Not Restarting,
Restart Age (in seconds)            = 0 sec,
Last Restart Helper Exit Reason     = None
```

output definitions

Neighbor's IP Address	The IP address of the neighbor.
Neighbor's Router Id	The identification number for the selected host's record. It is most often the router's IP address.
Neighbor's Area Id	Identifier of the OSPF Area to which the neighbor is attached. 255.255.255.255 shows that this neighbor is not attached to any area.
Neighbor's DR Address	The address of the neighbors Designated Router.
Neighbor's BDR Address	The address of the neighbors Backup Designated Router.
Neighbor's Priority	The priority value for this neighbor becoming the DR.
Neighbor's State	The condition of the OSPF neighbor's state machine.
Hello Suppressed	Whether sending hello messages to this neighbor is suppressed.
Neighbor's type	What type of neighbor this is, either dynamic or static.
DR Eligible	Shows the eligibility status of the static neighbor. If it is configured as "non-eligible" during creation of the neighbor, it shows up as **No**. Otherwise, if configured as Eligible (the default), it shows up as **Yes**.
# of State Events	The number of state events restricted for this neighbor and the local router.
Mode	The role the neighbor has with the local router during DD Exchange, which can be Master or Slave.
MD5 Sequence Number	The sequence number of the MD5 authorization key.
Time since Last Hello	The amount of time (in seconds) since the last HELLO messages was received from this neighbor.
# of Outstanding LS Requests	The number of Link State requests to this neighbor that have not received a response from this neighbor.
# of Outstanding LS Acknowledgements	Number of Link state Acknowledgements queued up by the local router to be sent to the neighbor.

output definitions (continued)

# of Outstanding LS Retransmissions	The number of Link State updates to the neighbor that need to be retransmitted by the OSPF router.
Restart Helper Status	Indicates whether the router is acting as a hitless restart helper for the neighbor.
Restart Age	The remaining time, in seconds, for the current OSPF hitless restart interval if the router is acting as a restart helper for the neighbor.
Last Restart Helper Exit Reason	The outcome of the last attempt at acting as a hitless restart helper for the neighbor.

Release History

Release 5.1; command was introduced.

Related Commands

ip ospf neighbor	Creates a static neighbor on a Non Broadcast Multi Access (NBMA) interface.

MIB Objects

```
ospfNbrTable
   ospfNbrIpAddr
   ospfNbrRtrId
   ospfNbrOptions
   ospfNbrPriority
   ospfNbrState
   ospfNbrEvents
   ospfNbrHelloSuppressed
alaOspfNbrAugTable
   alaOspfNbrRestartHelperStatus
   alaOspfNbrRestartHelperAge
   alaOspfNbrRestartHelperExitReason
```

show ip ospf redist-filter

Displays OSPF redistribution filter attributes.

show ip redist-filter [local | static | rip | bgp] [*ip_address***] [***subnet_mask***]**

Syntax Definitions

local	Displays the local type of router being redistributed.
static	Displays the static type of router being redistributed.
rip	Displays the RIP type of router being redistributed.
bgp	Displays the BGP type of router being redistributed. (BGP is not supported on OmniSwitch 6600 Family switches.)
ip_address	A 32-bit IP address specified by a redistribution filter.
subnet_mask	A subnet mask of the redistribution filter.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command is used to display the parameters of a redistribution filter on the OSPF router.
- See the Related Commands section below to modify the list.

Examples

```
-> show ip ospf redist-filter

   Proto     Destination/Mask        Control     Effect  Metric  RouteTag
----------+--------------------+--------------+------+--------+---------
 STATIC     143.209.92.0/24       sub-on          Yes     0       0
 RIP        192.168.112.0/16      sub-on          No      0       0
```

output definitions

Proto	The filter's protocol type.
Destination/Mask	The IP address and mask of the redistribution filter.
Control	This may be subnets, aggregates, or no subnets.
Effect	Whether the redistribution of routes in this range is allowed or denied.
Metric	The filter's metric that is enforced on the OSPF route.
RouteTag	The specified route tag for the filter.

```
-> show ip ospf redist-filter bgp 192.168.112.0 255.255.0.0

 Destination IP Address                    = 192.168.112.0,
 Destination IP Mask                       = 255.255.0.0,
 Protocol                                  = RIP,
 Metric                                    = 0,
 Control                                   = subnets-on,
 Filter Permission                         = Yes,
 Route Tag                                 = 0,
```

output definitions

Destination IP Address	The IP address of the redistribution filter.
Destination IP Mask	The mask of the redistribution filter.
Protocol	The filter's protocol type.
Metric	The filter's metric that is enforced on the OSPF route.
Control	This may be subnets, aggregates, or no subnets.
Filter Permission	Shows the type of permission for the filter, either **permit** or **deny**.
Route Tag	The specified route tag for the filter.

Release History

Release 5.1; command was introduced.

Related Commands

ip ospf redist-filter	Creates or deletes an OSPF redistribution filter.
ip ospf redist status	Enables or disables OSPF redistribution.

MIB Objects

```
alactel1INDOspf
   alaOspfRedistRouteProto
   alaOspfRedistRouteDest
   alaOspfRedistRouteMask
   alaOspfRedistRouteMetric
   alaOspfRedistRouteControl
   alaOspfRedistRouteTagMatch
   alaOspfRedistRouteEffect
```

show ip ospf redist

Displays the redistribution instances that allow routes to be redistributed into OSPF.

show ip ospf redist [local | static | rip | bgp]

Syntax Definitions

local	Displays the redistribution instances corresponding to local routes.
static	Displays the redistribution instances corresponding to static routes.
rip	Displays the redistribution instances corresponding to RIP routes.
bgp	Displays the redistribution instances corresponding to BGP routes. (BGP is not supported on OmniSwitch 6600 Family switches.)

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command is used to display specific redistribution instances.
- See the Related Commands section below to modify the list.

Examples

```
-> show ip ospf redist
  Protocol    Metric Type    Metric    Route Tag      Subnets
----------+--------------+---------+------------+----------+
 STATIC          type2          0          0          Enabled
 BGP             type2          0          0          Enabled
 OSPF            type1          1          2          Enabled

-> show ip ospf redist static

Protocol        = STATIC,
Metric Type     = type2,
Route Tag       = 0,
Subnets         = Enabled
```

output definitions

Protocol	The protocol type being redistributed.
Metric Type	The classification of the redistributed route.
Metric	The cost of the redistribution route.

output definitions (continued)

Route Tag	The route tag associated with the redistribution instance.
Subnets	The status of the subnet route redistribution.

Release History

Release 5.1; command was introduced.

Related Commands

ip ospf redist	Creates and deletes a redistribution instance that allows routes to be redistributed into OSPF.

MIB Objects

```
Alcatel1INDOspf
   alaOspfRedistProtoId
   alaOspfRedistProtoSubnets
   alaOspfRedistProtoMetricType
   alaOspfRedistProtoMetric
   alaOspfRedistProtoStatu
```

show ip ospf routes

Displays OSPF routes known to the router.

show ip ospf routes [*ip_addr mask tos gateway***]**

Syntax Definitions

ip_addr	The 32-bit IP address of the route destination in dotted decimal format.
mask	The IP subnet mask of the route destination.
tos	The Type of Service of the route.
gateway	The next hop IP address for this router.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

If no variables are entered, all routes are displayed. If the variables are entered, then only routes matching the specified criteria are shown. All the variables described above must be entered for a route match. If all of the variables are not entered, an error message is returned.

Examples

```
-> show ip ospf routes

Destination/Mask          Gateway       Metric   Vlan     Type
--------------------+-----------------+--------+------+----------
198.168.100.100       195.5.2.8          0        5       AS-Ext
```

output definitions

Destination/Mask	The destination address of the route. This can also display the destination IP address mask if it is known.
Gateway	The gateway address of the route.
Metric	The cost of the route.
Vlan	The VLAN number on which the gateway can be routed.
Type	The type of OSPF route.

Release History

Release 5.1; command was introduced.

Related Commands

show ip ospf	Displays OSPF status and general configuration parameters.

MIB Objects

```
Alcatel1INDOspf
   alaOspfRouteDest
   alaOspfRouteMask
   alaOspfRouteNextHop
   alaOspfRouteMetric1
```

show ip ospf virtual-link

Displays virtual link information. A virtual link is used to connect OSPF backbone routers that are not physically contiguous.

show ip ospf virtual-link [*router_id***]**

Syntax Definitions

router_id	The router ID of the remote end of the virtual link that is to be viewed.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

See the Related Commands section below to modify the list.

Examples

```
-> show ip ospf virtual-link
                                      State
 Transit AreaId      Router-id    Link / Adjacency  AuthType   OperStatus
---------------+----------------+---------------+----------+------------
1.1.1.1           172.17.1.1     P2P  / Full       none        up
```

output definitions

Transit AreaId	The area identification for the area assigned to the virtual link.
Router-Id	The destination router identification for the virtual link.
State Link	The state of the virtual link in regard to the local router.
State Adjacency	The state of the virtual link adjacency.
AuthType	The type of authorization employed by the virtual link.
OperStatus	Displays whether the virtual link is enabled or disabled.

Release History

Release 5.1; command was introduced.

Related Commands

ip ospf virtual-link	Creates or deletes a virtual link.
show ip ospf virtual-neighbor	Displays OSPF virtual neighbors.

MIB Objects

```
ospfVirtIfTable
   ospfVirtIfAreaId
   ospfVirtIfNeighbor
   ospfVirtIfState
   ospfVirtIfAuthType
```

show ip ospf virtual-neighbor

Displays OSPF virtual neighbors. A virtual neighbor is connected to the router via a virtual link rather than a physical one.

show ip ospf virtual-neighbor *area_id router_id*

Syntax Definitions

area_id	A unique 32-bit value in IP address format.
router_id	A unique 32-bit value, such as an IP address, that identifies the configured OSPF area in the AS.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command is used to display all virtual neighbors for the OSPF router.
- See the Related Commands section below to modify the list.

Examples

```
-> show ip ospf virtual-neighbor 0.0.0.0 10.0.0.1

     AreaId           RouterId     Priority Events RxmtQLen LastHello  State
----------------+----------------+--------+------+--------+---------+-------
 0.0.0.0           10.0.0.0           1        10     100      323     INIT
```

output definitions

AreaId	The area identification for the area of which the virtual neighbor is a part.
RouterId	The router identification of the virtual neighbor.
Priority	The number used to determine whether the virtual neighbor will become the designated router for its area.
Events	The number of OSPF control message sent by the neighbor to the router.
RxmtQlen	The length (in number of packets) of the retransmit queue.
LastHello	The last Hello message sent by the neighbor
State	The current state the virtual neighbor is in relative to the router; this will be INIT, Exchange, or Full.

```
-> show ip ospf virtual-neighbor 0.0.0.1 2.0.0.254
Neighbor's IP Address               = 2.0.0.254,
Neighbor's Router Id                = 2.0.0.254,
Neighbor's Area Id                  = 0.0.0.1,
Neighbor's DR Address               = 2.0.0.1,
Neighbor's BDR Address              = 2.0.0.254,
Neighbor's Priority                 = 1,
Neighbor's State                    = Full,
Hello Suppressed ?                  = No,
Neighbor's type                     = Dynamic,
# of State Events                   = 6,
Mode = Master,
MD5 Sequence Number                 = 0,
Time since Last Hello               = 5 sec,
Last DD I_M_MS                      =
# of Outstanding LS Requests        = 0,
# of Outstanding LS Acknowledgements= 0,
# of Outstanding LS Retransmissions = 0,
Restart Helper Status               = Not Restarting,
Restart Age (in seconds)            = 0 sec,
Last Restart Helper Exit Reason     = None
```

output definitions

Neighbor's IP Address	The IP address of the virtual neighbor.
Neighbor's Router Id	The identification number for the selected host's record. It is most often the router's IP address.
Neighbor's Area Id	Identifier of the OSPF Area to which the virtual neighbor is attached. 255.255.255.255 shows that this virtual neighbor is not attached to any area.
Neighbor's DR Address	The address of the virtual neighbor's Designated Router.
Neighbor's BDR Address	The address of the virtual neighbor's Backup Designated Router.
Neighbor's Priority	The priority value for this virtual neighbor becoming the DR.
Neighbor's State	The condition of the OSPF virtual neighbor's state machine.
Hello Suppressed	Whether sending hello messages to this virtual neighbor is suppressed.
Neighbor's type	What type of virtual neighbor this is, either dynamic or static.
DR Eligible	Shows the eligibility status of the virtual neighbor. If it is configured as "non-eligible" during creation of the neighbor, it shows up as **No**. Otherwise, if configured as Eligible (the default), it shows up as **Yes**.
# of State Events	The number of state events restricted for this virtual neighbor and the local router.
Mode	The role the virtual neighbor has with the local router during DD Exchange, which can be Master or Slave.
MD5 Sequence Number	The sequence number of the MD5 authorization key.
Time since Last Hello	The amount of time (in seconds) since the last HELLO messages was received from this virtual neighbor.
Last DD I_M_MS	The initialize (I), more (M) and master (MS) bits, and Options field Data Description (DD) packet received from the virtual neighbor. This parameter is used to determine whether the next DD packet has been received or not.

output definitions (continued)

# of Outstanding LS Requests	The number of Link State requests to this virtual neighbor that have not received a response from this virtual neighbor.
# of Outstanding LS Acknowledgements	Number of Link state Acknowledgements queued up by the local router to be sent to the virtual neighbor.
# of Outstanding LS Retransmissions	The number of Link State updates to the virtual neighbor that need to be retransmitted by the OSPF router.
Restart Helper Status	Indicates whether the router is acting as a hitless restart helper for the virtual neighbor.
Restart Age	The remaining time, in seconds, for the current OSPF hitless restart interval if the router is acting as a restart helper for the virtual neighbor.
Last Restart Helper Exit Reason	The outcome of the last attempt at acting as a hitless restart helper for the virtual neighbor.

Release History

Release 5.1; command was introduced.

Related Commands

ip ospf virtual-link	Creates or deletes a virtual link.

MIB Objects

```
ospfVirtNbrTable
   ospfVirtNbrArea
   ospfVirtNbrRtrId
   ospfVirtNbrState
alaOspfVirtNbrAugTable
   alaOspfVirtNbrRestartHelperStatus
   alaOspfVirtNbrRestartHelperAge
   alaOspfVirtNbrRestartHelperExitReason
```

show ip ospf area

Displays either all OSPF areas, or a specified OSPF area.

show ip ospf area [*area_id*]

Syntax Definitions

area_id	A unique 32-bit value in IP address format.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Allows you to view the details of a specified OSPF area.
- Not specifying an OSPF area will display all known areas for the OSPF router.
- See the Related Commands section below for information on modifying an area.

Examples

```
-> show ip ospf area


    Area Id      AdminStatus      Type       OperStatus
---------------+-------------+-------------+------------
1.1.1.1           disabled     normal       down
0.0.0.1           disabled     normal       down

-> show ip ospf area 0.0.0.0

Area Identifier                          = 1.1.1.1,
Admin Status                             = Disabled,
Operational Status                       = Down,
Area Type                                = normal,
Area Summary                             = Enabled,
Time since last SPF Run                  = 00h:00m:27s,
# of Area Border Routers known           = 0,
# of AS Border Routers known             = 0,
# of LSAs in area                        = 0,
# of SPF Calculations done               = 0,
# of Incremental SPF Calculations done   = 0,
# of Neighbors in Init State             = 0,
# of Neighbors in 2-Way State            = 0,
# of Neighbors in Exchange State         = 0,
# of Neighbors in Full State             = 0,
# of Interfaces attached                 = 0
Attached Interfaces                      = vlan-213
```

output definitions

Area Identifier	The unique 32-bit value, such as IP address, that identifies the OSPF area in the AS.
Admin Status	Whether the area is enabled or disabled.
Operational Status	Whether the area is active.
Area Type	The area type. This field will be **normal**, **stub**, or **NSSA**.
Area Summary	Whether Area Summary is enabled or disabled.
Time since last SPF Run	The last time the Shortest Path First calculation was performed.
# of Area Border Routers known	The number of Area Border Routers in the area.
# of AS Border Routers known	The number of Autonomous System Border Routers in the area.
# of LSAs	The total number of Link State Advertisements for the Area.
# of SPF Calculations	The number of times the area has calculated the Shortest Path.
# of Incremental SPF Calculations	The number of incremental Shortest Path First calculations that have been performed in the area.
# of Neighbors in Init State	The number of OSPF neighbors that are in initialization.
# of Neighbors in 2-Way State	The number of OSPF 2-way state neighbors in this area.
# of Neighbors in Exchange State	The number of OSPF neighbors that are currently establishing their status.
# of Neighbors in Full State	The number of OSPF neighbors.
# of Interfaces attached	The number of OSPF interfaces.
Attached Interfaces	The names of the OSPF interfaces attached to this area.

Release History

Release 5.1; command was introduced.

Related Commands

ip ospf area	Creates or deletes an OSPF area, assigning default metric, cost, and type.
ip ospf area range	Creates a route summarization instance whereby a range of addresses will be advertised as a single route.
show ip ospf interface	Displays OSPF interface information.

MIB Objects

```
ospfAreaTable
   ospfAreaId
   ospfImportAsExtern
   ospfSpfRuns
   ospfAreaBdrRtrCount
   ospfAsBdrRtrCount
   ospfAreaLsaCount
   ospfAreaSummary
   ospfAreaStatus
alaOspfIfAugTable
   alaOspfIfIntfName
```

show ip ospf area range

Displays all or specified route summaries in a given area.

show ip ospf area *area_id* **range [{summary | nssa}** *ip_address ip_mask***]**

Syntax Definitions

area_id	A unique 32-bit value in IP address format.
summary	Specifies that routes are summarized.
nssa	Specifies the Not So Stubby Area (NSSA) routers are summarized.
ip_address	A 32-bit IP address.
ip_mask	A 32-bit subnet mask.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Allows you to view the details of a specified OSPF area range.
- See the Related Commands section below for information on modifying an area.

Examples

```
-> show ip ospf area 0.0.0.0 range

     AreaId        Type     Destination        Advertise
---------------+---------+-----------------+-----------
0.0.0.0          Summary   192.168.12.1/24   Matching
0.0.0.0          NSSA      143.209.92.71/24  noMatching
```

output definitions

AreaId	The area identification for the area range.
Type	The type of area the range is associated with.
Destination	The destination address of the range.
Advertise	Shows the filter effect of the range. LSAs in the range are either advertised (Matching) or not advertised (noMatching).

Release History

Release 5.1; command was introduced.

Related Commands

ip ospf area range	Creates a route summarization instance whereby a range of addresses assigned for the route at the area border router will be advertised.

MIB Objects

```
ospfAreaRangeTable
   ospfAreaRangeAreaId
   ospfAreaRangeNet
   ospfAreaRangeMask
   ospfAreaRangeStatus
   ospfAreaRangeEffect
```

show ip ospf area stub

Displays stub default area metrics, if configured.

show ip ospf area *area_id* **stub**

Syntax Definitions

area_id	A unique 32-bit value in IP address format.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show ip ospf area 0.0.0.1 stub

    Area Id       TOS     Metric    MetricType
---------------+-------+----------+------------
0.0.0.1           1          1        ospf
```

output definitions

Area Id	The identification number of the stub area.
TOS	The Type of Service assignment.
Metric	The metric assignment of the default router in the stub area.
MetricType	The metric type of the stub area. It will be either **ospf**, **type1**, or **type2**.

Release History

Release 5.1; command was introduced.

Related Commands

ip ospf area	Creates or deletes an OSPF area.

MIB Objects

```
ospfStubAreaTable
   ospfStubAreaId
   ospfStubTOS
   ospfStubMetric
   ospfStubStatus
   ospfStubMetricType
```

show ip ospf interface

Displays OSPF interface information.

show ip ospf interface [*ip_address* **|** *interface_name***]**

Syntax Definitions

ip_address	The 32-bit IP address for the interface.
interface_name	The name of the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Not specifying an IP address displays all known interfaces for the OSPF router.

Examples

No IP address is specified (OmniSwitch 6600, 7700, 7800, 8800):

```
-> show ip ospf interface
    Interface                DR           Backup DR      Admin    Oper
      Name                 Address         Address       Status  Status  State
--------------------+---------------+---------------+--------+------+-------
vlan-213              213.10.10.1     213.10.10.254    enabled   up    DR
vlan-215              215.10.10.254   215.10.10.1      enabled   up    BDR
```

Output fields when no IP address is specified are described below:

output definitions

IP Address	The IP address assigned to the interface.
Interface Name	The name of the interface. This field is only displayed on OmniSwitch 6600, 7700, 7800, and 8800 switches.
DR Address	The designated router IP address on this network segment. Make sure you configure a VLAN for the router IP. (See Chapter 21, "VLAN Management Commands," for more information.)
Backup DR Address	The IP address of the backup designated router.
Vlan	The VLAN to which the interface is assigned.
Admin Status	The current administration status of the interface, either **enabled** or **disabled**.
Oper Status	Whether the interface is an active OSPF interface.
State	The current state of the OSPF interface. It will be **down**, **up**, **dp**, **dr**, or **other**.

The following is an example of MD5 authentication:

```
-> show ip ospf interface 100.10.10.2
Interface IP Name                     = vlan-3
VLAN Id                               = 3,
Interface IP Address                  = 100.10.10.2,
Interface IP Mask                     = 255.255.255.0,
Admin Status                          = Enabled,
Operational Status                    = Up,
OSPF Interface State                  = BDR,
Interface Type                        = Broadcast,
Area Id                               = 0.0.0.2,
Designated Router IP Address          = 100.10.10.88,
Designated Router RouterId            = 100.10.10.88,
Backup Designated Router IP Address   = 100.10.10.2,
Backup Designated Router RouterId     = 192.169.1.2,
MTU  (bytes)                          = 1500,
Metric Cost                           = 1,
Priority                              = 1,
Hello Interval (seconds)              = 10,
Transit Delay (seconds)               = 1,
Retrans Interval (seconds)            = 5,
Dead Interval (seconds)               = 40,
Poll Interval (seconds)               = 120,
Link Type                             = Broadcast,
Authentication Type                   = md5,
#   Id   Key   Status   StartAccept  StopAccept  StartGen  StopGen
--+----+-----+----------+-----------+-----------+---------+--------
1  1     Set  Enabled       0           0         0        0
# of Events                           = 2,
# of Init State Neighbors             = 0,
# of 2-Way State Neighbors            = 0,
# of Exchange State Neighbors         = 0,
# of Full State Neighbors             = 1
```

Note. See the table of the following page for output definitions.

The following is an example of simple authentication:

```
-> show ip ospf interface 100.10.10.2
Interface IP Name                     = vlan-3
VLAN Id                               = 3,
Interface IP Address                  = 100.10.10.2,
Interface IP Mask                     = 255.255.255.0,
Admin Status                          = Enabled,
Operational Status                    = Up,
OSPF Interface State                  = DR,
Interface Type                        = Broadcast,
Area Id                               = 0.0.0.2,
Designated Router IP Address          = 100.10.10.2,
Designated Router RouterId            = 192.169.1.2,
Backup Designated Router IP Address   = 0.0.0.0,
Backup Designated Router RouterId     = 0.0.0.0,
MTU  (bytes)                          = 1500,
Metric Cost                           = 1,
Priority                              = 1,
Hello Interval (seconds)              = 10,
Transit Delay (seconds)               = 1,
Retrans Interval (seconds)            = 5,
Dead Interval (seconds)               = 40,
Poll Interval (seconds)               = 120,
Link Type                             = Broadcast,
Authentication Type                   = simple,
Authentication Key                    = Set,
# of Events                           = 3,
# of Init State Neighbors             = 0,
# of Exchange State Neighbors         = 0,
# of 2-Way State Neighbors            = 0,
# of Full State Neighbors             = 0
```

Output fields when an IP address is specified are described below:

output definitions

Interface IP Name	The name of the VLAN to which the interface is assigned.
VLAN Id	The VLAN to which the interface is assigned.
Interface IP Address	The IP address assigned to the interface.
Interface IP Mask	The IP mask associated with the IP address assigned to the interface.
Admin Status	The current administration status of the interface, either **enabled** or **disabled**.
Operational Status	Whether the interface is an active OSPF interface.
OSPF Interface State	The current state of the OSPF interface. It will be **down**, **up**, **dp**, **dr**, or **other**.
Interface Type	The OSPF interface type, which can be Broadcast, NBMA, Point-to-Point, or Point-to-Multipoint.
Area Id	The area identification number to which the interface is assigned. This field is not applicable if an interface has not yet been assigned to an area
Designated Router IP Address	The designated router IP address.
Designated Router RouterId	The identification number of the designated router.

output definitions (continued)

Backup Designated Router IP Address	The IP address of the backup designated router.
Backup Designated Router RouterId	The identification number of the backup designated router.
MTU	The Maximum Transfer Unit (in bytes) for the interface.
Metric Cost	The cost added to routes learned on this interface.
Priority	The priority of the interface in regards to becoming the designated router. The higher the number, the higher the priority.
Hello Interval	The number of seconds between hello messages sent out on the interface.
Transit Delay	The estimated number of seconds required to transmit a link state update over this interface.
Retrans Interval	The number of seconds the interface waits before resending hello messages.
Dead Interval	The number of seconds the interface waits for hello messages received from a neighbor before declaring the neighbor as dead.
Poll Interval	The larger time interval, in seconds, between hello messages sent to inactive neighbors
Link Type	The IP interface type, either **broadcast** or **non broadcast**.
Authentication Type	The type of authentication used by this interface, either **none**, **simple**, or **md5**.
#	The indexing of the MD5 key. (This field is only displayed for MD5 authentication.)
Id	A key identifier that identifies the algorithm and MD5 secret key associated with this interface. (This field is only displayed for MD5 authentication.)
Key	Indicates whether the MD5 key has been set or not. (This field is only displayed for MD5 authentication.)
Status	The status of the configured MD5 authentication key. (This field is only displayed for MD5 authentication.)
StartAccept	The time that OSPF router will start accepting packets that have been created with this key. (This field is only displayed for MD5 authentication.)
StopAccept	The time that OSPF router will stop accepting packets that have been created with this key. (This field is only displayed for MD5 authentication.)
StartGen	The time that OSPF router will start using this key for packet generation. (This field is only displayed for MD5 authentication.)
StopGen	The time that OSPF router will stop using this key for packet generation. (This field is only displayed for MD5 authentication.)
Authentication Key	This field displays whether the authentication key has been configured or not. (This field is only displayed for simple and no authentication.)
# of Events	The number of interface state machine events.
# of Init State Neighbors	The number of OSPF neighbors in the initialization state.

output definitions (continued)

# of 2-Way State Neighbors	The number of OSPF 2-way state neighbors on this interface.
# of Exchange State Neighbors	The number of OSPF neighbors in the exchange state.
# of Full State Neighbors	The number of OSPF neighbors in the full state. The full state is a neighbor that is recognized and passing data between itself and the interface.

Release History

Release 5.1; command was introduced.
Release 5.1.6; *interface_name* parameter added.

Related Commands

ip ospf interface	Creates and deletes an OSPF interface.
ip ospf interface auth-key	Configures OSPF authentication key for simple authentication on an interface.
ip ospf interface dead-interval	Configures the OSPF interface dead interval.
ip ospf interface hello-interval	Configures the OSPF interface hello interval.
ip ospf interface md5	Creates and deletes the OSPF interface MD5 key identification number.
ip ospf interface md5 key	Configures the OSPF key string.
ip ospf interface cost	Configures the OSPF interface cost.
ip ospf interface poll-interval	Configures the OSPF poll interval for a Non Broadcast Multi Access (NBMA) interface.
ip ospf interface priority	Configures the OSPF interface priority.
ip ospf interface retrans-interval	Configures the OSPF interface retransmit interval.
ip ospf interface transit-delay	Configures the OSPF interface transit delay.
ip ospf interface auth-type	Sets the OSPF interface authentication type.
ip ospf interface area	Configures an OSPF interface area.
ip ospf interface type	Configures the OSPF interface type.
ip ospf interface status	Enables or disables the administration status on an OSPF interface.

MIB Objects

```
ospfIfTable
   ospfIfIpAddress
   ospfIfAreaId
   ospfIfType
   ospfIfAdminStat
   ospfIfRtrPriority
   ospfIfTransitDelay
   ospfIfRetransInterval
   ospfIfHelloInterval
   ospfIfRtrDeadInterval
   ospfIfPollInterval
   ospfIfState
   ospfIfDesignatedRouter
   ospfIfBackupDesignatedRouter
   ospfIfEvents
   ospfIfAuthType
   ospfIfStatus
   ospfIfAuthKey
alaOspfIfMd5Table
   alaOspfIfMd5IpAddress
   alaOspfIfMd5KeyId
   alaOspfIfMd5Key
   alaOspfIfMd5EncryptKey
   alaOspfIfMd5KeyStartAccept
   alaOspfIfMd5KeyStopAccept
   alaOspfIfMd5KeyStartGenerate
   alaOspfIfMd5KeyStopGenerate
alaOspfIfAugTable
   alaOspfIfIntfName
```

show ip ospf restart

Displays the OSPF graceful restart related configuration and status.

show ip ospf restart

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The minimum hardware configuration for this command is a redundant CMM configuration. This command is not supported on OmniSwitch 7700/7800/8800 switches with a single CMM or OmniSwitch 6600 Family switches in a standalone configuration.
- On OmniSwitch 6600 Family switches, a graceful restart is only supported only on active ports (i.e., interfaces), which are on the secondary or idle modules in a stack during a takeover. It is not supported on ports on a primary switch in a stack.

Examples

```
-> show ip ospf restart
Restart Support                     = Enabled,
Restart Interval (in seconds)       = 120,
Restart Status                      = Not Restarting,
Restart Age (in seconds)            = 0,
Last Restart Exit Reason            = None,
Restart Helper Support              = Enabled,
Restart Helper Strict Checking      = Enabled,
Restart Helper Mode                 = NotHelping
```

output definitions

Restart Support	The administrative status of OSPF graceful restart, which can be **Enabled** or **Disabled**.
Restart Interval	The configured OSPF hitless restart timeout interval, in seconds. Use the **ip ospf restart-interval** command to modify this parameter.
Restart Status	The current of status OSPF graceful restart, which can be **Not Restarting**, **Unplanned Restart** (after a CMM takeover), or **Planned Restart** (before CMM takeover).
Restart Age	The remaining time, in seconds, for the current OSPF graceful restart interval.

output definitions (continued)

Last Restart Exit Reason	The outcome of the last attempt at a graceful restart. If the value is **None**, then no restart has yet been attempted. If the value is **In Progress**, then a restart attempt is currently underway. Other possible values include **Completed** (successfully completed), **Timed Out** (timed out), and **Topology Changed** (aborted due to topology change).
Restart Helper Support	The administrative status of the capability of an OSPF router to operate in helper mode in response to a router performing a graceful restart, which can be **Enabled** or **Disabled**. Use the **ip ospf restart-helper status** command to modify this parameter.
Restart Helper Strict Checking	The administrative status of whether or not a changed Link State Advertisement (LSA) will result in termination of graceful restart by a helping router, which can be **Enabled** or **Disabled**. Use the **ip ospf restart-helper strict-lsa-checking-status** command to modify this parameter.
Restart Helper Mode	Whether this OSPF router is operating as a helper to a restarting router.

Release History

Release 5.1; command was introduced.

Related Commands

ip ospf restart-support	Administratively enables and disables support for the graceful restart feature on an OSPF router.

MIB Objects

```
alaProtocolOspf
   alaOspfRestartSupport
   alaOspfRestartInterval
   alaOspfRestartStatus
   alaOspfRestartAge
   alaOspfRestartExitReason
   alaOspfRestartHelperSupport
   alaOspfRestartHelperStrictLSAChecking
   alaOspfRestartHelperStatus
```

show ip ospf debug

Displays current OSPF debug level and types.

show ip ospf debug

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command is used to display the debugging information currently enabled for the OSPF router.
- See the related commands sections below to modify the list.

Examples

```
-> show ip ospf debug

Debug Level       = 0,
Types/Sections
error             = on,
warning           = on,
state             = on,
recv              = on,
send              = on,
flood             = on,
spf               = on,
lsdb              = on,
rdb               = on,
age               = on,
vlink             = on,
redist            = on,
summary           = on,
dbexch            = on,
hello             = on,
auth              = on,
area              = on,
intf              = on,
mip               = on,
info              = on,
setup             = on,
time              = on,
tm                = on,
restart          = on,
helper           = on
```

output definitions

Debug Level	The granularity of the debug messages. This number will be 10, 50, or 99, where the lower number is least specific.
error	The error debug messages status. Error messages provide information of program faults.
warning	The warning debug messages status. Debugging messages show router operation calls.
state	The state debug messages status. State messages show the router state in relation to its neighbors.
recv	The received OSPF packet debug messages status.
send	The status OSPF packet debug messages status.
flood	The flood debug messages status.
spf	The Shortest Path First (SPF) debug messages status.
lsdb	The Link State Database (LSDB) debug messages status.
rdb	The Routing Database (RDB) debug messages status.
age	The aging debug messages status.
vlink	The virtual link debug messages status.
redist	The redistribution debug messages status.
summary	The summary debug messages status. Summarization of routes can be set for stubby areas and NSSAs.
dbexch	The data base exchange debug messages status.
hello	The hello debug messages status.
auth	The authorization debug messages status.
area	The area related debug messages status.
intf	The interface related debug messages status.
mip	The MIP operations debug messages status.
info	The information debug messages status.
setup	The setup debug messages status.
time	The time debug messages status.
tm	The DRC debug messages status.
restart	The graceful helper debug messages status.
helper	The graceful helper debug messages status.

Release History

Release 5.1; command was introduced.

Related Commands

ip ospf debug-level	Configures OSPF debugging level.
ip ospf debug-type	Configures type of OSPF traffic to debug.

MIB Objects

```
alaOspfDebugConfig
   alaOspfDebugLevel
   alaOspfDebugError
   alaOspfDebugWarning
   alaOspfDebugState
   alaOspfDebugRecv
   alaOspfDebugSend
   alaOspfDebugFlood
   alaOspfDebugSPF
   alaOspfDebugLsdb
   alaOspfDebugRdb
   alaOspfDebugAge
   alaOspfDebugVlink
   alaOspfDebugRedist
   alaOspfDebugSummary
   alaOspfDebugDbexch
   alaOspfDebugHello
   alaOspfDebugAuth
   alaOspfDebugArea
   alaOspfDebugIntf
   alaOspfDebugMip
   alaOspfDebugInfo
   alaOspfDebugSetup
   alaOspfDebugTime
   alaOspfDebugTm
   alaOspfDebugRestart
   alaOspfDebugHelper
   alaOspfDebugAll
```

31 BGP Commands

This chapter describes the CLI commands used to configure the BGP (Border Gateway Protocol). BGP is a protocol for exchanging routing information between gateway hosts in a network of ASs (autonomous systems). BGP is the most common protocol used between gateway hosts on the Internet. The routing table exchanged contains a list of known routers, the addresses they can reach, and a preference metrics associated with the path to each router so that the best available route is chosen.

The Alcatel implementation of BGP-4 complies with the following RFCs: 1771, 2439, 2842, 2385, 1997, 1966, 1965, and 1657.

Note. In the following document, the BGP terms “peer” and “neighbor” are used interchangeably to mean any BGP entity known to the local router.

MIB information for BGP is as follows:

Filename: *AlcatelIND1Bgp.MIB*
Module: *ALCATEL-IND1-BGP-MIB*

Filename: *IETF_BGP4.MIB*
Module: *BGP4-MIB*

Global BGP Commands	**ip load bgp** **ip bgp status** **ip bgp autonomous-system** **ip bgp bestpath as-path ignore** **ip bgp cluster-id** **ip bgp default local-preference** **ip bgp fast-external-failover** **ip bgp always-compare-med** **ip bgp bestpath med missing-as-worst** **ip bgp client-to-client reflection** **ip bgp as-origin-interval** **ip bgp synchronization** **ip bgp confederation identifier** **ip bgp maximum-paths** **ip bgp log-neighbor-changes** **ip bgp dampening** **ip bgp dampening clear** **ip bgp debug-type** **ip bgp debug-level** **show ip bgp** **show ip bgp statistics** **show ip bgp dampening** **show ip bgp dampening-stats** **show ip bgp path** **show ip bgp routes** **show ip bgp debug**

Aggregate Configuration	**ip bgp aggregate-address** **ip bgp aggregate-address status** **ip bgp aggregate-address as-set** **ip bgp aggregate-address community** **ip bgp aggregate-address local-preference** **ip bgp aggregate-address metric** **ip bgp aggregate-address summary-only** **show ip bgp aggregate-address**
Network (local route) Configurations	**ip bgp network** **ip bgp network status** **ip bgp network community** **ip bgp network local-preference** **ip bgp network metric** **show ip bgp network**
Neighbor (Peer) Configuration	**ip bgp neighbor** **ip bgp neighbor status** **ip bgp neighbor advertisement-interval** **ip bgp neighbor clear** **ip bgp neighbor route-reflector-client** **ip bgp neighbor default-originate** **ip bgp neighbor timers** **ip bgp neighbor conn-retry-interval** **ip bgp neighbor auto-restart** **ip bgp neighbor maximum-prefix** **ip bgp neighbor md5 key** **ip bgp neighbor ebgp-multihop** **ip bgp neighbor description** **ip bgp neighbor next-hop-self** **ip bgp neighbor passive** **ip bgp neighbor remote-as** **ip bgp neighbor remove-private-as** **ip bgp neighbor soft-reconfiguration** **ip bgp neighbor stats-clear** **ip bgp confederation neighbor** **ip bgp neighbor update-source** **ip bgp neighbor in-aspathlist** **ip bgp neighbor in-communitylist** **ip bgp neighbor in-prefixlist** **ip bgp neighbor out-aspathlist** **ip bgp neighbor out-communitylist** **ip bgp neighbor out-prefixlist** **ip bgp neighbor route-map** **ip bgp neighbor clear soft** **show ip bgp neighbors** **show ip bgp neighbors policy** **show ip bgp neighbors timer** **show ip bgp neighbors statistics**

Policy Commands	**ip bgp policy aspath-list** **ip bgp policy aspath-list action** **ip bgp policy aspath-list priority** **ip bgp policy community-list** **ip bgp policy community-list action** **ip bgp policy community-list match-type** **ip bgp policy community-list priority** **ip bgp policy prefix-list** **ip bgp policy prefix-list action** **ip bgp policy prefix-list ge** **ip bgp policy prefix-list le** **ip bgp policy route-map** **ip bgp policy route-map action** **ip bgp policy route-map aspath-list** **ip bgp policy route-map asprepend** **ip bgp policy route-map community** **ip bgp policy route-map community-list** **ip bgp policy route-map community-mode** **ip bgp policy route-map lpref** **ip bgp policy route-map lpref-mode** **ip bgp policy route-map match-community** **ip bgp policy route-map match-mask** **ip bgp policy route-map match-prefix** **ip bgp policy route-map match-regexp** **ip bgp policy route-map med** **ip bgp policy route-map med-mode** **ip bgp policy route-map origin** **ip bgp policy route-map prefix-list** **ip bgp policy route-map weight** **ip bgp policy route-map community-strip** **show ip bgp policy aspath-list** **show ip bgp policy community-list** **show ip bgp policy prefix-list** **show ip bgp policy route-map**
Route import and export	**ip bgp redist-filter** **ip bgp redist-filter community** **ip bgp redist-filter effect** **ip bgp redist-filter local-preference** **ip bgp redist-filter metric** **ip bgp redist-filter subnets** **show ip bgp redist-filter**

ip load bgp

Loads the BGP protocol software into running memory on the switch. The image file containing BGP should already be resident in flash memory before issuing this command.

ip load bgp

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- This command requires that the BGP software be resident in flash memory in the active directory.
- Enter this command in the switch's configuration file (boot.cfg) to ensure BGP software is running after a reboot.
- The command does not administratively enable BGP on the switch; BGP will be disabled after issuing this command. You must issue the **ip bgp status** to start the BGP protocol.

Example

```
-> ip load bgp
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp autonomous-system	Unloads the BGP software from running memory.
ip bgp status	Administratively enables or disables BGP.

MIB Objects

```
alaDrcTmIPBgpStatus
```

ip bgp status

Administratively enables or disables BGP. The BGP protocol will not be active until you enable it using this command.

ip bgp status {enable | disable}

Syntax Definitions

enable	Enables BGP.
disable	Disables BGP.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- You must first load the BGP software into running memory using the **ip load bgp** command before initiating this command.
- Many BGP commands require that the protocol be disabled (**ip bgp status**) before issuing them.

Example

```
-> ip bgp status enable
-> ip bgp status disable
```

Release History

Release 5.1; command was introduced.

Related Commands

ip load bgp	Loads the BGP software.

MIB Objects

```
alaBgpGlobal
   alaBgpProtoStatus
```

ip bgp autonomous-system

Configures the Autonomous System (AS) number for this switch. This number identifies this BGP speaker (this switch) instance to other BGP routers. The AS number for a BGP speaker determines whether it is an internal or an external peer in relation to other BGP speakers. BGP routers in the same AS are internal peers while BGP routers in different ASs are external peers. BGP routers in the same AS exchange different routing information with each other than they exchange with BGP routers in external ASs. BGP speakers append their AS number to routes passing through them; this sequence of AS numbers is known as a route's AS path.

ip bgp autonomous-system *value*

Syntax Definitions

value	The AS number. The valid range is 1–65535

Defaults

parameter	default
value	1

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- A switch can belong to only one AS. Do not specify more than one AS value for each switch.
- The BGP protocol must be disabled (using the **ip bgp status** command) before using this command.

Example

```
-> ip bgp autonomous-system 64724
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp status	Enables and disables the BGP protocol.

MIB Objects

```
alaBgpGlobal
   alaBgpAutonomousSystemNumber
```

ip bgp bestpath as-path ignore

Indicates whether AS path comparison will be used in route selection. The AS path is the sequence of ASs through which a route has traveled. A shorter AS path is preferred over a longer AS path. The AS path is always advertised in BGP route updates. This command informs BGP to use the length of the AS path as a criteria for determining the best route.

ip bgp bestpath as-path ignore

no ip bgp bestpath as-path ignore

Syntax Definitions

N/A

Defaults

This command is enabled by default.

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- AS path comparison does not consider the type of links connecting the ASs along the path. In some cases a longer path over very fast connections may be a better route than a shorter path over slower connections. For this reason the AS path should not be the only criteria used for route selection. BGP considers local preference before AS path when making path selections.
- The BGP protocol must be disabled (using the **ip bgp status** command) before using this command.
- The **no** form of this command disables this feature after it has been enabled.

Example

```
-> ip bgp bestpath as-path ignore
-> no ip bgp bestpath as-path ignore
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp aggregate-address as-set	Specifies whether AS path aggregation is to be performed or not.
ip bgp policy aspath-list	Creates or removes an AS path list.
ip bgp default local-preference	Configures the default local preference (lpref) value to be used when advertising routes.

MIB Objects

```
alaBgpGlobal
   alaBgpAsPathCompare
```

ip bgp cluster-id

Configures a BGP cluster ID when there are multiple, redundant, route reflectors in a cluster. This command is not necessary for configurations containing only one route reflector.

ip bgp cluster-id *ip_address*

Syntax Definitions

ip_address	32-bit IP address that is the Cluster ID of the router acting as a route reflector.

Defaults

parameter	default
ip_address	0.0.0.0

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- In a route-reflection configuration where there are multiple route-reflectors in a cluster, use this command to configure this cluster ID. Configuring multiple route-reflectors enhances redundancy and avoids a single point of failure. When there is only one reflector in a cluster, the router ID of the reflector is used as the cluster-ID.
- The BGP protocol must be disabled (using the **ip bgp status** command) before using this command.
- Using many redundant reflectors in a single cluster places demands on the memory required to store routes for all redundant reflectors' peers.

Example

```
-> ip bgp cluster-id 1.2.3.4
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp status	Enables and disables BGP.
ip bgp client-to-client reflection	Enables route reflection and sets this speaker as the route reflector.

MIB Objects

```
alaBgpGlobal
   alaBgpClusterId
```

ip bgp default local-preference

Configures the default local preference (lpref) value to be used when advertising routes. A higher local preference value is preferred over a lower value. The local preference value is sent to all BGP peers in the local autonomous system; it is not advertised to external peers.

ip bgp default local-preference *value*

Syntax Definitions

value	The default local preference value for this switch. The valid range is 0–4294967295.

Defaults

parameter	default
value	100

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Unless a route is specifically configured for a different local preference value it will default to value you specify in this command. This value is used for routes learned from external autonomous systems (the local preference value is not advertised in routes received from external peers) and for aggregates and networks that do not already contain local preference values.
- This value is specific to the switch so it can compare its own local preference to those received in advertised paths. If other switches belong to the same AS, then they should use the same default local preference value.
- The BGP protocol must be disabled (using the **ip bgp status** command) before using this command.
- Entering the command with no value restores the default value.

Example

```
-> ip bgp default local-preference 200
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp aggregate-address local-preference	Sets the local preference for a BGP aggregate.
ip bgp network local-preference	Sets the local preference for a BGP network.

MIB Objects

```
alaBgpGlobal
   alaBgpDefaultLocalPref
```

ip bgp fast-external-failover

Enables fast external failover (FEFO). When enabled, FEFO resets a session when a link to a directly connected external peer is operationally down. The BGP speaker will fall back to Idle and then wait for a connection retry by the external peer that went down.

ip bgp fast-external-failover

no ip bgp fast-external-failover

Syntax Definitions

N/A

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- When enabled, this command allows BGP to take immediate action when a directly connected interface, on which an external BGP session is established, goes down. Normally BGP relies on TCP to manage peer connections. Fast External failover improves upon TCP by resetting connections as soon as they go down.
- The BGP protocol must be disabled (using the **ip bgp status** command) before using this command.
- Use the no form of this command to disable Fast External Failover.

Example

```
-> ip bgp fast-external-failover
-> no ip bgp fast-external-failover
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp neighbor clear	Restarts a BGP peer.
ip bgp neighbor auto-restart	Enables or disables BGP peer automatic restart.
ip bgp neighbor timers	Configures the time interval between KEEPALIVE messages sent by this peer and the tolerated hold time interval, in seconds, for messages to this peer from other peers.

MIB Objects

```
alaBgpFastExternalFailOver
```

ip bgp always-compare-med

Enables or disables Multi-Exit Discriminator (MED) comparison between peers in different autonomous systems. The MED value is considered when selecting the best path among alternatives; it indicates the weight for a particular exit point from the AS. A path with a lower MED value is preferred over a path with a higher MED value.

ip bgp always-compare-med

no ip bgp always-compare-med

Syntax Definitions

N/A

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- By default, BGP only compares MEDs from the same autonomous system when selecting routes. Enabling this command forces BGP to also compare MEDs values received from external peers, or other autonomous systems.
- The BGP protocol must be disabled (using the **ip bgp status** command) before using this command.
- Use the no form of this command to disable MED comparison for external peers.

Example

```
-> ip bgp always-compare-med
-> no ip bgp always-compare-med
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp bestpath med missing-as-worst	Configures the MED parameter when it is missing in a BGP path.

MIB Objects

```
alaBgpGlobal
   alaBgpMedAlways
```

ip bgp bestpath med missing-as-worst

Configures the MED parameter when it is missing in a BGP path.

ip bgp bestpath med missing-as-worst

no ip bgp bestpath med missing-as-worst

Syntax Definitions

N/A

Defaults

By default this command is disabled.

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- This command is used to specify how a missing MED in an external BGP path is to be treated for route selection purposes. The default behavior is to treat missing MEDs as zero (best). This command allows you to treat missing MEDs as worst (2^{32}-1) for compatibility reasons.
- Use the **no** form of the command to disabled missing MEDs as worst.
- The BGP protocol must be disabled (using the **ip bgp status** command) before using this command.

Example

```
-> ip bgp bestpath med missing-as-worst
-> no ip bgp bestpath med missing-as-worst
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp always-compare-med	Forces BGP to consider MED values from external routes.

MIB Objects

```
alaBgpGlobal
   alaBgpMissingMed
```

ip bgp client-to-client reflection

Enables or disables this BGP speaker (switch) to be a route reflector. Route reflectors advertise routing information to internal BGP peers, referred to as *clients*. BGP requires all internal routers to know all routes in an AS. This requirement demands a fully meshed (each router has a direct connection to all other routers in the AS) topology. Route reflection loosens the fully meshed restriction by assigning certain BGP routers as route reflectors, which take on the responsibility of advertising routing information to local BGP peers.

ip bgp client-to-client reflection

no ip bgp client-to-client reflection

Syntax Definitions

N/A

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- In addition to defining this switch as the route reflector, this command also enable route reflection for this cluster. After setting this command this reflector will begin using route reflection behavior when communicating to client and non-client peers.
- Once route reflectors are configured, you need to indicate the clients (those routers receiving routing updates from the reflectors) for each route reflector. Use the **ip bgp neighbor route-reflector-client** command to configure clients.
- The BGP protocol must be disabled (using the **ip bgp status** command) before using this command.
- The **no** form of this command disables the speaker as a route reflector.

Example

```
-> ip bgp client-to-client reflection
-> no ip bgp client-to-client reflection
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp status	Administratively disables BGP in this switch.
ip bgp neighbor route-reflector-client	Configures a BGP peer to be a client to the this route reflector.

MIB Objects

```
alaBgpGlobal
   alaBgpRouteReflection
```

ip bgp as-origin-interval

Specifies the frequency at which routes local to the autonomous system are advertised. These advertisements are also referred to as UPDATE messages. This interval applies to advertisements to internal peers.

ip bgp as-origin-interval *seconds*

no ip bgp as-origin-interval

Syntax Definitions

seconds	The update interval in seconds. The valid range is 1–65535.

Defaults

parameter	default
seconds	15

Usage Guidelines

- A lower value may increase the likelihood of route flapping as route status is updated more frequently.
- The **no** form of this command resets the feature to the default value.

Example

```
-> ip bgp as-origin-interval 15
-> no ip bgp as-origin-interval
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp neighbor advertisement-interval	Set the route advertisement interval for external peers.

MIB Objects

```
alaBgpGlobal
   alaBgpAsOriginInterval
```

ip bgp synchronization

Enables or disables BGP internal synchronization. Enabling this command will force all routers (BGP and non-BGP) in an AS to learn all routes learned over external BGP. Learning the external routes forces the routing tables for all routers in an AS to be synchronized and ensure that all routes advertised within an AS are known to all routers (BGP and non-BGP). However, since routes learned over external BGP can be numerous, enabling synchronization can place an extra burden on non-BGP routers.

ip bgp synchronization

no ip bgp synchronization

Syntax Definitions

N/A

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- A BGP router is not supposed to advertise routes learned through internal BGP updates unless those routes are also known by the primary internal routing protocol (e.g, RIP or OSPF). However, requiring all routers in an AS to know all external routes places a heavy burden on routers focusing mainly on Intra-AS routing. Therefore, disabling synchronization avoids this extra burden on internal routers. As long as all BGP routers in an AS are fully meshed (each has a direct connection to all other BGP routers in the AS) then the problem of unknown external router should not be a problem and synchronization can be disabled.
- By default, synchronization is disabled and the BGP speaker can advertise a route without waiting for the IGP to learn it. When the autonomous system is providing transit service, BGP should not propagate IGP paths until the IGP prefixes themselves are known to be reachable through IGP. If BGP advertises such routes before the IGP routers have learned the path, they will drop the packets causing a blackhole.
- The BGP protocol must be disabled (using the **ip bgp status** command) before using this command.
- Use the no form of this command to disable IGP synchronization.

Example

```
-> ip bgp synchronization
-> no ip bgp synchronization
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip bgp	Displays the current global settings for the local BGP speaker.

MIB Objects

```
alaBgpGlobal
   alaBgpIgpSynchStatus
```

ip bgp confederation identifier

Sets a confederation identification value for the local BGP speaker (this switch). A confederation is a grouping of sub-ASs into a single AS. To peers outside a confederation, the confederation appears to be a single AS. Within the confederation multiple ASs may exist and even exchange information with each other as using external BGP (EBGP).

ip bgp confederation identifier *value*

Syntax Definitions

value	The confederation identification value. The valid range is 0–65535.

Defaults

parameter	default
value	0

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- A value of 0 means this local speaker is not a member of any confederation.
- The BGP protocol must be disabled (using the **ip bgp status** command) before using this command.
- Use this command in conjunction with the **ip bgp confederation neighbor** command to specify those peers that are a members of the same confederation as the local BGP speaker.
- Entering the command with no value restores the default value.

Example

```
-> ip bgp confederation identifier 3
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp autonomous-system	Sets the AS number for this switch.
ip bgp confederation neighbor	Specifies peers that are members of a confederation.

MIB Objects

```
alaBgpGlobal
   alaBgpConfedId
```

ip bgp maximum-paths

Enables or disables support for multiple equal cost paths. When multipath support is enabled and the path selection process determines that multiple paths are equal when the router-id is disregarded, then all equal paths are installed in the hardware forwarding table. When multipath support is disabled, only the best route entry is installed in the hardware forwarding table.

ip bgp maximum-paths

no ip bgp maximum-paths

Syntax Definitions

N/A

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- The BGP protocol must be disabled (using the **ip bgp status** command) before using this command.
- Use the **no** form of this command to disable support for multiple equal cost paths.

Example

```
-> ip bgp maximum-paths
-> no ip bgp maximum-paths
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip bgp	Displays the current global settings for the local BGP speaker.

MIB Objects

```
alaBgpGlobal
   alaBgpMultiPath
```

ip bgp log-neighbor-changes

Enables or disables the logging of peer state changes. If enabled, this logging tracks changes in the state of BGP peers from ESTABLISHED to IDLE and from IDLE to ESTABLISHED. Viewing peer state logging requires that certain debug parameters be set.

ip bgp log-neighbor-changes

no ip bgp log-neighbor-changes

Syntax Definitions

N/A

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- The BGP protocol must be disabled (using the **ip bgp status** command) before using this command.
- In order to view peer state changes, you must also configure the level of debugging (using the **ip bgp debug-level** command). You must also enable the logging of peer information (using the **ip bgp debug-type** command).

Example

```
-> ip bgp log-neighbor-changes
-> no ip bgp log-neighbor-changes
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp status	Disables BGP within the switch.
ip bgp debug-level	Sets the BGP debug level.
ip bgp debug-type	Sets the type of debugging information to log.

MIB Objects

```
alaBgpGlobal
   alaBgpPeerChanges
```

ip bgp dampening

Enables or disables BGP route dampening or the suppression of unstable routes. Route dampening helps control the advertisement of routes that are going up and then down at an abnormally high rate. Routes that are changing states (available then unavailable) are said to be *flapping*.

ip bgp dampening [half-life *half_life* **reuse** *reuse* **suppress** *suppress* **max-suppress-time** *max_suppress_time***]**

no ip bgp dampening

Syntax Definitions

half_life	The half-life duration, in seconds. The valid range is 0–65535.
reuse	The number of route withdrawals set for the re-use value. The valid range is 1–9999.
suppress	The dampening cutoff value. The valid range is 1–9999.
max_suppress_time	The maximum number of seconds a route can be suppressed. The valid range is 0–65535.

Defaults

parameter	value
half_life	300
reuse	200
suppress	300
max_suppress_time	1800

This command is disabled by default.

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- BGP dampening is disabled by default. When enabled, route dampening suppresses routes that are unstable, or “flapping,” and disrupting the network.
- This command enables dampening, and can also be used to change the default times for the dampening variables.
- Use the dampening variables to set penalties, suppression limits, and reuse values for flapping routes.

- The half-life value configures the half-life duration for a reachable route. After the time interval specified in this command, the penalty value for the route will be reduced by half. This command sets the duration in seconds during which the accumulated stability value is reduced by half if the route is considered reachable, whether suppressed or not. A larger value may be desirable for routes that are known for their instability. A larger value will also result in a longer suppression time if the route exceeds the flapping rate.
- The reuse value configures the number of route withdrawals necessary to begin readvertising a previously suppressed route. If the penalty value for a suppressed route fall below this value, then it will be advertised again. This command sets the reuse value, expressed as a number of route withdrawals. When the stability value for a route reaches or falls below this value, a previously suppressed route will be advertised again. The instability metric for a route is decreased by becoming more stable and by passing half-life time intervals
- The suppress value configures the cutoff value, or number of route withdrawals, at which a flapping route is suppressed and no longer advertised to BGP peers. This value is expressed as a number of route withdrawals. When the stability value for a route exceeds this cutoff value, the route advertisement is suppressed.
- The max-suppress-time value configures the maximum time (in seconds) a route can be suppressed. This time is also known as the maximum holdtime or the maximum instability value. Once this time is reached the route flap history for a route will be deleted and the route will be advertised again (assuming it is still reachable). This maximum holdtime as applied on an individual route basis. Each suppressed route will be held for the amount of time specified in this command unless the route is re-advertised by falling below the reuse value.
- Entering the command with no variables returns the variables back to their defaults.
- The **no** form of the command disables dampening.

Example

```
-> ip bgp dampening
-> ip bgp dampening half-life 20 reuse 800 suppress 60 max-suppress-time 40
-> no ip bgp dampening
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp dampening clear	Clears the dampening history data for all routes on the switch, resetting route flap counters and unsuppressing any routes that had been suppressed due to route flapping violations.
show ip bgp dampening	Displays the BGP route dampening settings.
show ip bgp dampening-stats	Displays BGP dampening statistics.

MIB Objects

```
alaBgpGlobal
   alaBgpDampening
   alaBgpDampMaxFlapHistory
   alaBgpDampHalfLifeReach
   alaBgpDampReuse
   alaBgpDampCutOff
```

ip bgp dampening clear

Clears the dampening history data for all routes on the switch, resetting route flap counters and unsuppressing any routes that had been suppressed due to route flapping violations.

ip bgp dampening clear

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

Use this command to clear all of the currently stored information on routes for dampening purposes. When this command is entered, all route information in regards to dampening is cleared.

Example

```
-> ip bgp dampening clear
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp dampening	Enables or disables route dampening.

MIB Objects

```
alaBgpGlobal
   alaBgpDampeningClear
```

ip bgp debug-type

Sets the type of BGP debug messages that are produced.

ip bgp debug-type [warnings | tm | tcp | sync | sendudp | peer | redist | recvudp | policy | peer | open | notify | mip | local | keepalive | info | fsm | errors | damp | aggr | all]

Syntax Definitions

warnings	Track warning information.
tm	Track DRC Task Manager interaction.
tcp	Track TCP information.
sync	Track BGP synchronization information
sendudp	Track sent UDP information.
route	Track BGP route information.
redist	Track BGP redistribution information.
recvudp	Track received UDP information.
policy	Track BGP policy information.
peer	Track BGP peer information.
open	Track BGP OPEN messages.
notify	Track notify message information.
mip	Track software MIP information.
local	Track BGP local peer information.
keepalive	Track BGP KEEPALIVE message information.
info	Track BGP informational events.
fsm	Track BGP Finite State Machine events.
errors	Track ERROR message information.
damp	Track BGP dampening information.
aggr	Track BGP aggregate route information.
all	Track all of the information listed above.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

This command allows you to set the type of debugging information the switch records.

Example

```
-> ip bgp debug-type all
-> ip bgp debug-type tcp
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp debug-level	Sets the current BGP debug level.

MIB Objects

N/A

ip bgp debug-level

Sets the current BGP debug level.

ip bgp debug-level *level*

Syntax Definitions

level	The debug level. The higher the number, the more detailed the level of information kept. The range is 0 to 255.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- This command allows you to set the level of information that the switch records. The higher the number, the more detailed the information.
- The range is 0 to 255. The currently defined levels are as follows:

  10 - Critical/Fatal errors
  51 - Non-Fatal Errors
  71 - Low level of debug output
  74 - Medium level of debug output
  84 - High level of debug output

Example

```
-> ip bgp debug-level 51
-> ip bgp debug-level 84
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp debug-type	Sets the type of BGP debug messages that are produced.

MIB Objects

N/A

ip bgp aggregate-address

Creates and deletes a BGP aggregate route. Aggregate routes are used to reduce the size of routing tables by combining the attributes of several different routes and allowing a single aggregate route to be advertised to peers.

The base command (**ip bgp aggregate-address**) may be used with other keywords to set up aggregate address configuration. These keywords are listed here and described as separate commands later in this chapter. In addition, some keywords have a **no** form to remove the parameter or return it to its default.

ip bgp aggregate-address *ip_address ip_mask*
[status {enable | disable}]
[as-set]
[community *string***]**
[local-preference *value***]**
[metric *metric***]**
[summary-only]

no ip bgp aggregate-address *ip_address ip_mask*

Syntax Definitions

ip_address	32-bit IP address to be used as the aggregate address.
ip_mask	32-bit subnet mask that determines how many bits of the IP address denote the network number.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- This command allows administrative operations on a BGP aggregate. You must still enable the aggregate route through the **ip bgp aggregate-address status** command.
- You cannot aggregate an address (for example, 100.10.0.0) if you do not have at least one more-specific route of the address (for example, 100.10.20.0) in the BGP routing table.
- Only the aggregate is advertised unless aggregate summarization is disabled using the **ip bgp aggregate-address summary-only** command.
- Use the **no** form of this command to delete an aggregate route.

Example

```
-> ip bgp aggregate-address 172.22.2.0 255.255.255.0
-> no ip bgp aggregate-address 172.22.2.0 255.255.255.0
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp aggregate-address summary-only	Enables or disables aggregate summarization, which suppresses more-specific routes.

MIB Objects

```
alaBgpAggrAddr
alaBgpAggrSet
alaBgpAggrCommunity
alaBgpAggrLocalPref
alaBgpAggrMetric
alaBgpAggrSummarize
alaBgpAggrMask
```

ip bgp aggregate-address status

Enables or disables a BGP aggregate route.

ip bgp aggregate-address *ip_address ip_mask* **status {enable | disable}**

Syntax Definitions

ip_address	32-bit IP address for this aggregate route.
ip_mask	32-bit subnet mask that determines how many bits of the network address denote the network number.
enable	Enables this aggregate route.
disable	Disables this aggregate route.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Configure all aggregate route parameters before enabling the aggregate with this command. Use the **ip bgp aggregate-address** command to configure individual aggregate parameters.
- The **show ip bgp path** command displays every aggregate currently defined.

Example

```
-> ip bgp aggregate-address 172.22.2.0 255.255.255.0 status enable
-> ip bgp aggregate-address 172.22.2.0 255.255.255.0 status disable
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp aggregate-address	Creates an aggregate route.
show ip bgp path	Displays aggregate routes.

MIB Objects

```
alaBgpAggrTable
   alaBgpAggrAddr
   alaBgpAggrMask
```

ip bgp aggregate-address as-set

Specifies whether AS path aggregation is to be performed or not. AS path aggregation takes the AS path for all routes in this aggregate and creates a new AS path for the entire aggregate. This aggregated AS path includes all the ASs from the routes in the aggregate, but it does not repeat AS numbers if some routes in the aggregate include the same AS in their path.

ip bgp aggregate-address *ip_address ip_mask* **as-set**

no ip bgp aggregate-address *ip_address ip_mask* **as-set**

Syntax Definitions

ip_address	32-bit IP address.
ip_mask	32-bit subnet mask that determines how many bits of the IP address denote the network number.

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- When AS path aggregation is disabled (the default), the AS path for the aggregate defaults to the AS number of the local BGP speaker (configured in the **ip bgp autonomous-system** command).
- If AS path aggregation is enabled, a flap in a more specific path's AS path will cause a flap in the aggregate as well.
- Do not use this command when aggregating many paths because of the numerous withdrawals and updates that must occur as path reachability information for the summarized routes changes.
- The **no** form of this command disables the **as-set** option.

Example

```
-> ip bgp aggregate-address 172.22.2.115 255.255.255.0 as-set
-> no ip bgp aggregate-address 172.22.2.115 255.255.255.0 as-set
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp aggregate-address	Creates and deletes a BGP aggregate route.

MIB Objects

```
alaBgpAggrTable
   alaBgpAggrAddr
   alaBgpAggrMask
   alaBgpAggrSet
```

ip bgp aggregate-address community

Defines a community for an aggregate route created by the **ip bgp aggregate-address** command. Communities are a way of grouping BGP peers that do not share an IP subnet or an AS number.

ip bgp aggregate-address *ip_address ip_mask* **community** *string*

Syntax Definitions

ip_address	32-bit IP address of the aggregate route.
ip_mask	32-bit subnet mask that determines how many bits of the IP address denote the network number.
string	Community name, e.g., CommListAIn, ranging from 0 to 70 characters, or a value of none. The Community name is case sensitive.

Defaults

parameter	default
string	none

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

You can revert the aggregate community string to its default value by setting the community string to “none”. For example:

```
-> ip bgp aggregate-address 172.22.2.115 255.255.255.0 community none
```

Example

```
-> ip bgp aggregate-address 172.22.2.115 255.255.255.0 community no-export
-> no ip bgp aggregate-address 172.22.2.115 255.255.255.0 community no-export
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp aggregate-address	Creates and deletes a BGP aggregate route.

MIB Objects

```
alaBgpAggrTable
   alaBgpAggrAddr
   alaBgpAggrMask
   alaBgpAggrCommunity
```

ip bgp aggregate-address local-preference

Configures the local preference attribute value for this BGP aggregate. This value will override the default local preference value; it is used when announcing this aggregate to internal peers.

ip bgp aggregate-address *ip_address ip_mask* **local-preference** *value*

no ip bgp aggregate-address *ip_address ip_mask* **local-preference** *value*

Syntax Definitions

ip_address	An IP address for the aggregate route.
ip_mask	A 32-bit subnet mask that determines how many bits of the IP address denote the network number.
value	The local preference attribute. The valid range is 0–4294967295

Defaults

parameter	default
value	0

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- You can specify that this route use the default local preference value for the AS by specifying zero (0). In this case the local preference for this route will take the default local preference value set for this AS (defined in the **ip bgp default local-preference** command).
- The **no** form of this command sets the local preference back to the default value.

Example

```
-> ip bgp aggregate-address 172.22.2.115 255.255.255.0 local-preference 200
-> no ip bgp aggregate-address 172.22.2.115 255.255.255.0 local-preference 200
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp default local-preference	Sets the default local preference value for this AS.

MIB Objects

```
alaBgpAggrTable
   alaBgpAggrAddr
   alaBgpAggrMask
   alaBgpAggrLocalPref
```

ip bgp aggregate-address metric

Configures the MED attribute value for a BGP aggregate. This value is used when announcing this aggregate to internal peers; it indicates the best exit point from the AS.

ip bgp aggregate-address *ip_address ip_mask* **metric** *value*

no ip bgp aggregate-address *ip_address ip_mask* **metric** *value*

Syntax Definitions

ip_address	A 32-bit IP address.
ip_mask	A 32-bit subnet mask that determines how many bits of the IP address denote the network number.
value	The MED attribute. The valid range is 0–4294967295

Defaults

parameter	default
value	0

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- The default value of zero indicates that a MED will not be sent for this aggregate. When a MED value is missing for a route, BGP will determine a MED value based upon the settings specified in the **ip bgp bestpath med missing-as-worst** command.
- The **no** form of this command resets the aggregate metric back to its default value.

Example

```
-> ip bgp aggregate-address 172.22.2.115 255.255.255.0 metric 0
-> no ip bgp aggregate-address 172.22.2.115 255.255.255.0 metric 0
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp bestpath med missing-as-worst	Configures the MED for paths that do not contain a MED value.
ip bgp always-compare-med	Forces BGP to use the MED for comparison of external routes.

MIB Objects

```
alaBgpAggrTable
   alaBgpAggrAddr
   alaBgpAggrMask
   alaBgpAggrMetric
```

ip bgp aggregate-address summary-only

Enables or disables aggregate summarization, which supresses more-specific routes. Disabling aggregate summarization means that more-specific routes will be announced to BGP peers (internal and external peers).

ip bgp aggregate-address *ip_address ip_mask* **summary-only**

no ip bgp aggregate-address *ip_address ip_mask* **summary-only**

Syntax Definitions

ip_address	IP address for the aggreagte route.
ip_mask	32-bit subnet mask that determines how many bits of the IP address denote the network number.

Defaults

This command is enabled by default.

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- This command specifies whether more-specific routes should be announced or suppressed.
- By default, aggregate summarization is enabled, which means that only the aggregate entry (for example, 100.10.0.0) is advertised. Advertisements of more-specific routes (for example, 100.10.20.0) are suppressed.
- The **no** form of this command disables this feature.

Example

```
-> ip bgp aggregate-address 172.22.2.115 255.255.255.0 summary-only
-> no ip bgp aggregate-address 172.22.2.115 255.255.255.0 summary-only
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp aggregate-address	Creates and deletes a BGP aggregate route.

MIB Objects

```
alaBgpAggrTable
   alaBgpAggrAddr
   alaBgpAggrMask
   alaBgpAggrSummarize
```

ip bgp network

Creates or deletes a BGP network. A network must be known to the local BGP speaker; it also must originate from the local BGP speaker. The network may be directly connected, dynamically learned, or static.

In lieu of these options, the base command (**ip bgp network**) may be used with other keywords to set up network configuration. These keywords are listed here and described as separate commands later in this chapter. In addition, some keywords have a **no** form to remove the parameter or return it to its default.

ip bgp network *network_address ip_mask*
[community *string***]**
[local-preference *value***]**
[metric *metric***]**
[status {enable | disable}]

no ip bgp network *network_address ip_mask*

Syntax Definitions

network_address	32-bit IP address.
ip_mask	32-bit subnet mask that determines how many bits of the network address denote the network number.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Creating and enabling a network entry indicates to BGP that this network should originate from this router. The network specified must be known to the router, whether it is connected, static, or dynamically learned.
- You can create up to 200 network entries. The basic **show ip bgp path** command will display every network currently defined.
- This command allows administrative operations on a BGP network. You must still enable the network through the **ip bgp network status** command.
- Use the **no** form of this command to delete a local network.

Example

```
-> ip bgp network 172.22.2.115 255.255.255.0
-> no ip bgp network 172.22.2.115 255.255.255.0
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp network status	Enables a BGP network.

MIB Objects

```
alaBgpNetworkTable
   alaBgpNetworkAddr
   alaBgpNetwrokMetric
   alaBgpNetworkLocalPref
   alaBgpNetworkCommunity
   alaBgpNetworkMask
```

ip bgp network status

Enables or disables a BGP network.

ip bgp network *network_address ip_mask* **status {enable | disable}**

Syntax Definitions

network_address	32-bit IP address.
ip_mask	32-bit subnet mask that determines how many bits of the network address denote the network number.
enable	Enables this network.
disable	Disables this network.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Configure all network parameters before enabling this BGP network with this command. Use the **ip bgp network** command to configure individual aggregate parameters.
- You can create up 200 network entries. The **show ip bgp path** command displays every network currently defined.

Example

```
-> ip bgp network 172.22.2.115 255.255.255.0 status enable
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp network	Create a BGP network.
show ip bgp path	Display currently defined BGP networks.

MIB Objects

```
alaBgpNetworkTable
   alaBgpNetworkAddr
   alaBgpNetworkMask
```

ip bgp network community

Defines a community for a route created by the **ip bgp network** command. Communities are a way of grouping BGP peers that do not share an IP subnet or an AS.

ip bgp network *network_address ip_mask* **community** *string*

Syntax Definitions

network_address	32-bit IP address of the network.
ip_mask	32-bit subnet mask that determines how many bits of the network address denote the network number.
string	Community name, e.g., CommListAIn, ranging from 0 to 70 characters, or a value of none. The Community name is case sensitive.

Defaults

parameter	default
string	none

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

You can revert the network community string to its default value by setting the community string to “none”. For example:

```
-> ip bgp network 172.22.2.115 255.255.255.0 community none
```

Example

```
-> ip bgp network 172.22.2.115 255.255.255.0 community export
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp network	Creates or deletes a BGP network

MIB Objects

```
alaBgpNetworkTable
   alaBgpNetworkAddr
   alaBgpNetworkMask
   alaBgpNetworkCommunity
```

ip bgp network local-preference

Defines the local preference value for a route generated by the **ip bgp network** command. This value will override the default local preference value; it is used when announcing this network to internal peers.

ip bgp network *network_address ip_mask* **local-preference** *value*

no ip bgp network *network_address ip_mask* **local-preference** *value*

Syntax Definitions

network_address	A 32-bit IP address.
ip_mask	A 32-bit subnet mask that determines how many bits of the network address denote the network number.
value	The local preference attribute value. The valid range is 0–4294967295.

Defaults

parameter	default
value	0

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- You can specify that this route use the default local preference value for the AS by specifying zero (0). In this case the local preference for this route will take the default local preference value set for this AS (defined in the **ip bgp default local-preference** command).
- The **no** form of this command returns the local preference of the specified network to its default setting.

Example

```
-> ip bgp network 172.22.2.115 255.255.255.0 local-preference 600
-> no ip bgp network 172.22.2.115 255.255.255.0 local-preference 600
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp network	Creates or deletes a BGP network.
ip bgp default local-preference	Sets the default local preference for this AS.

MIB Objects

```
alaBgpNetworkTable
   alaBgpNetworkAddr
   alaBgpNetworkMask
   alaBgpNetworkLocalPref
```

ip bgp network metric

Configures the Multi-Exit Discriminator (MED) attribute value for an network generated by the **ip bgp network** command. This value is used when announcing this network to internal peers; it indicates the best exit point from the AS.

ip bgp network *network_address ip_mask* **metric** *value*

no ip bgp network *network_address ip_mask* **metric** *value*

Syntax Definitions

network_address	A 32-bit IP address.
ip_mask	A 32-bit subnet mask that determines how many bits of the network address denote the network number.
value	A MED attribute value. The valid range is 0–4294967295.

Defaults

parameter	default
value	0

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- The default value of zero indicates that a MED will not be sent for this network. When a MED value is missing for a route, BGP will determine a MED value based upon the settings specified in the **ip bgp bestpath med missing-as-worst** command.
- The **no** form of this command returns the metric for this network to its default value.

Example

```
-> ip bgp network 172.22.2.115 255.255.255.0 metric 100
-> no ip bgp network 172.22.2.115 255.255.255.0 metric 100
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp network	Creates or deletes a BGP network.
ip bgp bestpath med missing-as-worst	Specifies the MED value when it is missing.

MIB Objects

```
alaBgpNetworkTable
   alaBgpNetworkAddr
   alaBgpNetworkMask
   alaBgpNetwrokMetric
```

ip bgp neighbor

Creates or deletes a BGP peer.

ip bgp neighbor *ip_address*

no ip bgp neighbor *ip_address*

Syntax Definitions

ip_address	32-bit IP address of the new BGP peer.

Defaults

No peers configured.

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- You must still enable a BGP peer after creating it. A BGP peer is enabled using the **ip bgp neighbor status** command.
- Once created, a BGP peer cannot be enabled until it is assigned an autonomous system number using the **ip bgp neighbor remote-as** command.
- Use the **no** form of this command to delete a BGP peer.

Example

```
-> ip bgp neighbor 172.22.2.115
-> no ip bgp neighbor 172.22.2.115
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp neighbor status	Enable or disable a BGP peer.
ip bgp neighbor remote-as	Configure the AS number for the peer.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
```

ip bgp neighbor status

Enables or disables a BGP peer.

ip bgp neighbor *ip_address* **status {enable | disable}**

Syntax Definitions

ip_address	32-bit IP address of the new BGP peer.
enable	Enables this peer.
disable	Disables this peer.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- You must first create a peer and assign it an IP address using the **ip bgp neighbor** command before enabling the peer.
- Configure all BGP peer related commands before enabling a peer using this command. Once you enable the peer it will begin sending BGP connection and route advertisement messages.

Example

```
-> ip bgp neighbor 172.22.2.115 status enable
-> ip bgp neighbor 172.22.2.115 status disable
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp neighbor	Creates a BGP peer.
show ip bgp neighbors	Displays peer parameters.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
```

ip bgp neighbor advertisement-interval

Configures the time interval for updates between external BGP peers.

ip bgp neighbor *ip_address* **advertisement-interval** *value*

Syntax Definitions

ip_address	32-bit IP address of the neighbor.
value	An advertisement time interval in seconds. The valid range is 0–65535.

Defaults

parameter	default
value	30

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

Internal peers sharing the same AS as the local BGP speaker (configured in the **ip bgp autonomous-system** command) use the global route advertisement update interval. This command sets the interval this peer uses to send BGP UPDATE messages to external peers.

Example

```
-> ip bgp neighbor 172.22.2.115 255.255.255.0 advertisement-interval 60
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip bgp neighbors	Displays BGP peer main status.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   bgpPeerMinRouteAdvertisementTinterval
```

ip bgp neighbor clear

Restarts a BGP peer. The peer will be unavailable during this restart.

ip bgp neighbor *ip_address* **clear**

Syntax Definitions

ip_address	32-bit IP address of the neighbor.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Use this command whenever changes occur to BGP-related access lists, weights, distribution lists, timer specifications, or administrative distance.
- Many peer commands restart the peer as soon as they are configured. The following commands restart the BGP peer for which they are configured:

  ip bgp neighbor remote-as
  ip bgp neighbor md5 key
  ip bgp neighbor passive
  ip bgp neighbor ebgp-multihop
  ip bgp neighbor maximum-prefix
  ip bgp neighbor update-source
  ip bgp neighbor next-hop-self
  ip bgp neighbor soft-reconfiguration
  ip bgp neighbor route-reflector-client
  ip bgp confederation neighbor
  ip bgp neighbor remove-private-as
  ip bgp neighbor update-source.

- You do not need to issue the **ip bgp neighbor clear** command after issuing any of the above commands.

Example

```
-> ip bgp neighbor 172.22.2.115 clear
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp neighbor auto-restart	Automatically attempts to restart a BGP peer session after a session terminates.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerRestart
```

ip bgp neighbor route-reflector-client

Configures this peer as a client to the local route reflector.

ip bgp neighbor *ip_address* **route-reflector-client**

no ip bgp neighbor *ip_address* **route-reflector-client**

Syntax Definitions

ip_address	32-bit IP address of the neighbor.

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- This command configures this peer as one of the clients to the local route reflector.
- All of the peers configured using this command become part of the client group. The remaining peers are members of the non-client group for the local route reflector.
- When route reflection is configured all of the internal BGP speakers in an autonomous system need not be fully meshed. The route reflector take responsibility for passing internal BGP-learned routes to its peers.
- Use the **no** form of this command to remove this peer as a client to the local route reflector.

Example

```
-> ip bgp neighbor 172.22.2.115 route-reflector-client
-> no ip bgp neighbor 172.22.2.115 route-reflector-client
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp client-to-client reflection Configures the local BGP speaker as a route reflector

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerClientStatus
```

ip bgp neighbor default-originate

Enables or disables BGP peer default origination.

ip bgp neighbor *ip_address* **default-originate**

no ip bgp neighbor *ip_address* **default-originate**

Syntax Definitions

ip_address	32-bit IP address of the neighbor.

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

When this command is enabled, the local BGP speaker advertises itself as a default to the peer. Such a default route overrides any learned default (propagation) and outbound policy. The default route 0.0.0.0 does not need to exist on the local router.

The **no** form of this command disables this feature.

Example

```
-> ip bgp neighbor 172.22.2.115 default-originate
-> no ip bgp neighbor 172.22.2.115 default-originate
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp neighbor	Creates or deletes a BGP peer.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerDefaultOriginate
```

ip bgp neighbor timers

Configures the KEEPALIVE message interval and hold time interval (in seconds) with regards to the specified peer.

ip bgp neighbor *ip_address* **timers** *keepalive holdtime*

Syntax Definitions

ip_address	A 32-bit IP address for the BGP peer.
keepalive	The interval (in seconds) between KEEPALIVE messages. The valid values are zero (0) or the range 1–21845.
holdtime	The hold time interval between updates to peers, in seconds. The valid range is 0, 3–65535.

Defaults

parameter	default
keepalive	30
holdtime	90

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Configures the time interval between KEEPALIVE messages sent by this peer. KEEPALIVE messages do not contain route updates or indicate a change in the status of the BGP peer; they serve only to tell the receiving BGP peer that the connection is still live and the peer is reachable.
- By default, the keep alive interval of 30 seconds is one-third the default hold-time interval of 90 seconds. The keep alive interval can never be more than one-third the value of the hold-time interval. When the hold interval is reached without receiving keep alive or other updates messages, the peer is considered dead.
- Setting the keep alive value to zero means no keep alive messages will be sent.
- You must restart the peer (using the **ip bgp neighbor clear** command) after issuing this command before the new keep-alive time interval takes effect.
- Once a connection is established with a peer and a time period of the length specified in this command transpires with no messages from the remote peer, then the connection with that remote peer will be considered dead.
- Configures the tolerated hold time interval, in seconds, for messages to this peer from other peers. The hold timer is used during the connection setup process and in on-going connection maintenance with BGP peers. If this peer does not receive a KEEPALIVE, UPDATE, or NOTIFICATION message within this time period, then the BGP connection will be closed.

- By default, the hold-interval of 180 seconds is three times the default keep-alive interval of 60 seconds. The hold-interval can never be less than three times the keep-alive value.
- You must restart the peer (using the **ip bgp neighbor clear** command) after issuing this command before the new hold time interval takes effect.
- Both values must be set at the same time.
- Entering this command without the variables resets the variables to their default value.

Example

```
-> ip bgp neighbor 172.22.2.115 timers 80 240
-> ip bgp neighbor 172.22.2.115 timers
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp neighbor conn-retry-interval	The interval, in seconds, between BGP retries to set up a connection via the transport protocol with another peer.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   bgpPeerHoldTimeConfigured
   bgpPeerKeepAliveConfigured
```

ip bgp neighbor conn-retry-interval

The interval, in seconds, between BGP retries to set up a connection via the transport protocol with another peer. In the connect state, BGP tries to set up a connection with a remote peer. If the connection fails, then the connect retry interval is started. Once this interval elapses, BGP retries setting up the connection.

ip bgp neighbor *ip_address* **conn-retry-interval** *seconds*

Syntax Definitions

ip_address	A 32-bit IP address for the neighbor.
seconds	The time interval (in seconds) between retries. The valid range is 0–65535.

Defaults

parameter	default
seconds	120

Usage Guidelines

- The time interval is started when a connection to a peer is lost.
- Other BGP peers may automatically attempt to restart a connection with this peer if they have configured automatic peer session restart (using the **ip bgp neighbor auto-restart** command).
- You must restart the peer (using the **ip bgp neighbor clear** command) after issuing this command before the new connection retry interval takes effect.
- Entering this command without the *seconds* variable resets the variable to its default value.

Example

```
-> ip bgp neighbor 172.22.2.115 connect-interval 60
-> ip bgp neighbor 172.22.2.115 connect-interval
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp neighbor auto-restart	Enable automatic session restart after a session termination.
ip bgp neighbor clear	Restarts the peer.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   bgpPeerConnectRetryInterval
```

ip bgp neighbor auto-restart

Enables or disables BGP peer automatic restart. When enabled, this peer will automatically attempt to restart a session with another peer after a session with that peer terminates. When disabled, this peer will not try to re-establish a session with another peer after the session terminates; in such a case, the other peer will have to restart the session for the two peers to resume communication.

ip bgp neighbor *ip_address* **auto-restart**

Syntax Definitions

ip_address	32-bit IP address for the neighbor.

Defaults

This command is enabled by default.

Usage Guidelines

- After a session with another peer terminates, the local BGP speaker will wait 60 seconds before attempting to restart the session. If the session does not start on the first attempt a second attempt will be made after another 120 seconds (60x2). On each unsuccessful session attempt, the previous delay between restarts is multiplied by 2, up to a maximum delay of 240 seconds. An exception to this rule occurs when the peer session terminates on receipt of a NOTIFY message with 'unsupported option' code or 'unsupported capability' code; in these cases the delay between restart attempts will begin at 1 second and multiply by 2 after each unsuccessful restart attempt (up to a maximum of 240 second delay).
- Use the **no** form of this command to disable automatic peer restart.
- Disabling this option can be helpful in cases where other peers are prone to frequent flapping or sending many NOTIFY messages. By not restarting sessions with unstable neighbors, the local BGP speaker forces those unstable neighbors to re-initialize the connection.

Example

```
-> ip bgp neighbor 172.22.2.115 auto-restart
-> no ip bgp neighbor 172.22.2.115 auto-restart
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp neighbor	Creates a BGP peer.
ip bgp neighbor status	Enables a BGP peer.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerAutoRestart
```

ip bgp neighbor maximum-prefix

Configures the maximum number of prefixes, or paths, the local router can receive from this peer in UPDATE messages.

ip bgp neighbor *ip_address* **maximum-prefix** *maximum* **[warning-only]**

Syntax Definitions

ip_address	A 32-bit IP address of the BGP peer.
maximum	The maximum number of prefixes. The valid range is 0–4294967295.

Defaults

parameter	default
threshold	5000

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- When the number of prefixes sent by this peer reaches this limit, the peer is restarted.
- You can use BGP logging to receive a warning when the number of prefixes received from this peer reaches 80 percent of the value you configure in this command.
- If the **warning-only** prefix is used, the operator will be warned when the peer exceeds 80 percent of the configured number of maximum prefixes. To see this warning message, you must configure the level of debugging (using the **ip bgp debug-level** command) to 20. You must also activate the **recvupd** debug type (using the **ip bgp debug-type** command).
- The BGP peer is restarted after issuing this command.

Example

```
-> ip bgp neighbor 172.22.2.115 maximum-prefix 1000
-> ip bgp neighbor 172.22.2.115 maximum-prefix 1000 warning only
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp neighbor clear	Restarts the BGP peer.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerMaxPrefixWarnOnly
   alaBgpPeerMaxPrefix
```

ip bgp neighbor md5 key

Sets an encrypted MD5 signature for TCP sessions with this peer in compliance with RFC 2385.

ip bgp neighbor *ip_address* **md5 key {***string* **| none}**

Syntax Definitions

ip_address	32-bit IP address of the BGP peer.
string	The MD5 public key. Maximum character length is 200.
none	Removes the MD5 public key.

Defaults

parameter	default
string	no password

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Due to security concerns the actual password that you specify in this command is encrypted using a 3DES algorithm before it appears in a saved snapshot file. Also, if you were to view this command in a snapshot file, or **boot.cfg** file, it would appear in a different syntax. The syntax for this command used for snapshot files is as follows:

  ip bgp neighbor *ip_address* **md5 key-encrypt** *encrypted_string*

  However, you should not use this syntax to actually set an MD5 password; it will not work.
- Entering the keyword **none** in place of a key removes the password and disables authentication.
- The BGP peer is restarted after issuing this command.

Example

```
-> ip bgp neighbor 172.22.2.115 md5 key openpeer5
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp neighbor clear	Restarts the BGP peer.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerMD5Key
```

ip bgp neighbor ebgp-multihop

Allows external peers to communicate with each other even when they are not directly connected. The absence of communication between disconnected peers can occur when a router that is not running BGP sits between two BGP speakers; in such a scenario the BGP speakers are multiple hops from each other. By enabling this command, you allow the BGP peers to speak to each other despite the non-BGP router that sits between them.

ip bgp neighbor *ip_address* **ebgp-multihop [***ttl***]**

no ip bgp neighbor *ip_address* **ebgp-multihop**

Syntax Definitions

ip_address	32-bit IP address of the BGP peer.
ttl	The Time to Live for the multi-hop connection, in seconds. The range is 1 to 255.

Defaults

parameter	default
ttl	255

This command is disabled by default.

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- By default an external BGP peer is on a directly connected subnet. This command allows you to configure an external BGP peer that is not directly connected and may be multiple hops away. It should be used with caution and only with the guidance of qualified technical support.
- As a safeguard against loops, the multi-hop connection will not be made if the only route to a multi-hop peer is the default route (0.0.0.0).
- Use the **no** form of this command to disable multi-hop connections.
- The BGP peer is restarted after issuing this command.

Example

```
-> ip bgp neighbor 172.22.2.115 ebgp-multihop 250
-> no ip bgp neighbor 172.22.2.115 ebgp-multihop 50
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp neighbor	Creates or deletes a BGP peer.
ip bgp neighbor next-hop-self	Sets the BGP peer to use next hop processing behavior.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerMultiHop
```

ip bgp neighbor description

Configures the BGP peer name.

ip bgp neighbor *ip_address* **description** *string*

Syntax Definitions

ip_address	32-bit IP address of the BGP peer.
string	Peer name (1 - 20 characters).

Defaults

parameter	default
string	peer(ip_address)

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- The peer name is a text identifier that, by default, follows the format “peer(x.x.x.x)” where x.x.x.x is the IP address of the BGP peer. For example, the default name of a peer at address 198.216.14.23 would be “peer(198.216.14.23)”.
- A peer name with embedded spaces must be enclosed in quotation marks.

Example

```
-> ip bgp neighbor 172.22.2.115 description “peer for building 3”
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp neighbor	Sets the IP address for the peer.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerName
```

ip bgp neighbor next-hop-self

Sets the BGP peer to use next hop processing behavior. By default, the next-hop processing of BGP updates is disabled. Using this command to enable next-hop behavior may be useful in non-meshed networks where BGP peers do not have direct access to other peers.

ip bgp neighbor *ip_address* **next-hop-self**

no ip bgp neighbor *ip_address* **next-hop-self**

Syntax Definitions

N/A

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- In partially meshed networks a BGP peer may not have direct connections to other peers. When such a peer receives route updates from these distant peers (via other peers), it may treat the remote peer as if it were the next hop in the routing path. Packet forwarding will not work in such a case because no direct connection exists. This command allows this peer to deem itself the next hop on the routing path so that the two non-connected peers can route packets. This peer would have a direct connection to both peers that want to exchange packets.
- Use the **no** form of this command to disable next hop processing behavior.
- The BGP peer is restarted after issuing this command.

Example

```
-> ip bgp neighbor 172.22.2.115 next-hop-self
-> no ip bgp neighbor 172.22.2.115 next-hop-self
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp neighbor	Creates or deletes a BGP peer.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerNextHopSelf
```

ip bgp neighbor passive

Configures the local BGP speaker to wait for this peer to establish a connection. When enabled, the local BGP speaker will not initiate a peer session with this peer; in this sense, the BGP speaker is “passive.” When disabled, the local BGP speaker will attempt to set up a session with this peer.

ip bgp neighbor *ip_address* **passive**

no ip bgp neighbor *ip_address* **passive**

Syntax Definitions

ip_address	32-bit IP address of the BGP peer.

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- By default BGP will initiate a session to a peer once the peer is configured, has an AS number, and is enabled. You can use this command to configure the local BGP speaker as passive and an outbound session will not be initiated to this peer. For such peers, BGP will always wait passively for the inbound session attempt.
- Use the **no** form of this command to disable passive peer behavior.
- The BGP peer is restarted after issuing this command.

Example

```
-> ip bgp neighbor 172.22.2.115 passive
-> no ip bgp neighbor 172.22.2.115 passive
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp neighbor	Creates or deletes a BGP peer.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerPassive
```

ip bgp neighbor remote-as

Assigns an AS number to this BGP peer.

ip bgp neighbor *ip_address* **remote-as** *value*

Syntax Definitions

ip_address	32-bit IP address of the BGP peer.
value	Autonomous system number in the range 1 - 65535.

Defaults

parameter	default
value	1

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- A BGP peer created with the **ip bgp neighbor** command cannot be enabled (**ip bgp neighbor status enable**) until it is assigned an autonomous system number. If the AS number matches the AS number assigned to the local BGP speaker (assigned using the **ip bgp autonomous-system** command), the peer is considered internal to the local autonomous system. Otherwise, the peer is consider external to the local BGP speaker's AS.
- This BGP peer may not be operational within this switch and it may be in an external AS, but it must still be configured on this switch before the local BGP speaker can establish a connection to the peer. The local BGP speaker does not auto-discover peers in other switches; it initially learns about peers through the peer commands.
- The BGP peer is restarted after issuing this command.

Example

```
-> ip bgp neighbor 172.22.2.115 remote-as 100
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp autonomous-system	Set the AS for the local BGP speaker.
ip bgp neighbor	Create a BGP peer.
ip bgp neighbor status enable	Enables a BGP peer.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerAS
```

ip bgp neighbor remove-private-as

Enables or disables the stripping of private autonomous system numbers from the AS path of routes destined to this peer.

ip bgp neighbor *ip_address* **remove-private-as**

no ip bgp neighbor *ip_address* **remove-private-as**

Syntax Definitions

ip_address	32-bit IP address of the BGP peer.

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- By default all AS numbers in the AS path are passed to peers. Enabling his command strips any private AS numbers in the AS path before sending updates to this peer. AS numbers in the range 64512 to 65535 are considered private ASs; they intended for internal use within an organization (such as an enterprise network), but they are not intended for use on public networks (such as the Internet).
- This command has no effect if you are not using ASs in the range 64512 to 65535.
- Use the **no** form of this command to disable stripping of private AS numbers.
- The BGP peer is restarted after issuing this command.

Example

```
-> ip bgp neighbor 172.22.2.115 remove-private-as
-> no ip bgp neighbor 172.22.2.115 remove-private-as
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp neighbor remote-as	Configures the AS number for this peer.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerRemovePrivateAs
```

ip bgp neighbor soft-reconfiguration

Enables or disables BGP peer soft reconfiguration. Soft reconfiguration increases the stability of the peer by allowing you to reconfigure attributes that require peer resets without halting the TCP connection with other peers.

ip bgp neighbor *ip_address* **soft-reconfiguration**

no ip bgp neighbor *ip_address* **soft-reconfiguration**

Syntax Definitions

ip_address	32-bit IP address of the BGP peer.

Default

This command is enabled by default.

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- This feature stores routes and other configuration information in local memory. When you make configuration changes that require a peer reset, the routing cache is not cleared and connections with other peers are not interrupted.
- By default BGP stores all paths from peers, even those that are policy rejected, in anticipation of policy changes in the future. Storing these paths consumes memory. You can use this command to disable the storing of these paths, or soft reconfiguration. However, if soft reconfiguration is disabled and the inbound policy changes, the peer will have to be restarted using the **ip bgp neighbor out-aspathlist** command.
- The **no** form of this command disables this feature.
- The BGP peer is restarted after issuing this command.

Example

```
-> ip bgp neighbor 172.22.2.115 soft-reconfiguration
-> no ip bgp neighbor 172.22.2.115 soft-reconfiguration
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp neighbor clear	Restarts this BGP peer.
ip bgp neighbor out-aspathlist	Resets inbound policies to this peer.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerSoftReconfig
```

ip bgp neighbor stats-clear

Clears the statistics for a peer.

ip bgp neighbor *ip_address* **stats-clear**

Syntax Definitions

ip_address	32-bit IP address of the BGP peer.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- This command clears the statistical variables for a peer so they can accumulate from a known point.
- The cleared statistics include the total messages sent and received from this peer, the total UPDATE messages sent and received from this peer, the total NOTIFY messages sent and received from this peer, and the total peer state transition messages sent and received from this peer. These statistics can be displayed through **show ip bgp neighbors statistics**.

Example

```
-> ip bgp neighbor 172.22.2.115 stats-clear
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip bgp neighbors statistics	Displays peer statistics.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerClearCounter
```

ip bgp confederation neighbor

Configures this peer as a member of the same confederation as the local BGP speaker.

ip bgp confederation neighbor *ip_address*

no ip bgp confederation neighbor *ip_address*

Syntax Definitions

ip_address	32-bit IP address of the peer.

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- You must first assign a confederation number to the local BGP speaker before assigning peers to the confederation. Use the **ip bgp confederation identifier** command to assign a confederation number to the local BGP speaker.
- The **no** form of this command disables this feature.
- The BGP peer is restarted after issuing this command.

Example

```
-> ip bgp confederation neighbor 172.22.2.115
-> no ip bgp confederation neighbor 172.22.2.115
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp confederation identifier	Sets a confederation identification value for the local BGP speaker (this switch).

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerConfedStatus
```

ip bgp neighbor update-source

Configures the local address from which this peer will be contacted. This local address can be configured for internal and external BGP peers.

ip bgp neighbor *ip_address* **update-source [***interface_address* **|** *interface_name***]**

Syntax Definitions

ip_address	The 32-bit IP address for this peer.
interface_address	The 32-bit IP address for the local BGP router.
interface_name	The name of the interface.

Defaults

parameter	default
interface_address	0.0.0.0

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- This address does not override the router identification for this BGP peer (configured in the **ip bgp neighbor** command). It is the address through which this peer can be contacted within this switch. The router identification for a peer, especially an external peer, may not exist in the local switch, but that distant peer can still be contacted via this switch. This command sets the local address through which this distant peer can be contacted.
- The default is restored by entering the command without a IP address.
- The BGP peer is restarted after issuing this command.
- The update-source is not related to the router ID, it specifies the interface to be used for the TCP connection endpoint. By default, the nearest interface is selected.

Example

```
-> ip bgp neighbor 172.22.5.115 update-source 172.22.2.117
-> ip bgp neighbor 172.22.5.115 update-source vlan-22
-> ip bgp neighbor 172.22.5.115 update-source
```

Release History

Release 5.1; command was introduced.
Release 5.1.6; *interface_name* parameter added.

Related Commands

ip bgp neighbor	Sets the router identification for a BGP peer.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerLocalAddr
   alaBgpPeerLocalIntfName
```

ip bgp neighbor in-aspathlist

Assigns an inbound AS path list filter to a BGP peer.

ip bgp neighbor *ip_address* **in-aspathlist {***string* | **none}**

Syntax Definitions

ip_address	32-bit IP address of the BGP peer.
string	Inbound AS path list (0 to 70 characters). This name is case sensitive.
none	Removes this AS path list from the peer.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- The AS path list name *(***InboundASpath** in the example below) is created using the **ip bgp policy aspath-list** command. Any inbound routes from the BGP peer must match this AS path filter before being accepted or passed to inbound policy.
- To deassign an input AS path filter list, use this command to assign a value of **none**.

Example

```
-> ip bgp neighbor 172.22.2.115 in-aspathlist InboundASpath
-> ip bgp neighbor 172.22.2.115 in-aspathlist none
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp policy aspath-list	Creates or removes an AS path list.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAspathListIn
```

ip bgp neighbor in-communitylist

Assigns an inbound community list filter to a BGP peer.

ip bgp neighbor *ip_address* **in-communitylist {***string* | **none}**

Syntax Definitions

ip_address	32-bit IP address of the BGP peer.
string	Input community list (0 to 70 characters. This name is case sensitive.
none	Removes this community list from the peer.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- The community filter list name (**InboundCommlist** in the example below) is created using the **ip bgp policy community-list** command. Any inbound routes from the BGP peer must match this community filter before being accepted or passed to inbound policy.
- To deassign an input community filter list, use this command to assign a value of “none.”

Example

```
-> ip bgp neighbor 172.22.2.115 in-communitylist InboundCommlist
-> ip bgp neighbor 172.22.2.115 in-communitylist none
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp policy community-list	Creates or deletes a community list.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerCommunityListIn
```

ip bgp neighbor in-prefixlist

Assigns an inbound prefix filter list to a BGP peer.

ip bgp neighbor *ip_address* **in-prefixlist {***string* | **none}**

Syntax Definitions

ip_address	32-bit IP address.
string	Input prefix filter list (0 to 70 characters). This name is case sensitive.
none	Removes the prefix list from the peer.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- The prefix list name (**InboundPrefix** in the example below) is created using the **ip bgp policy prefix-list** command. Any inbound routes from the BGP peer must match this prefix filter before being accepted or passed to inbound policy.
- To deassign an input prefix filter list, use this command to assign a value of “none.”

Example

```
-> ip bgp neighbor 172.22.2.115 in-prefixlist InboundPrefix
-> ip bgp neighbor 172.22.2.115 in-prefixlist none
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp policy prefix-list	Creates or deletes a prefix match list.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerPrefixListIn
```

ip bgp neighbor out-aspathlist

Assigns an outbound AS path filter list to a BGP peer.

ip bgp neighbor *ip_address* **out-aspathlist {***string* | **none}**

Syntax Definitions

ip_address	32-bit IP address of the BGP peer.
string	Outbound AS path list (0 - 70 characters).
none	Removes the AS path list from the peer.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- The AS path list name (**OutboundASpath** in the example below) is created using the **ip bgp policy aspath-list** command. Any outbound routes from the BGP peer must match this AS path filter, or policy, before being advertised or passed to outbound policy.
- To deassign an output AS path filter list, use this command to assign a value of “none”.

Example

```
-> ip bgp neighbor 172.22.2.115 out-aspathlist OutboundASpath
-> ip bgp neighbor 172.22.2.115 out-aspathlist none
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp policy aspath-list	Creates or removes an AS path list.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAspathListOut
```

ip bgp neighbor out-communitylist

Assigns an outbound community filter list to a BGP peer.

ip bgp neighbor *ip_address* **out-communitylist {***string* **| none}**

Syntax Definitions

ip_address	32-bit IP address of the BGP peer.
string	Outbound community list (0 - 70 characters).
none	Removes the community list from the peer.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- The community filter list name (**OutboundCommlist** in the example below) is created using the **ip bgp policy community-list** command. Any outbound routes from the BGP peer must match this community filter before being advertised or passed to outbound policy.
- To deassign an output community filter list, use this command to assign a value of “none”.

Example

```
-> ip bgp neighbor 172.22.2.115 out-communitylist OutboundCommlist
-> ip bgp neighbor 172.22.2.115 out-communitylist none
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp policy community-list	Creates or deletes a community list.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerCommunityListOut
```

ip bgp neighbor out-prefixlist

Assigns an outbound prefix filter list to a BGP peer.

ip bgp neighbor *ip_address* **out-prefixlist {***string* | **none}**

Syntax Definitions

ip_address	32-bit IP address of the BGP peer.
string	Output prefix filter list (0 - 70 characters).
none	Removes the prefix list from the peer.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- The prefix list name (**OutboundPrefix** in the example below) is created using the **ip bgp policy prefix-list** command. Any outbound routes from the BGP peer must match this prefix filter before being advertised or passed to outbound policy.
- To deassign an output prefix filter list, use this command to assign a value of “none”.

Example

```
-> ip bgp neighbor 172.22.2.115 out-prefixlist OutboundPrefix
-> ip bgp neighbor 172.22.2.115 out-prefixlist none
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp policy prefix-list	Creates or deletes a prefix match list.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerPrefixListOut
```

ip bgp neighbor route-map

Assigns an inbound policy map to a BGP peer.

ip bgp neighbor *ip_address* **route-map {***string* **| none} {in | out}**

no ip bgp neighbor *ip_address* **route-map {in | out}**

Syntax Definitions

ip_address	32-bit IP address of the peer.
string	Inbound policy map name (0 to 70 characters). This name is case sensitive.
none	Deletes the route map if entered rather than a text string.
in	Designates this route map policy as an inbound policy.
out	Designates this route map policy as an outbound policy.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- The policy route map name (**peeringPointAMap** in the example below) is created using the **ip bgp policy route-map** command. Any inbound routes from the BGP peer must match this route map filter before being accepted or passed to inbound policy.
- To deassign an inbound map, use this command's **no** variant.
- It is also possible to deassign a route map by entering **none** in place of a route map name.

Example

```
-> ip bgp neighbor 172.22.2.115 route-map InboundRoute in
-> ip bgp neighbor 172.22.2.115 route-map OutboundRoute out
-> ip bgp neighbor 172.22.2.115 route-map none in
-> no ip bgp neighbor 172.22.2.115 route-map in
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp policy route-map	Creates or deletes a policy route map.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerRouteMapOut
   alaBgpPeerRouteMapIn
```

ip bgp neighbor clear soft

Invokes an inbound or outbound policy reconfiguration for a BGP peer.

ip bgp neighbor *ip_address* **clear soft {in | out}**

Syntax Definitions

ip_address	32-bit IP address for the BGP peer.
in	Applies reconfiguration to the inbound policies.
out	Applies reconfiguration to the outbound policies.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- This command reconfigures (or reapplies) all inbound or outbound policies to existing routes without restarting the peer session.
- This command is useful if policies have been changed.

Example

```
-> ip bgp neighbor 172.22.2.115 clear soft in
-> ip bgp neighbor 172.22.2.115 clear soft out
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp neighbor soft-reconfiguration	Enables or disables BGP peer soft reconfiguration.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerReconfigureInBound
   alaBgpPeerReconfigureOutBound
```

ip bgp policy aspath-list

Creates or removes an AS path list.

ip bgp policy aspath-list *name* **"***regular_expression***"**

no ip bgp policy aspath-list *name* **"***regular_expression***"**

Syntax Definitions

name	AS path name, e.g., InboundAspath, ranging from 0 to 70 characters, or a value of none. The AS path name is case sensitive.
regular_expression	Regular expression, e.g., "^100 200$" where 100 (followed by a space) represents the beginning of the list and 200 represents the end. The regular expression must be enclosed by quotation marks.

Defaults

No IP BGP peer policy AS path-list exists.

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- To create an AS path list, use the **ip bgp policy aspath-list** command.
- To remove an AS path list, use the **no** form of the command.
- A regular expression consists of a character string presented in the form of a pattern, e.g., ^100 200$. Valid regular expression characters (metacharacters) are shown in the table below. See also "Configuring BGP" in your Advanced Routing Guide for more information on using regular expressions in BGP commands.

Symbol	Description
^	Matches the beginning of the AS path list.
123	Matches the AS number 123.
.	Matches any single AS number.
?	Matches zero or one occurrence of the previous token, which must be an AS number, a dot, an alternation or a range.
+	Matches one or more occurrences of the previous token, which must be an AS number, a dot, an alternation or a range.
*	Matches zero or more occurrences of the previous token, which must be an AS number, a dot, an alternation or a range.
(	Begins an alternation sequence of AS numbers. It matches any AS number listed in the alternation sequence.

Symbol	Description
|	Separates AS numbers in an alternation sequence.
)	Ends an alternation sequence of AS numbers
[	Begins a range pair consisting of two AS numbers separated by a dash. It matches any AS number within that inclusive range.
-	Separates the endpoints of a range.
]	Ends a range pair.
$	Matches the end of the AS path list.
,_	Commas, underscores and spaces are ignored.

- When using a regular expression in the CLI, the regular expression must be enclosed in quotation marks.
- This command creates AS path lists that can be applied to a peer's inbound and outbound routes using the **ip bgp neighbor in-aspathlist** and **ip bgp neighbor out-aspathlist** commands. The AS path list filters routes based on one or more regular expressions, as shown in the example below. If the route matches the AS path list filter, then the *permit* or *deny* action (i.e., policy) associated with the regular expression applies.
- If a BGP AS path list is configured to deny routes from a particular string of regular expression then by default all of the routes coming from any AS would be denied. You must configure the policy instance in the same policy to allow other routes to come in to be permitted from other ASs.
- General or more specific AS path list information can be displayed by varying the use of the **show ip bgp** command.

Examples

```
-> ip bgp policy aspath-list InboundAspath "^100 200$"
-> ip bgp policy aspath-list OutboundAspath "^300 400$"
-> no ip bgp policy aspath-list InboundAspath "^100 200$"
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp neighbor in-aspathlist	Assigns an inbound AS path list filter to a BGP peer.
ip bgp neighbor out-aspathlist	Assigns an outbound AS path list filter to a BGP peer.
ip bgp policy aspath-list action	Configures a policy action (either permit or deny a route from passing) to be taken for an AS path list when a match is found.
ip bgp policy aspath-list priority	Configures priority for processing regular expressions in an AS path list.

MIB Objects

```
alaBgpAspathMatchListTable
   alaBgpAspathMatchListRowStatus
```

ip bgp policy aspath-list action

Configures a policy action (either permit or deny a route from passing) to be taken for an AS path list when a match is found. Matching criteria are specified in the regular expression.

ip bgp policy aspath-list *name* **"***regular_expression***" action {permit | deny}**

Syntax Definitions

name	AS path name, e.g., InboundAspath, ranging from 0 to 70 characters, or a value of none. The AS path name is case sensitive.
regular_expression	Regular expression, e.g., "^100 200$" where 100 (followed by a space) represents the beginning of the list and 200 represents the end. The regular expression must be enclosed by quotation marks.
permit	Allows matching routes to pass.
deny	Stops matching routes from passing.

Defaults

parameter	default
permit | deny	permit

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- A regular expression consists of a character string presented in the form of a pattern, e.g., ^100 200$. Refer to **ip bgp policy aspath-list** on page 31-95 for a table of valid regular expression characters (metacharacters). See also "Configuring BGP" in your Advanced Routing Guide for more information on using regular expressions in BGP commands.
- This command allows or stops AS path lists from being applied to a peer's inbound and outbound routes configured via the **ip bgp neighbor in-aspathlist** and **ip bgp neighbor out-aspathlist** commands. The AS path list filters routes based on one or more regular expressions, as shown in the example below. If the route matches the AS path list filter, then the *permit* or *deny* action (i.e., policy) associated with the regular expression applies.
- General or more specific AS path list information can be displayed by varying the use of the **show ip bgp** command.

Example

```
-> ip bgp policy aspath-list InboundAspath "^100 200$" action permit
-> ip bgp policy aspath-list OutboundAspath "^300 400$" action deny
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp neighbor in-aspathlist	Assigns an inbound AS path list filter to a BGP peer.
ip bgp neighbor out-aspathlist	Assigns an outbound AS path list filter to a BGP peer.
ip bgp policy aspath-list	Creates or removes an AS path list.
ip bgp policy aspath-list priority	Configures priority for processing regular expressions in an AS path list.

MIB Objects

```
alaBgpAspathMatchListTable
   alaBgpAspathMatchListAction
```

ip bgp policy aspath-list priority

Configures the priority for processing regular expressions in an AS path list.

ip bgp policy aspath-list *name* **"***regular_expression***" priority** *value*

Syntax Definitions

name	The AS path name, e.g., InboundAspath, ranging from 0 to 70 characters, or a value of none. The AS path name is case sensitive.
regular_expression	A regular expression, e.g., "^100 200$" where 100 (followed by a space) represents the beginning of the list and 200 represents the end. The regular expression must be enclosed by quotation marks.
value	A priority value, e.g., 1, assigned to the policy action. Valid priority range is from 1 - 255.

Defaults

parameter	default
value	1

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- A regular expression consists of a character string presented in the form of a pattern, e.g., ^100 200$. Refer to **ip bgp policy aspath-list** on page 31-95 for a table of valid regular expression characters (metacharacters). See also "Configuring BGP" in your Advanced Routing Guide for more information on using regular expressions in BGP commands.
- This command specifies the priority of an AS path list filter being applied to a peer's inbound and outbound routes configured via the **ip bgp neighbor in-aspathlist** and **ip bgp neighbor out-aspath-list** commands. The AS path list filters routes based on one or more regular expressions, as shown in the example below. If the route matches the AS path list filter, then the *permit* or *deny* action (i.e., policy) associated with the regular expression applies, but only in the order designated by the priority value.
- The higher the priority value specified in the command, the later the matching is processed. For example, regular expressions with a priority of 1 (the default) are processed before an expression assigned a priority of 3. When regular expressions have an equal priority, the processing order is indeterminate.
- General or more specific AS path list information can be displayed by varying the use of the **show ip bgp** command.

Example

```
-> ip bgp policy aspath-list InboundAspath "^100 200$" priority 1
-> ip bgp policy aspath-list OutboundAspath "^300 400$" priority 5
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp neighbor in-aspathlist	Assigns an inbound AS path list filter to a BGP peer.
ip bgp neighbor out-aspathlist	Assigns an outbound AS path list filter to a BGP peer.
ip bgp policy aspath-list	Creates or removes an AS path list.
ip bgp policy aspath-list action	Configures a policy action (either permit or deny a route from passing) to be taken for an AS path list when a match is found.

MIB Objects

```
alaBgpAspathMatchListTable
   alaBgpAspathMatchListPriority
```

ip bgp policy community-list

Creates or deletes a community list.

ip bgp policy community-list *name* **{none | no-export | no-advertise | no-export-subconfed |** *num:num***}**

no ip bgp policy community-list *name* **{none | no-export | no-advertise | no-export-subconfed |** *num:num***}**

Syntax Definitions

name	Community name, e.g., CommListAIn, ranging from 0 to 70 characters, or a value of none. The Community name is case sensitive.
none	Removes the community restrictions on the community section of the route map.
no-export	Routes in this community are advertised within the AS but not beyond the local AS.
no-advertise	Routes in this community are not advertised to any peer.
no-export-subconfed	Routes in this community are not advertised to any external BGP peer.
num:num	The community number, given in the form of the AS number and the community number, separated by a colon, as defined in RFC 1997.

Defaults

No IP BGP peer policy community-list exists.

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- To remove a community-list, use the **no** form of the command.
- This command creates community lists that can be applied to a peer's inbound and outbound routes using the **ip bgp neighbor in-communitylist** and **ip bgp neighbor out-communitylist** commands. The community list filters routes based on one or more community match list strings, as shown in the example below. If the route matches the community list filter, according to the matching type *exact* or *occur*, then the *permit* or *deny* policy action associated with the match list string applies.
- General or more specific community list information can be displayed by varying the use of the **show ip bgp** command.

Example

```
-> ip bgp policy community-list CommListAIn 40:40
-> ip bgp policy community-list CommListAOut 400:20
-> ip bgp policy community-list none
-> no ip bgp policy community-list CommListAIn 400:20
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp neighbor in-communitylist	Assigns an inbound AS community list filter to a BGP peer.
ip bgp neighbor out-communitylist	Assigns an outbound AS community list filter to a BGP peer.
ip bgp policy community-list action	Configures a policy action (either permit or deny a route from passing) to be taken for an AS community list filter when a match is found.
ip bgp policy community-list match-type	Configures type of matching to be performed with a community string list.
ip bgp policy community-list priority	Configures priority for processing multiple items in a community list filter.

MIB Objects

```
alaBgpCommunityMatchListTable
   alaBgpCommunityMatchListRowStatus
```

ip bgp policy community-list action

Configures the action to be taken for a community list when a match is found.

ip bgp policy community-list *name* **{none | no-export | no-advertise | no-export-subconfed |** *num:num***} action {permit | deny}**

Syntax Definitions

name	Community name, e.g., CommListAIn, ranging from 0 to 70 characters, or a value of none. The Community name is case sensitive.
none	Removes the community restrictions on the community section of the route map.
no-export	Routes in this community are advertised within the AS but not beyond the local AS.
no-advertise	Routes in this community are not advertised to any peer.
no-export-subconfed	Routes in this community are not advertised to any external BGP peer.
num:num	The community number, given in the form of the AS number and the community number, separated by a colon, as defined in RFC 1997.
permit	Allows matching routes to pass.
deny	Stops matching routes from passing.

Defaults

parameter	default
permit | deny	permit

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

By default, this command allows routes that match the criteria specified in the community list to pass.

Example

```
-> ip bgp policy community-list commListAIn 600:1 action permit
-> ip bgp policy community-list commListAIn 600:1 action deny
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp neighbor in-communitylist	Assigns an inbound AS community list filter to a BGP peer.
ip bgp neighbor out-communitylist	Assigns an outbound AS community list filter to a BGP peer.
ip bgp policy community-list match-type	Configures type of matching to be performed with a community string list.
ip bgp policy community-list priority	Configures priority for processing multiple items in a community list filter.

MIB Objects

```
alaBgpCommunityMatchListTable
   alaBgpCommunityMatchListAction
```

ip bgp policy community-list match-type

Configures the type of matching to be performed with a community string list.

ip bgp policy community-list *name* **{none | no-export | no-advertise | no-export-subconfed |** *num:num***} match-type {exact | occur}**

Syntax Definitions

name	Community name, e.g., CommListAIn, ranging from 0 to 70 characters, or a value of none. The Community name is case sensitive.
none	Removes the community restrictions on the community section of the route map.
no-export	Routes in this community are advertised within the AS but not beyond the local AS.
no-advertise	Routes in this community are not advertised to any peer.
no-export-subconfed	Routes in this community are not advertised to any external BGP peer.
num:num	The community number, given in the form of the AS number and the community number, separated by a colon, as defined in RFC 1997.
exact	Checks for an exact match of the community string and the community attribute.
occur	Checks for an occurrence of the community string anywhere in the community attribute.

Defaults

parameter	default
exact | occur	exact

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

By default, this command only allows routes to pass if the community string exactly matches the community attribute of the route.

Example

```
-> ip bgp policy community-list commListC 600:1 match-type exact
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp neighbor in-communitylist	Assigns an inbound AS community list filter to a BGP peer.
ip bgp neighbor out-communitylist	Assigns an outbound AS community list filter to a BGP peer.
ip bgp policy community-list action	Configures a policy action (either permit or deny a route from passing) to be taken for an AS community list filter when a match is found.
ip bgp policy community-list priority	Configures priority for processing multiple items in a community list filter.

MIB Objects

```
alaBgpCommunityMatchListTable
   alaBgpCommunityMatchListType
```

ip bgp policy community-list priority

Configures the priority for processing multiple items in a community list filter.

ip bgp policy community-list *name* **{none | no-export | no-advertise | no-export-subconfed |** *num:num***} priority** *value*

Syntax Definitions

name	Community name, e.g., CommListAIn, ranging from 0 to 70 characters, or a value of none. The Community name is case sensitive.
none	Removes the community restrictions on the community section of the route map.
no-export	Routes in this community are advertised within the AS but not beyond the local AS.
no-advertise	Routes in this community are not advertised to any peer.
no-export-subconfed	Routes in this community are not advertised to any external BGP peer.
num:num	The community number, given in the form of the AS number and the community number, separated by a colon, as defined in RFC 1997.
value	Priority value in the range 0 - 255.

Defaults

parameter	default
value	1

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

The higher the priority value specified in the command, the later the matching is processed. For example, items with a priority of 1 (the default) are processed before items assigned a priority of 3. When items have an equal priority, the processing order is indeterminate.

Example

```
-> ip bgp policy community-list commListB 500:1 priority 3
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp policy community-list	Creates or deletes a community list.
ip bgp policy community-list action	Configures a policy action (either permit or deny a route from passing) to be taken for an AS community list filter when a match is found.
ip bgp policy community-list match-type	Configures type of matching to be performed with community string list.

MIB Objects

```
alaBgpCommunityMatchListTable
   alaBgpCommunityMatchListPriority
```

ip bgp policy prefix-list

Creates or deletes a prefix match list.

ip bgp policy prefix-list *name ip_address ip_mask*

no ip bgp policy prefix-list *name ip_address ip_mask*

Syntax Definitions

name	Prefix list name.
ip_address	IP address for the prefix list.
ip_mask	Mask for the prefix list.

Defaults

No IP BGP policy prefix-list exists.

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- This command creates prefix lists that can be applied to a peer's inbound and outbound routes using the **ip bgp neighbor in-prefixlist** and **ip bgp neighbor out-prefixlist** commands. The prefix list filters routes based on one or more prefixes, as shown in the example below. If the route matches the prefix list filter, according to the **ge** (lower) and **le** (upper) limits defined, then the **permit** or **deny** action associated with the prefix applies.
- General or more specific prefix list information can be displayed by varying the use of the **show ip bgp** command.

Example

```
-> ip bgp policy prefix-list prefixListA 12.0.0.0 255.0.0.0
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp policy prefix-list action	Configures action to be taken for a prefix list when a match is found.
ip bgp policy prefix-list ge	Configures lower limit on length of prefix to be matched.
ip bgp policy prefix-list le	Configures upper limit on length of prefix to be matched.

MIB Objects

```
alaBgpPrefixMatchListTable
   alaBgpPrefixMatchListRowStatus
```

ip bgp policy prefix-list action

Configures the action to be taken for a prefix list when a match is found.

ip bgp policy prefix-list *name ip_address ip_mask* **action {permit | deny}**

Syntax Definitions

name	Prefix list name.
ip_address	IP address of the prefix list.
ip_mask	Mask for the prefix list.
permit	Allows matching routes to pass.
deny	Stops matching routes from passing.

Defaults

parameter	default
permit | deny	permit

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

Configures the action to be taken for a prefix list when a match is found.

Example

```
-> ip bgp policy prefix-list prefixListA 12.0.0.0 255.0.0.0 action deny
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp policy prefix-list	Creates or deletes a prefix match list.
ip bgp policy prefix-list ge	Configures lower limit on length of prefix to be matched.
ip bgp policy prefix-list le	Configures upper limit on length of prefix to be matched.

MIB Objects

```
alaBgpPrefixMatchListTable
   alaBgpPrefixMatchListAction
```

ip bgp policy prefix-list ge

Configures the lower limit on the length of the prefix to be matched.

ip bgp policy prefix-list *name ip_address ip_mask* **ge** *value*

Syntax Definitions

name	Prefix list name.
ip_address	IP address of the prefix list.
ip_mask	Mask of the prefix list.
value	The lower limit value in the range 0 to 32.

Defaults

parameter	default
value	0

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- The default value of zero indicates there is no lower limit on the length of the prefix to be matched.
- This command is used in conjunction with the **ip bgp policy prefix-list le** command to set the prefix matching range. The two commands can be combined, as show in the Example section below.
- The **ge** (lower limit) value must be greater than or equal to the prefix length (8 in the example below) and less than or equal to the **le** (upper limit) value.

Example

```
-> ip bgp policy prefix-list prefixListA 14.0.0.0 255.0.0.0 ge 8 le 16
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp policy prefix-list	Creates or deletes a prefix match list.
ip bgp policy prefix-list action	Configures action to be taken for a prefix list when a match is found.
ip bgp policy prefix-list le	Configures upper limit on length of prefix to be matched.

MIB Objects

```
alaBgpPrefixMatchListTable
   alaBgpPrefixMatchListGE
```

ip bgp policy prefix-list le

Configures the upper limit on the length of the prefix to be matched.

ip bgp policy prefix-list *name ip_address ip_mask* **le** *value*

Syntax Definitions

name	Prefix list name.
ip_address	Prefix list IP address for the prefix list.
ip_mask	Prefix list mask for the prefix list.
value	The upper limit value in the range of 0 to 32.

Defaults

parameter	default
value	0

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- The default value of zero indicates there is no upper limit on the length of the prefix to be matched. This command is used in conjunction with **ip bgp policy prefix-list ge** to set the prefix matching range. The two commands can be combined, as show in the Example section below.
- The **ge** (lower limit) value must be greater than or equal to the prefix length (8 in the example below) and less than or equal to the **le** (upper limit) value.

Example

```
-> ip bgp policy prefix-list prefixListA 14.0.0.0 255.0.0.0 ge 8 le 16
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp policy prefix-list	Creates or deletes a prefix match list.
ip bgp policy prefix-list action	Configures action to be taken for a prefix list when a match is found.
ip bgp policy prefix-list ge	Configures lower limit on length of prefix to be matched.

MIB Objects

```
alaBgpPrefixMatchListTable
   alaBgpPrefixMatchListLE
```

ip bgp policy route-map

Creates or deletes a policy route map.

ip bgp policy route-map *name sequence_number*

Syntax Definitions

name	Route map name. Case-sensitive.
sequence_number	Route map sequence number in the range of 1 to 255. The sequence number allows for multiple instances of the same route map name.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- This command creates policy route maps. Each route map can be configured using the following match commands to specify the match criteria by which routes are allowed to pass. Match criteria is examined in the order the commands are listed below.

  1. **ip bgp policy route-map aspath-list**
  2. **ip bgp policy route-map prefix-list**
  3. **ip bgp policy route-map community-list**
  4. **ip bgp policy route-map match-regexp**
  5. **ip bgp policy route-map match-prefix**
  6. **ip bgp policy route-map match-mask**
  7. **ip bgp policy route-map match-community**

- Each route map can also be configured using the following set commands to sequentially specify the actions to be taken when a match is found.
  - **ip bgp policy route-map community**
  - **ip bgp policy route-map community-mode**
  - **ip bgp policy route-map lpref**
  - **ip bgp policy route-map lpref-mode**
  - **ip bgp policy route-map med**
  - **ip bgp policy route-map med-mode**
  - **ip bgp policy route-map origin**

- **ip bgp policy route-map weight**

- Route maps can be referenced as a filtering mechanism for displaying paths using the **show ip bgp path** command. They are also referenced in filtering inbound and outbound routes for BGP peers using the **ip bgp neighbor route-map** commands.

Example

```
-> ip bgp policy route-map routemap1 1
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp policy route-map action Configures action to be taken for a route when a match is found.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapRowStatus
```

ip bgp policy route-map action

Configures the action to be taken for a route when a match is found.

ip bgp policy route-map *name sequence_number* **action {permit | deny}**

Syntax Definitions

name	A route map name.
sequence_number	A route map sequence number. The valid range is 1–255.
permit	Allows matching routes to pass.
deny	Stops matching routes from passing. In addition, no further instances (sequence numbers) of the route map are examined.

Defaultst

parameter	default
permit | deny	*permit*

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

By default, this command allows routes that match the criteria specified in the route map to pass. If no matching routes are found, any additional instances (sequence numbers) of the route map name are examined. When all instances have been examined with no match, the route is dropped.

Example

```
-> ip bgp policy route-map routemap1 1 action deny
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp policy route-map	Creates or deletes a policy route map.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapAction
```

ip bgp policy route-map aspath-list

Assigns an AS path matching list to the route map.

ip bgp policy route-map *name sequence_number* **aspath-list** *as_name*

Syntax Definitions

name	The route map name.
sequence_number	The route map sequence number. The valid range is 1–255.
as_name	The AS path list name or “none”.

Defaults

parameter	default
as_name	none

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- By default, no AS path list is assigned to a route map.
- This default behavior can be reset by changing the value of the AS path list name to “none”.
- The **ip bgp policy aspath-list** and **ip bgp policy aspath-list action** commands are used to create and set permit/deny actions for an AS path list.

Example

```
-> ip bgp policy route-map routemap1 1 aspath-list aspathlist1
-> ip bgp policy route-map routemap1 1 aspath-list none
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp policy route-map	Creates or deletes a policy route map.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapAsPathMatchListId
```

ip bgp policy route-map asprepend

Configures the AS path prepend action to be taken when a match is found.

ip bgp policy route-map *name sequence_number* **asprepend** *path*

Syntax Definitions

name	The route map name.
sequence_number	The route map sequence number. The valid range is 1–255.
path	The AS path to prepend or “none”.

Defaults

parameter	default
path	none

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

By default, no AS path is prepended. This command allows AS path numbers to be prepended (added to the beginning of the AS path list) to the AS path attribute of a matching route. The default behavior can be reset by changing the value to “none”.

Example

```
-> ip bgp policy route-map routemap1 1 asprepend 700 700 700
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp policy route-map	Creates or deletes a policy route map.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapAsPrepend
```

ip bgp policy route-map community

Configures the action to be taken on the community attribute when a match is found.

ip bgp policy route-map *name sequence_number* **community [none | no-export | no-advertise | no-export-subconfed |** *num***:***num***]**

Syntax Definitions

name	The route map name.
sequence_number	The route map sequence number. The valid range is 1–255.
none	Removes the community restrictions on the community section of the route map.
no-export	Routes in this community are advertised within the AS but not beyond the local AS.
no-advertise	Routes in this community are not advertised to any peer.
no-export-subconfed	Routes in this community are not advertised to any external BGP peer.
num:num	The community number, given in the form of the AS number and the community number, separated by a colon, as defined in RFC 1997.

Defaults

parameter	default
string	none

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- By default, no action is taken on a community attribute when a match on a route is found.
- The default behavior can be reset by setting the value to “none”.
- The **ip bgp policy community-list** and **ip bgp policy community-list action** commands are used to create and set permit/deny actions for a community path list. This command is used in conjunction with **ip bgp policy route-map community-mode**.

Example

```
-> ip bgp policy route-map routemap1 1 community 400:1 500:1
-> ip bgp policy route-map routemap1 1 community 400:1 500:1 community-mode replace
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp policy route-map	Creates or deletes a policy route map.
ip bgp policy route-map community-mode	Configures the action to be taken for a community string when a match is found.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapCommunity
```

ip bgp policy route-map community-list

Assigns a community matching list to the route map.

ip bgp policy route-map *name sequence_number* **community-list** *name*

Syntax Definitions

name	The route map name.
sequence_number	The route map sequence number. The valid range is 1–255.
name	The community list name, or “none”.

Defaults

parameter	default
name	none

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

By default, no community list is assigned to the route map. The default behavior can be reset by changing the value to “none”.

Example

```
-> ip bgp policy route-map routemap1 1 community-list listB
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp policy route-map	Creates or deletes a policy route map.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapCommunityMatchListId
```

ip bgp policy route-map community-mode

Configures the action to be taken for a community string when a match is found.

ip bgp policy route-map *name sequence_number* **community-mode {add | replace}**

Syntax Definitions

name	The route map name.
sequence_number	The route map sequence number. The valid range is 1–255.
add	Adds the community string specified in the command **ip bgp policy route-map community**.
replace	Replaces the community string specified in the command **ip bgp policy route-map community**.

Defaults

parameter	default
add | replace	add

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

This command is used in conjunction with **ip bgp policy route-map community**. The example on the next line shows the combined usage.

Example

```
-> ip bgp policy route-map routemap1 1 community-mode replace
-> ip bgp policy route-map routemap1 1 community 400:1 500:1 community-mode replace
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp policy route-map	Creates or deletes a policy route map.
ip bgp policy route-map community	Configures the action to be taken on the community attribute when a match is found.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapSetComunityMode
```

ip bgp policy route-map lpref

Configures the local preference value for the route map.

ip bgp policy route-map *name sequence_number* **lpref** *value*

Syntax Definitions

name	The route map name.
sequence_number	The route map sequence number. The valid range is 1–255.
value	The local preference value. The valid range is 0–4294967295

Defaults

parameter	default
value	0

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- This command is used in conjunction with **ip bgp policy route-map lpref-mode**. The example on the next line shows the combined usage.
- In this example, the local preference value will be incremented for a matching route by 555.

Example

```
-> ip bgp policy route-map routemap1 1 lpref 555
-> ip bgp policy route-map routemap1 1 lpref 555 lpref-mode inc
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp policy route-map	Creates or deletes a policy route map.
ip bgp policy route-map lpref-mode	Configures the action to be taken when setting local preference attribute for a local matching route.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapLocalPref
```

ip bgp policy route-map lpref-mode

Configures the action to be taken when setting local preference attribute for a local matching route.

ip bgp policy route-map *name sequence_number* **lpref-mode {none | inc | dec | rep}**

Syntax Definitions

name	The route map name.
sequence_number	The route map sequence number. The valid range is 1–255.
none	Do not set the local preference attribute.
inc	Increment the local preference attribute in the matching route by the value specified in the **ip bgp policy route-map med** command. No action is taken if no local preference attribute is found in the matching route.
dec	Decrement the local preference attribute in the matching route by the value specified in the **ip bgp policy route-map med** command. No action is taken if no local preference attribute is found in the matching route.
rep	Replace the local preference attribute in the matching route by the value specified in the **ip bgp policy route-map med** command even if no local preference attribute is found in the matching route.

Defaults

parameter	default
none | inc | dec | rep	none

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- This command is used in conjunction with **ip bgp policy route-map lpref**. The example below shows the combined usage.
- In this example, the local preference value is incremented for a matching route by 555.

Example

```
-> ip bgp policy route-map routemap1 1 lpref-mode none
-> ip bgp policy route-map routemap1 1 lpref 555 lpref-mode inc
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp policy route-map	Creates or deletes a policy route map.
ip bgp policy route-map lpref	Configures the local preference value for the route map.
ip bgp policy route-map med	Configures the Multi-Exit Discriminator (MED) value for a route map.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapLocalPrefMode
```

ip bgp policy route-map match-community

Configures a matching community primitive for the route map.

ip bgp policy route-map *name sequence_number* **match-community [none | no-export | no-advertise | no-export-subconfed |** *num:num***]**

Syntax Definitions

name	The route map name.
sequence_number	The route map sequence number. The valid range is 1–255.
none	Removes the community match from the route-map.
no-export	Routes in this community are advertised within the AS but not beyond the local AS.
no-advertise	Routes matching the community restricting advertisement to any peer.
no-export-subconfed	Routes matching the community restricting advertisement to any external BGP peer.
num:num	The community number, given in the form of the AS number and the community number, separated by a colon, as defined in RFC 1997.

Defaults

parameter	default
community_string	none

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

This command allows a matching community string primitive to be placed directly in the route map. By default, no community string is specified. The default behavior can be reset by changing the value to “none”.

Example

```
-> ip bgp policy route-map routemap1 1 match-community 400:1 500 700:1
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp policy route-map	Creates or deletes a policy route map.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapMatchCommunity
```

ip bgp policy route-map match-mask

Configures a matching mask primitive in the route map.

ip bgp policy route-map *name sequence_number* **match-mask** *ip_address*

Syntax Definitions

name	The route map name.
sequence_number	The route map sequence number. The valid range is 1–255.
ip_address	The 32-bit IP address of the matching mask or “none”.

Defaults

parameter	default
ip_address	0.0.0.0

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- This command allows a matching mask primitive to be placed directly in the route map. By default, no mask primitive is specified. The default behavior can be reset by changing the value to “none”
- The example on the next line shows usage combined with the **ip bgp policy route-map match-prefix** command.

Example

```
-> ip bgp policy route-map routemap1 1 match-mask 255.255.0.0
-> ip bgp policy route-map routemap1 1 match-prefix 17.0.0.0 match-mask 255.255.0.0
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp policy route-map	Creates or deletes a policy route map.
ip bgp policy route-map match-prefix	Configures a matching prefix primitive in the route map.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapMatchMask
```

ip bgp policy route-map match-prefix

Configures a matching prefix primitive in the route map.

ip bgp policy route-map *name sequence_number* **match-prefix** *ip_address*

Syntax Definitions

name	The route map name.
sequence_number	The route map sequence number. The valid range is 1–255.
ip_address	The 32-bit IP address of the matching prefix.

Defaults

parameter	default
ip_address	0.0.0.0

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- This command allows a matching prefix primitive to be placed directly in the route map. By default, no prefix primitive is specified. The default behavior can be reset by changing the value to “none”.
- The example on the next line shows usage combined with the **ip bgp policy route-map match-mask** command.

Example

```
-> ip bgp policy route-map routemap1 1 match-prefix 17.0.0.0
-> ip bgp policy route-map routemap1 1 match-prefix 17.0.0.0 match-mask 255.255.0.0
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp policy route-map match-mask	Configures a matching prefix primitive in the route map.
ip bgp policy route-map	Configures an AS path matching regular expression primitive in the route map.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapMatchPrefix
```

ip bgp policy route-map match-regexp

Configures an AS path matching regular expression primitive in the route map.

ip bgp policy route-map *name sequence_number* **match-regexp "***regular_expression***"**

Syntax Definitions

name	The route map name.
sequence_number	The route map sequence number. The valid range is 1–255.
regular_expression	Regular expression or "none". The regular expression must be enclosed by quotation marks.

Defaults

parameter	default
regular_expression	none

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- This command allows a regular expression matching directive to be placed directly in the route map. By default, no matching regular expression is specified. Regular expressions are defined in **ip bgp policy aspath-list** on page 31-95.
- When using regular expressions in the CLI, the regular expression must be enclosed by quotation marks.
- The default behavior can be reset by changing the value to "none".
- See the *OmniSwitch 7700/7800/8800 Advanced Routing Configuration Guide* for more information on the use of regular expressions in BGP commands.

Example

```
-> ip bgp policy route-map routemap1 1 match-regexp "500 .* 400$"
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp policy route-map	Configures an AS path matching regular expression primitive in the route map.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapMatchAsRegExp
```

ip bgp policy route-map med

Configures the Multi-Exit Discriminator (MED) value for a route map.

ip bgp policy route-map *name sequence_number* **med** *value*

Syntax Definitions

name	The route map name.
sequence_number	The route map sequence number. The valid range is 1–255.
value	The MED value. The valid range is 0–4294967295.

Defaults

parameter	default
value	0

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

This command is used in conjunction with **ip bgp policy route-map med-mode** command. The first example below shows the combined usage. In the second example, the MED value is incremented for a matching route by 5.

Example

```
-> ip bgp policy route-map routemap1 1 med 555
-> ip bgp policy route-map routemap1 1 med 555 med-mode inc
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp policy route-map med-mode	Configures Multi-Exit Discriminator (MED) value for a route map.
ip bgp policy route-map	Configures an AS path matching regular expression primitive in the route map.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapMed
```

ip bgp policy route-map med-mode

Configures the action to be taken when setting the Multi-Exit Discriminator (MED) attribute for a matching route.

ip bgp policy route-map *name sequence_number* **med-mode {none | inc | dec | rep}**

Syntax Definitions

name	The route map name.
sequence_number	The route map sequence number. The valid range is 1–255.
none	Do not set the MED.
inc	Increment the MED in the matching route by the value specified in the **ip bgp policy route-map med** command. No action is taken if no MED is found in the matching route.
dec	Decrement the MED in the matching route by the value specified in the **ip bgp policy route-map med** command. No action is taken if no MED is found in the matching route.
rep	Replace the MED in the matching route by the value specified in the **ip bgp policy route-map med** command even if no MED is found in the matching route.

Defaults

parameter	default
none | inc | dec | rep	none

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

This command is used in conjunction with **ip bgp policy route-map med**. The first example below shows the combined usage. In the second example, the MED value is incremented for a matching route by 5.

Example

```
-> ip bgp policy route-map routemap1 1 med-mode inc
-> ip bgp policy route-map routemap1 1 med 5 med-mode inc
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp policy route-map med	Configures action to take when setting Multi-Exit Discriminator (MED) attribute for a matching route.
ip bgp policy route-map	Configures an AS path matching regular expression primitive in the route map.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapMedMode
```

ip bgp policy route-map origin

Configures the action to be taken on the origin attribute when a match is found.

ip bgp policy route-map *name sequence_number* **origin {igp | egp| incomplete | none}**

Syntax Definitions

name	Route map name.
sequence_number	Route map sequence number. Valid range 1–255.
igp	Sets the origin attribute to remote internal BGP (IGP).
egp	Sets the origin attribute to local external BGP (EGP).
incomplete	Sets the origin attribute to incomplete, meaning the origin is unknown.
none	Sets the origin attribute to “none”.

Defaults

parameter	default
igp | egp| incomplete | none	none

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

By default, no action is taken on the origin attribute when a match is found. The default behavior can be reset by changing the value to “none”.

Example

```
-> ip bgp policy route-map routemap1 1 origin egp
```

Release History

Release 5.1; command was introduced.

Related Commands

iip bgp policy route-map origin	Configures action to take on origin attribute when a match is found.
ip bgp policy route-map	Configures an AS path matching regular expression primitive in the route map.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapOrgin
```

ip bgp policy route-map prefix-list

Assigns a prefix matching list to the route map.

ip bgp policy route-map *name sequence_number* **prefix-list** *prefix_name*

Syntax Definitions

name	The route map name.
sequence_number	The route map sequence number. The valid range is 1–255.
prefix_name	The prefix list name or “none”.

Defaults

parameter	default
prefix_name	none

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- By default, no prefix list is assigned to the route map. The default behavior can be reset by changing the value to “none”.
- The **ip bgp policy prefix-list**, **ip bgp policy prefix-list action**, **ip bgp policy prefix-list ge**, and **ip bgp policy prefix-list le** commands are used to create and set permit/deny actions for a prefix path list.

Example

```
-> ip bgp policy route-map routemap1 1 prefix-list listC
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp policy prefix-list	Assigns a prefix matching list to the route map.
ip bgp policy prefix-list action	Configures action to be taken for a prefix list when a match is found.
ip bgp policy route-map	Configures an AS path matching regular expression primitive in the route map.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapPrefixMatchListId
```

ip bgp policy route-map weight

Configures a BGP weight value to be assigned to inbound routes when a match is found.

ip bgp policy route-map *name sequence_number* **weight** *value*

Syntax Definitions

name	The route map name.
sequence_number	The route map sequence number. The valid range is 1–255.
value	The weight value. The valid range is 0–65535.

Defaults

parameter	default
value	0

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

This command sets the weight value for routes that pass the route map match criteria. It is only applicable for the inbound policy. The default value of zero means that the weight is not changed by the route map.

Example

```
-> ip bgp policy route-map routemap1 1 weight 500
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp policy route-map	Configures an AS path matching regular expression primitive in the route map.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapWeight
```

ip bgp policy route-map community-strip

Configures the value to strip from the community attribute of the routes matched by this route map instance (sequence number).

ip bgp policy route-map *name sequence_number* **community-strip** *community_list*

Syntax Definitions

name	The route map name.
sequence_number	The route map sequence number. The valid range is 1–255.
community_list	The community list name.

Defaults

No IP BGP policy route-map community list exists.

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

Configures the value to strip from the community attribute of the routes matched by this route map instance (sequence number).

Example

```
-> ip bgp policy route-map routemap1 1 commmunity_strip communitylist
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp policy route-map	Configures an AS path matching regular expression primitive in the route map.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapCommunityStrip
```

ip bgp redist-filter

Creates or deletes a local redistribution filter.

In lieu of these options, the base command (**ip bgp redist-filter**) may be used with other keywords to set up redistribution filter configuration. These keywords are listed here and described as separate commands later in this chapter. In addition, some keywords have a **no** form to remove the parameter or return it to its default.

ip bgp redist-filter {local | static | rip | ospf} *ip_address ip_mask*
[community *string***]**
[local-preference *value***]**
[metric *metric***]**
[effect {permit | deny}]
[subnets]
[status {enable | disable}]

no ip bgp redist-filter {local | static | rip | ospf} *ip_address ip_mask*

Syntax Definitions

local	Redistributes local routes.
static	Redistributes static routes.
rip	Redistributes routes using the RIP protocol.
ospf	Redistributes routes using the OSPF protocol.
ip_address	The destination IP address.
ip_mask	The destination mask.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

This command sets up a filter to redistribute routes from one routing domain to another routing domain by specifying a source protocol and a destination IP address. The operation of the redistribution filter can be controlled using the following commands:

- **ip bgp redist-filter effect**
- **ip bgp redist-filter subnets**

The redistribution filter can also be configured using the following commands to set certain values when a route is redistributed.

- **ip bgp redist-filter community**

- **ip bgp redist-filter local-preference**
- **ip bgp redist-filter metric**

Notice the use of the **show** command in the example below to display the distribution filters in a summary table or, by specifying the protocol and destination address, as a detailed list.

Example

```
-> ip bgp redist-filter local 172.22.2.115 255.255.255.0
-> no ip bgp redist-filter local 172.22.2.115 255.255.255.0
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp redist-filter community	Configures the community string attribute for the local redistribution filter.
ip bgp redist-filter effect	Specifies the local redistribution filter action for route importation.
ip bgp redist-filter local-preference	Configures the local preference value for the local redistribution filter.
ip bgp redist-filter metric	Configures the metric value for the local redistribution filter.
ip bgp redist-filter subnets	Enables or disables local subnet redistribution.

MIB Objects

```
alaBgpRedistRouteTable
   alaBgpRedistRouteRowStatus
```

ip bgp redist-filter community

Configures the community string attribute for the local redistribution filter.

ip bgp redist-filter {local | static | rip | ospf} *ip_address ip_mask* **community** *community_string*

Syntax Definitions

local	Redistributes local routes.
static	Redistributes static routes.
rip	Redistributes routes using the RIP protocol.
ospf	Redistributes routes using the OSPF protocol.
other	Redistributes routes using protocols other than RIP, OSPF, or BGP.
ip_address	Destination IP address.
ip_mask	Destination mask.
community_string	Community string or “none”.

Defaults

parameter	default
community_string	none

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

This command is used to set the community string attribute for routes generated by the redistribution filter. You can unset the community attribute by specifying the default value of “none”.

Example

```
-> ip bgp redist-filter local 172.22.2.115 255.255.255.0 community no-export
-> ip bgp redist-filter local 172.22.2.115 255.255.255.0 community none
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp redist-filter	Creates or deletes a local redistribution filter.
ip bgp redist-filter effect	Specifies the local redistribution filter action for route importation.
ip bgp redist-filter local-preference	Configures the local preference value for the local redistribution filter.
ip bgp redist-filter metric	Configures the metric value for the local redistribution filter.
ip bgp redist-filter subnets	Enables or disables local subnet redistribution.

MIB Objects

```
alaBgpRedistRouteTable
   alaBgpRedistRouteCommunity
```

ip bgp redist-filter effect

Specifies the local redistribution filter action for route importation.

ip bgp redist-filter {local | static | rip | ospf} *ip_address ip_mask* **effect {permit | deny}**

Syntax Definitions

local	Redistributes local routes.
static	Redistributes static routes.
rip	Redistributes routes using the RIP protocol.
ospf	Redistributes routes using the OSPF protocol.
other	Redistributes routes using protocols other than RIP, OSPF, or BGP.
ip_address	Destination IP address.
ip_mask	Destination mask.
permit	Permits the specified routes to be redistributed.
deny	Stops the specified routes from being redistributed.

Defaults

parameter	default
permit | deny	permit

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

By default, this command allows routes that match the criteria specified in the filter to be redistributed. By specifying **deny**, these same routes will be dropped.

Example

```
-> ip bgp redist-filter local 172.22.2.115 255.255.255.0 effect permit
-> ip bgp redist-filter local 172.22.2.115 255.255.255.0 effect deny
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp redist-filter	Creates or deletes a local redistribution filter.
ip bgp redist-filter community	Configures the community string attribute for the local redistribution filter.
ip bgp redist-filter local-preference	Configures the local preference value for the local redistribution filter.
ip bgp redist-filter metric	Configures the metric value for the local redistribution filter.
ip bgp redist-filter subnets	Enables or disables local subnet redistribution.

MIB Objects

```
alaBgpRedistRouteTable
   alaBgpRedistRouteEffect
```

ip bgp redist-filter local-preference

Configures the local preference value for the local redistribution filter.

ip bgp redist-filter {local | static | rip | ospf} *ip_address ip_mask* **local-preference** *value*

Syntax Definitions

local	Redistributes local routes.
static	Redistributes static routes.
rip	Redistributes routes using the RIP protocol.
ospf	Redistributes routes using the OSPF protocol.
ip_address	Destination IP address.
ip_mask	Destination mask.
value	The local preference attribute value. The valid range is 0–4294967295

Defaults

parameter	default
value	0

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- This command is used to set the local preference value for routes generated by the redistribution filter.
- You can unset the local preference value by specifying the default value of zero.

Example

```
-> ip bgp redist-filter local 172.22.2.115 255.255.255.0 local-preference 0
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp redist-filter	Creates or deletes a local redistribution filter.
ip bgp redist-filter community	Configures the community string attribute for the local redistribution filter.
ip bgp redist-filter effect	Specifies the local redistribution filter action for route importation.
ip bgp redist-filter metric	Configures the metric value for the local redistribution filter.
ip bgp redist-filter subnets	Enables or disables local subnet redistribution.

MIB Objects

```
alaBgpRedistRouteTable
   alaBgpRedistRouteLocalPref
```

ip bgp redist-filter metric

Configures the metric value for the local redistribution filter.

ip bgp redist-filter {local | static | rip | ospf} *ip_address ip_mask* **metric** *value*

Syntax Definitions

local	Redistributes local routes.
static	Redistributes static routes.
rip	Redistributes routes using the RIP protocol.
ospf	Redistributes routes using the OSPF protocol.
other	Redistributes routes using protocols other than RIP, OSPF, or BGP.
ip_address	Destination IP address.
ip_mask	Destination mask.
value	The metric value. The valid range is 0–2147483647

Defaults

parameter	default
value	0

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

This command sets the metric value for routes generated by the redistribution filter. You can unset the metric value by specifying the default value of zero.

Example

```
-> ip bgp redist-filter local 172.22.2.115 255.255.255.0 metric 0
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp redist-filter	Creates or deletes a local redistribution filter.
ip bgp redist-filter community	Configures the community string attribute for the local redistribution filter.
ip bgp redist-filter effect	Specifies the local redistribution filter action for route importation.
ip bgp redist-filter local-preference	Configures the local preference value for the local redistribution filter.
ip bgp redist-filter subnets	Enables or disables local subnet redistribution.

MIB Objects

```
alaBgpRedistRouteTable
   alaBgpRedistRouteMetric
```

ip bgp redist-filter subnets

Enables or disables local subnet redistribution.

ip bgp redist-filter {local | static | rip | ospf} *ip_address ip_mask* **subnets**

no ip bgp redist-filter {local | static | rip | ospf} *ip_address ip_mask* **subnets**

Syntax Definitions

local	Redistributes local routes.
static	Redistributes static routes.
rip	Redistributes routes using the RIP protocol.
ospf	Redistributes routes using the OSPF protocol.
bgp	Redistributes routes using the BGP protocol.
ip_address	Destination IP address.
ip_mask	Destination mask.

Defaults

This command is enabled by default.

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

Enabling this command allows the more specific subnets to be redistributed by the redistribution filter.

Example

```
-> ip bgp redist-filter local 172.22.2.115 255.255.255.0 subnets
```

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp redist-filter	Creates or deletes a local redistribution filter.
ip bgp redist-filter community	Configures the community string attribute for the local redistribution filter.
ip bgp redist-filter effect	Specifies the local redistribution filter action for route importation.
ip bgp redist-filter local-preference	Configures the local preference value for the local redistribution filter.
ip bgp redist-filter metric	Configures the metric value for the local redistribution filter.

MIB Objects

```
alaBgpRedistRouteTable
   alaBgpRedistRouteSubnetMatch
```

show ip bgp

Displays the current global settings for the local BGP speaker.

show ip bgp

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

Most of the parameters in this display can be altered through BGP global commands. See the output definitions below for references to the CLI commands used to configure individual parameters.

Example

```
-> show ip bgp
Admin Status                          = disabled,
Operational Status                    = down,
Autonomous system Number              = 1,
BGP Router Id                         = 128.0.1.4,
Confederation Id                      = 0,
IGP Synchronization Status            = disabled,
Minimum AS origin interval (seconds) = 15,
Default Local Preference              = 100,
Route Reflection                      = disabled,
Cluster Id                            = 0.0.0.0,
Missing MED Status                    = Best,
Aspath Comparison                     = enabled,
Always Compare MED                   = disabled,
Fast External Fall Over               = disabled,
Log Neighbor Changes                 = disabled,
Multi path                            = disabled,
```

output definitions

Admin Status	Indicates whether the BGP protocol has been enabled or disabled through the **ip bgp status** command.
Operational Status	Indicates if the local BGP speaker is actively participating in BGP messages, update, routing advertisements.
Autonomous system Number	The AS assigned to the local BGP speaker through the **ip bgp autonomous-system** command.
BGP Router Id	The IP address for the local BGP speaker.

output definitions (continued)

Confederation Id	Shows the confederation number assigned to the local BGP speaker. If the BGP speaker does not belong to a confederation, then this value will be zero (0). Confederation numbers are assigned through the **ip bgp confederation identifier** command.
IGP Synchronization Status	Indicates whether BGP is synchronizing its routing tables with those on non-BGP routers handling IGP traffic (such as a RIP or OSPF router). This value is configured through the **ip bgp synchronization** command.
Minimum AS origin interval	The frequency, in seconds, at which routes local to the autonomous system are advertised. This value is configured through the **ip bgp as-origin-interval** command.
Default Local Preference	The local preference that will be assigned to routes that do not already contain a local preference value. This default value is configured through the **ip bgp default local-preference** command.
Route Reflection	Indicates whether the local BGP speaker is acting as a route reflector for its AS. This value is configured through the **ip bgp client-to-client reflection** command.
Cluster Id	The IP address for cluster in route reflector configurations using multiple, redundant route reflectors. A value of 0.0.0.0 indicates that a cluster is not set up. This value is configured through the **ip bgp cluster-id** command.
Missing MED Status	Indicates the MED value that will be assigned to paths that do not contain MED values. Missing MED values will either be assigned to the worst possible value (2^{32}-1) or the best possible value (0). This value is set using the **ip bgp bestpath med missing-as-worst** command. By default, missing MED values are treated as **best**.
Aspath Comparison	Indicates whether the AS path will be in used in determining the best route. This value is configured through the **ip bgp bestpath as-path ignore** command.
Always Compare MED	Indicates whether multi-exit discriminator (MED) values are being compared only for internal peers or also for external peers. This value is configured through the **ip bgp always-compare-med** command.
Fast External Fail Over	Indicates whether Fast External Failover has been enabled or disabled. When enabled a BGP sessions will be reset immediately after a connection to a directly connected external peer goes down. This value is configured through the **ip bgp fast-external-failover** command.
Log Neighbor Changes	Indicates whether logging of peer state changes is enabled or disabled. This value is configured through the **ip bgp log-neighbor-changes** command.
Multi path	Indicates whether support for multiple equal cost paths is enabled or disabled. This value is configured through the **ip bgp maximum-paths** command.

Release History

Release 5.1; command was introduced.

Related Commands

show ip bgp statistics	Displays BGP global statistics.

MIB Objects

```
alabgpMIBGlobalsGroup
   alaBgpProtoStatus
   alaBgpAutonomousSystemNumber
   alaBgpIgpSynchStatus
   alaBgpProtoOperState
   alaBgpNumActiveRoutes
   alaBgpNumEstabExternalPeers
   alaBgpNumEstabInternalPeers
   alaBgpClusterId
   alaBgpDefaultLocalPref
   alaBgpFastExternalFailOver
   alaBgpMedAlways
   alaBgpMissingMed
   alaBgpRouterId
   alaBgpRouteReflection
   alaBgpAsOriginInterval
   alaNumIgpSyncWaitPaths
   alaBgpManualTag
   alaBgpPromiscuousneighbors
   alaBgpConfedId
   alaBgpMultiPath
   alaBgpMaxPeers
   alaBgpPeersChanges
```

show ip bgp statistics

Displays BGP global statistics.

show ip bgp statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

This command show various BGP statistics for the switch, such as number of neighbors, active prefixes, number of paths, etc.

Example

```
-> show ip bgp statistics
# of Active Prefixes Known                = 0,
# of EBGP Neighbors in Established State  = 0,
# of IBGP Neighbors in Established State  = 0,
# of Feasible Paths                       = 0,
# of Dampened Paths                       = 0,
# of Unsynchronized Paths                 = 0,
# of Policy unfeasible paths              = 0,
Total Number of Paths                     = 0
```

output definitions

# of Active Prefixes Known	The number of prefixes, or route paths, currently known to the local BGP speaker, that are currently up and active.
# of EBGP Neighbors in Established State	The number of peers outside the AS of the local BGP speaker that the local BGP speaker can route to.
# of IBGP Neighbors in Established State	The number of peers in the same AS as the local BGP speaker that the local BGP speaker can route to.
# of Feasible Paths	The number of route paths that are not active due to one of the following reasons: the route is dampened, the route is not permitted based on BGP policies, or the route is waiting to be synchronized with the IGP protocol.
# of Dampened Paths	The number of route paths that are not active because they have violated dampening parameters.
# of Unsynchronized Paths	The number of route paths that are not active because they are waiting to be synchronized with the IGP routing protocol.

output definitions (continued)

# of Unfeasible Paths	The number of route paths that are not active because they are not permitted based on a configured BGP policy.
Total Number of Paths	The total number of paths known to the speaker, active or not.

Release History

Release 5.1; command was introduced.

Related Commands

show ip bgp	Displays the current global settings for the local BGP speaker.

MIB Objects

```
alaBgpStatsTable
```

show ip bgp dampening

Displays the BGP route dampening settings.

show ip bgp dampening

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

This command shows the setting for dampening on the switch, assuming it is enabled.

Example

```
-> show ip bgp dampening
Admin Status                    = disabled,
Half life value (seconds)       = 300,
Reuse value                     = 200
Suppress value                  = 300,
Max suppress time (seconds)     = 1800,
```

output definitions

Admin Status	Indicates whether route dampening is enabled or disabled. This value is configured through the **ip bgp dampening** command.
Half life value	The half-life interval, in seconds, after which the penalty value for a reachable route will be reduced by half. This value is configured through the **ip bgp dampening** command.
Reuse value	The value that the route flapping metric must reach before this route is re-advertised. This value is configured through the **ip bgp dampening** command.
Suppress value	The number of route withdrawals necessary to begin readvertising a previously suppressed route. This value is configured through the **ip bgp dampening** command.
Max Suppress time	The maximum time (in seconds) that a route will be suppressed. This value is configured through the **ip bgp dampening** command.

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp dampening	Enables or disables BGP route dampening or the suppression of unstable routes.

MIB Objects

```
alaBgpDampTable
   alaBgpDampEntry
   alaBgpDampCeil
   alaBgpDampCutOff
   alaBgpDampMaxFlapHistory
   alaBgpDampReuse
   alaBgpDampening
   alaBgpDampeningClear
```

show ip bgp dampening-stats

Displays BGP dampening statistics.

show ip bgp dampening-stats [*ip_address ip_mask*] [*peer_address*]

Syntax Definitions

ip_address	A 32-bit IP address.
ip_mask	A 32-bit subnet mask number that determines how many bits of the IP address parameter denote the network number.
peer_address	A 32-bit IP address of peer (neighbor).

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

This command displays various statistics on routes that have flapped, and are thus subject to the settings of the dampening feature.

Example

```
-> show ip bgp dampening-stats
Network         Mask            From            Flaps Duration    FOM
--------------+---------------+---------------+-----+-----------+-----
155.132.44.73   255.255.255.255 192.40.4.121    8     00h:00m:35s 175
```

output definitions

Network	The IP address for the local BGP speaker that is responsible for route dampening in this switch.
Mask	The mask for the local BGP speaker that is responsible for route dampening in this switch.
From	The IP address for the route that is flapping.
Flaps	The number of times this route has moved from an UP state to a DOWN state or from a DOWN state to an UP state. If the route goes down and then comes back up, then this statistics would count 2 flaps.

output definitions (continued)

Duration	The time since the first route flap occurred. In the above example, this route has flapped 8 times in a 35 second period.
FOM	The Figure Of Merit, or instability metric, for this route. This value increases with each unreachable event. If it reaches the cutoff value (configured in **ip bgp dampening**), then this route will no longer be advertised.

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp dampening	Enables and disables route dampening.

show ip bgp path

Displays BGP paths.

show ip bgp path
[ip_addr *ip_address ip_mask***]**
[peer_addr *peer_address***]**
[aspath-list *aspathlist_name***]**
[community-list *community_list_name***]**
[prefix-list *prefix_name***]**
[route-map *routemap_name***]**
[cidr-only]
[community *community_number***]**
[neighbor_recv *recv_peer_address***]**
[neighbor_adv *adv_peer_addr***]**
[regexp "*regular_expression***"]**
[best]

Syntax Definitions

ip_address	A 32-bit IP address of the path.
ip_mask	A 32-bit subnet mask of the path.
peer_address	A 32-bit IP address of the path on which to filter.
aspathlist_name	AS path on which to filter.
community_list_name	Community name on which to filter.
prefix_name	Prefix on which to filter.
routemap_name	Route map on which to filter.
cidr-only	Filter out everything except CIDR routes.
community_number	Community number on which to filter.
recv_peer_address	Filter all except paths received from this path.
adv_peer_addr	Filter all except paths sent to this path.
regular_expression	Regular expression on which to filter. Regular expressions must be enclosed by quotes. For example, "$100".
best	Show only the best path.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

The basic command displays every path currently in the table. Since the number of paths may run into the thousands, this command provides a number of parameters for displaying a specific path or matching entries for a portion of a path or peer address.

Example

```
-> show ip bgp path
Legends: Sta     = Path state
         >       = best, F = feasible
         P       = policy changing, U = un-synchronized
         D       = dampened, N = none
         Nbr     = Neighbor
         (O)     = Path Origin (? = incomplete, i = igp, e = egp)
         degPref = degree of preference
Sta Network         Mask            Nbr address     Next Hop       (O)  degPref
---+--------------+---------------+--------------+--------------+---+--------
 >  192.40.4.0      255.255.255.0   192.40.4.29     192.40.4.29    i    100
 >  192.40.6.0      255.255.255.248 192.40.4.29     192.40.4.29    i    100
 >  192.40.6.8      255.255.255.248 192.40.4.29     192.40.4.29    i    100
 >  192.40.6.72     255.255.255.248 192.40.4.29     192.40.4.29    i    100
 >  192.40.6.80     255.255.255.248 192.40.4.29     192.40.4.29    i    100
 >  192.40.6.104    255.255.255.248 192.40.4.29     192.40.4.29    i    100
 >  192.40.6.112    255.255.255.248 192.40.4.29     192.40.4.29    i    100
 >  192.40.6.144    255.255.255.248 192.40.4.29     192.40.4.29    i    100
```

output definitions

Sta	Status flag. A greater-than sign (>) indicates this is the best route to the destination.
Network	The IP address for this route path. This is the destination of the route.
Mask	The mask for this route path.
Nbr address	The IP address of the BGP peer that is advertising this path.
Next Hop	The next hop along the route path.
(0)	The origin attribute of this route path. A question mark (**?**) indicates incomplete, and **i** indicates IGP, and an **e** indicates EGP.
degPref	The local preference value assigned to this route path.

```
-> show ip bgp path ip-addr 192.40.6.72 255.255.255.248
BGP Path parameters
Path address  = 192.40.6.72
Path mask     = 255.255.255.248
Path protocol = ebgp
Path peer     = 192.40.4.29
  Path nextHop            = 192.40.4.29,
  Path origin             = igp,
  Path local preference   = -1,
  Path state              = active,
  Path weight             = 0,
  Path preference degree  = 100,
  Path autonomous systems = [nAs=2] : 3 2 ,
  Path MED                = -1,
```

```
Path atomic             = no,
Path AS aggregator      = <none>,
Path IPaddr aggregator  = <none>,
Path community          = <none>,
Path unknown attribute  = <none>
```

output definitions

Path address	The IP address for route path.
Path mask	The mask for this route path.
Path protocol	The protocol from which this route path was learned. Possible values for this field are as follows: **local**, **static**, **directhost**, **rip**, **ospf**, **isis**, **ibgp**, **ebgp**, and **other**.
Path peer	The IP address of the peer that is advertising this route path.
Path nextHop	The next hop along the route path.
Path origin	The BGP origin attribute. Possible values will be **igp**, **egp**, **incomplete**, and **none**. The origin attribute is considered during the route decision process.
Path local preference	The local preference value for this route as received in an UPDATE message. A negative value (for example, the **-1** in the above display) indicates that the local preference value is missing for this route path.
Path state	Path state indicates the state of the path.The possible states are **best**, **feasible**, **policy-wait**, **un-synchronized**, **dampened**, or **none**. When path state is **none**, it indicates that there are no paths to this prefix and the route is being purged from the system.
Path weight	The path weight as assigned through inbound and outbound policies.
Path preference degree	The local preference assigned to this route through and inbound or outbound policy, or, if the local preference value is missing, the default local preference (which is assigned through the **ip bgp default local-preference**).
Path autonomous systems	The AS path for this route. These numbers show the ASs through which the route has traversed with the most recent AS listed first. In the above example, this route began its path in AS 2 and then traveled through AS 3.
Path MED	The multi-exit discriminator (MED) value for this route path. A negative value (for example, the **-1** in the above display) indicates that the MED value is missing for this route path.
Path atomic	Indicates whether the ATOMIC-AGGREGATE attribute has been set for this route. When set (this field would read **yes**), this attribute indicates that an aggregate has caused a loss of information for this route (a less specific route was chosen over a more specific route included in the aggregate).
Path AS aggregator	Part of the AGGREGATOR attribute. This field indicates the AS for the BGP speaker that created the aggregate. A value of **<none>** indicates this is not an aggregate route.
Path IPaddr aggregator	Part of the AGGREGATOR attribute. This field indicates the IP address for the BGP speaker that created the aggregate. A value of **<none>** indicates that this is not an aggregate route.

output definitions (continued)

Path community	Indicates the community to which this route path belongs, if applicable. A value of **<none>** indicates that this route does not belong to a community.
Path unknown attribute	Indicates BGP attributes found in UPDATE messages which the switch does not support. For example, multi-protocol attributes are not supported by the switch in this release, but it is possible for these attributes to appear in a BGP route.

Release History

Release 5.1; command was introduced.

Related Commands

show ip bgp routes	Displays BGP route details.

MIB Objects

```
alaBgpPathTable
   alaBgpPathEntry
```

show ip bgp routes

Displays BGP route details.

show ip bgp routes [*network_address ip_mask*]

Syntax Definitions

network_address	A 32-bit IP address.
ip_mask	A 32-bit subnet mask number that determines how many bits of the IP address parameter denote the network number

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

This command displays all the routes in the routing table with details.

Example

```
-> show ip bgp routes
Legends: ECL = EBGP change list, ICC = IBGP client change list
         ICL = IBGP change list, LCL = local change list
         AGG = Aggregation, AGC = Aggregation contribution
         AGL = Aggregation list, GDL = Deletion list
         AGW = Aggregation waiting, AGH = Aggregation hidden
         DMP = Dampening, ACT = Active route
Address         Mask            ECL ICC ICL LCL AGG AGC AGL AGW AGH GDL DMP ACT
--------------+---------------+---+---+---+---+---+---+---+---+---+---+---+---
192.40.4.0      255.255.255.0   No  No  No  No  No  No  No  No  No  No  No  Yes
192.40.6.0      255.255.255.248 No  No  No  No  No  No  No  No  No  No  No  Yes
192.40.6.8      255.255.255.248 No  No  No  No  No  No  No  No  No  No  No  Yes
192.40.6.72     255.255.255.248 No  No  No  No  No  No  No  No  No  No  No  Yes
192.40.6.80     255.255.255.248 No  No  No  No  No  No  No  No  No  No  No  Yes
192.40.6.104    255.255.255.248 No  No  No  No  No  No  No  No  No  No  No  Yes
192.40.6.112    255.255.255.248 No  No  No  No  No  No  No  No  No  No  No  Yes
192.40.6.144    255.255.255.248 No  No  No  No  No  No  No  No  No  No  No  Yes
```

output definitions

Address	The route destination network address.
Mask	The route destination network mask.
ECL	External BGP change list. When Yes, this route will be advertised as soon as the route advertisement timer expires.
ICC	Internal BGP client change list. When Yes, this route will be advertised to internal non-clients.

output definitions (continued)

ICL	Internal BGP change list. When Yes, this route has changes that need to be advertised.
LCL	Local change list. When Yes, this route is local.
AGG	Aggregation. When Yes, this route is an aggregate route.
AGC	Aggregation contribution. When Yes, this route is part of an aggregate route.
AGL	Aggregation list. When Yes, this route is placed on an aggregate list.
AGW	Aggregation waiting. When Yes, this route is waiting for an aggregate contributor.
AGH	Aggregation hidden. When Yes, this route is hidden as part of an aggregate route.
GDL	Deletion list. When Yes, this route will be deleted.
DMP	Dampening. Indicate whether this route has been dampened. If 'Yes', then this route has been dampened and a dampening history exists.
ACT	Active route. When Yes, the route is active.

Release History

Release 5.1; command was introduced.

Related Commands

show ip bgp path	Displays BGP paths.

MIB Objects

```
alaBgpRouteTable
   alaBgpRouteEntry
```

show ip bgp debug

Displays the current BGP debug level and types.

show ip bgp debug

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

This command displays the different debug options, if they are active, and what level of debugging is employed on each.

Example

```
-> show ip bgp debug
Debug Level = 1
Types/Sections
damp        = off,
fsm         = off,
recvupd     = off,
sendupd     = on,
open        = off,
keepalive   = on,
notify      = off,
policy      = on,
route       = off,
sync        = off,
aggr        = off,
tcp         = off,
warnings    = on,
errors      = on,
redist      = off,
peer        = off,
local       = off,
mip         = off,
tm          = off,
info        = on
```

output definitions

Debug Level	The level of debugging information being recorded. The range is 0 to 255. The currently defined levels are as follows: 10 -> Critical/Fatal errors 51 -> Non-Fatal Errors 71 -> Low level of debug output 74 -> Medium level of debug output 84 -> High level of debug output.
damp	Displays whether debugging information on dampening is turned on or off.
fsm	Displays whether debugging information on the BGP Finite State Machine information is turned on or off.
recvupd	Displays whether debugging information on received UDP packets is turned on or off.
sendupd	Displays whether debugging information on sent UDP packets is turned on or off.
open	Displays whether debugging information on BGP OPEN messages is turned on or off.
keepalive	Displays whether debugging information on KEEPALIVE messages is turned on or off.
notify	Displays whether debugging information on BGP NOTIFY messages is turned on or off.
policy	Displays whether debugging information on routing policies is turned on or off.
route	Displays whether debugging information on routes is turned on or off.
sync	Displays whether debugging information on BGP synchronization is turned on or off.
aggr	Displays whether debugging information on aggregate routes is turned on or off.
tcp	Displays whether debugging information on TCP packets is turned on or off.
warnings	Displays whether debugging information on BGP warnings is turned on or off.
errors	Displays whether debugging information on ERROR messages is turned on or off.
redist	Displays whether debugging information on redistribution filters is turned on or off.
peer	Displays whether debugging information on BGP peers is turned on or off.
local	Displays whether debugging information on local peers is turned on or off.
mip	Displays whether debugging information on MIP messages is turned on or off.

output definitions (continued)

tm	Displays whether debugging information on TM messages is turned on or off.
info	Displays whether debugging information on INFO messages is turned on or off.

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp debug-level	Sets the current BGP debug level.
ip bgp debug-type	Sets the type of BGP debug messages that are produced.

MIB Objects

```
alaBgpDebugLevel
alaBgpDebugType
```

show ip bgp aggregate-address

Displays aggregate route status.

show ip bgp aggregate-address [*ip_address ip mask*]

Syntax Definitions

ip_address	The 32-bit IP address of the aggregate address.
ip_mask	The 32-bit subnet mask number that determines how many bits of the IP address parameter denote the network number.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

This command displays a specific aggregate address, or all aggregate addresses on the switch.

Examples

```
-> show ip bgp aggregate-address
Network         Mask            Summarize As-Set   Admin state Oper state
--------------+---------------+---------+--------+-----------+----------
155.132.44.73   255.255.255.255 disabled  disabled disabled    not_active
192.40.6.0      255.255.255.255 disabled  disabled disabled    not_active

-> show ip bgp aggregate-address 192.40.6.0 255.255.255.255
Aggregate address          = 192.40.6.0,
Aggregate mask             = 255.255.255.255,
Aggregate admin state      = disabled,
Aggregate oper state       = not_active,
Aggregate as-set           = disabled,
Aggregate summarize        = disabled,
Aggregate metric           = 0,
Aggregate local preference = 0,
Aggregate community string = 0:500 400:1 300:2
```

output definitions

Network or **Aggregate address**	The IP address for this aggregate route. This value is configured through the **ip bgp aggregate-address** command.
Mask or **Aggregate mask**	The mask for this aggregate route. This value is configured through the **ip bgp aggregate-address** command.
Summarize or **Aggregate summarize**	Indicates whether aggregate summarization is enabled or disabled for this aggregate route. This value is configured through the **ip bgp aggregate-address summary-only** command.

output definitions (continued)

As-Set or **Aggregate as-set**	Indicates whether AS path aggregate is enabled or disabled. This value is configured through the **ip bgp aggregate-address as-set** command.
Admin State or **Aggregate admin state**	Indicates whether this aggregate route is administratively enabled or disabled. This value is configured through the **ip bgp aggregate-address status** command.
Oper State or **Aggregate oper state**	Indicates whether this aggregate route is operational and participating in BGP messages exchanges.
Aggregate metric	The multi-exit discriminator (MED) value configured for this aggregate route. This value is configured through the **ip bgp aggregate-address metric** command.
Aggregate local preference	The local preference value for this aggregate route. This value is configured through the **ip bgp aggregate-address local-preference** command.
Aggregate community string	The community string value for this aggregate route. This value is configured through the **ip bgp aggregate-address community** command.

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp aggregate-address	Creates and deletes a BGP aggregate route.

MIB Objects

```
alabgpMIBAggrGroup
   alaBgpAggrSet
   alaBgpAggrLocalPref
   alaBgpAggrMetric
   alaBgpAggrSummarize
   alaBgpAggrCommunity
```

show ip bgp network

Displays currently defined network configurations.

show ip bgp network [*network_address ip_mask*]

Syntax Definitions

network_address	A 32-bit IP address.
ip_mask	A 32-bit subnet mask number that determines how many bits of the IP address parameter denote the network number

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

This command displays all the configured networks, or a single network.

Example

```
-> show ip bgp network
Network         Mask            Admin state Oper state
---------------+---------------+-----------+----------
155.132.1.2     255.255.255.255 disabled    not_active
155.132.1.3     255.255.255.255 disabled    not_active


-> show ip bgp network 155.132.1.2 255.255.255.255
Network address          = 155.132.1.2,
Network mask             = 255.255.255.255,
Network admin state      = disabled,
Network oper state       = not_active,
Network metric           = 0,
Network local preference = 0,
Network community string = 0:500 400:1 300:2
```

output definitions

Network or **Network address**	The IP address configured for this local BGP network. This value is configured through the **ip bgp network** command.
Mask or **Network mask**	The mask configured for this local BGP network. This value is configured through the **ip bgp network** command.
Admin state or **Network admin state**	Indicates whether this local BGP network is administratively enabled or disabled. This value is configured through the **ip bgp network status** command.

output definitions (continued)

Oper state or **Network oper state**	Indicates whether this BGP local network is operationally active or inactive.
Network metric	The multi-exit discriminator (MED) value configured for this local BGP network. This value is configured through the **ip bgp network metric** command.
Network local preference	The local preference value for this local BGP network. This value is configured through the **ip bgp network local-preference** command.
Network community string	The community string value for this local BGP network. This value is configured through the **ip bgp network community** command.

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp network	Configures a a local BGP network.

MIB Objects

```
alabgpMIBNetworkGroup
   alaBgpNetworkEntry
```

show ip bgp neighbors

Displays BGP peer main status.

show ip bgp neighbors [*ip_address*]

Syntax Definitions

ip_address	A 32-bit IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

There are two output options for this command. If you specify show ip bgp peer without a peer IP address, then you see summary information for all peers known to the local BGP speaker. If you enter a specific peer IP address with the command, then you see detailed parameter information for that peer only.

Example

```
-> show ip bgp neighbors
Legends:Nbr = Neighbor
         As = Autonomous System
Nbr address     As    Admin state Oper state   BgpId           Up/Down
---------------+-----+-----------+------------+---------------+-----------
192.40.4.29     3     enabled     estab        192.40.4.29     00h:14m:48s
192.40.4.121    5     disabled    idle         0.0.0.0         00h:00m:00s
```

output definitions

Nbr address	The IP address for this BGP peer. Assign this address through the **ip bgp neighbor** command.
As	The autonomous system to which this peer belongs. A peer's AS number is assigned through the **ip bgp neighbor remote-as** command.
Admin state	Indicates whether this peer has been enabled or disabled through the **ip bgp neighbor status** command.
Oper state	The current BGP state for this peer. Possible states are **idle**, **connect**, **active**, **opensent**, **openconfirm**, and **established**.
BgpId	The unique BGP identifier of the peer. This value is configured through the **ip bgp neighbor update-source** command.
Up/Down	The time since this peer has transitioned to its current UP or DOWN state. If the peer is currently Established, then this is the time that the peer has been UP. If the peer is currently Idle, then this is the time the peer has been DOWN.

```
-> show ip bgp neighbors 0.0.0.1
Neighbor address                  = 0.0.0.1,
Neighbor autonomous system        = 1,
Neighbor Admin state              = enabled,
Neighbor Oper state               = connect,
Neighbor passive status           = disabled,
Neighbor name                     = peer(0.0.0.1),
Neighbor local address            = vlan-215,
Neighbor EBGP multiHop            = enabled,
Neighbor next hop self            = disabled,
Neighbor Route Refresh            = enabled,
Neighbor Ipv4 unicast             = enabled,
Neighbor Ipv4 multicast           = disabled,
Neighbor type                     = internal,
Neighbor auto-restart             = enabled,
Neighbor route-reflector-client   = disabled,
Neighbor confederation status     = disabled,
Neighbor remove private AS        = disabled,
Neighbor default originate        = disabled,
Neighbor maximum prefixes         = 5000,
Neighbor max prefixes warning     = enabled,
# of prefixes received            = 0,
Neighbor MD5 key                  = <none>,
Neighbor local port               = 0,
Neighbor TCP window size          = 32768
```

output definitions

Neighbor address	The IP address for this BGP peer. Assign this address through the **ip bgp neighbor** command.
Neighbor autonomous system	The autonomous system to which this peer belongs. A peer's AS number is assigned through the **ip bgp neighbor remote-as** command.
Neighbor Admin state	Indicates whether this peer has been enabled or disabled through the **ip bgp neighbor status** command.
Neighbor Oper state	The current BGP state for this peer. Possible states are **idle**, **connect**, **active**, **opensent**, **openconfirm**, and **established**.
Neighbor passive status	Indicates whether the local BGP speaker is "passive" (i.e., waiting for this peer to initiate a session). This value is configured through the **ip bgp neighbor passive** command.
Neighbor name	The name assigned to this peer through the **ip bgp neighbor description** command.
Neighbor local address	The interface assigned to this peer. This value is configured through the **ip bgp neighbor update-source** command.
Neighbor EBGP multihop	Indicates whether BGP multi-hop support is enabled or disabled. This supports allows external BGP peers to communicate with each other even when they are not directly connected. This value is configured through the **ip bgp neighbor ebgp-multihop** command.
Neighbor next hop self	Indicates whether this peer is using next hop processing. This value is configured through the **ip bgp neighbor next-hop-self** command.

output definitions (continued)

Neighbor Route Refresh	Indicates whether this peer supports Route Refresh capability as defined in RFC 2918. This capability is an alternative to soft-reconfiguration that can save CPU and memory resources. It allows peers to dynamically request the re-advertisement of BGP routing tables. Since this switch supports route refresh all BGP peers are automatically enabled for this capability.
Neighbor Ipv4 unicast	Indicates whether this peer is multi-protocol IP version 4 unicast capable. This switch is IP v4 unicasts capable so all peers will be enabled for this capability.
Neighbor Ipv4 multicast	Indicates whether this peer is multi-protocol IP version 4 multicast capable. This switch is not IP v4 multicasts capable so all peers will be disabled for this capability.
Neighbor type	Indicates whether this peer is internal or external to the switch.
Neighbor auto-restart	Indicates whether peer auto-restart is enabled or disabled. This value is configured through the **ip bgp neighbor auto-restart** command.
Neighbor route-reflector-client	Indicates whether this peer is a client to the local route reflector, if configured. This value is configured through the **ip bgp neighbor route-reflector-client** command.
Neighbor confederation status	Indicates whether this peer is a member of a BGP confederation. This value is configured through the **ip bgp confederation neighbor** command.
Neighbor remove private AS	Indicates whether the stripping of private AS numbers (64512 to 65535) from AS paths is enabled or disabled. This value is configured through the **ip bgp neighbor remove-private-as** command.
Neighbor default originate	Indicates whether peer default origination is enabled or disabled. When enabled, the local BGP speaker advertises itself as a default to the peer. This value is configured through the **ip bgp neighbor default-originate** command.
Neighbor maximum prefixes	The maximum number of prefixes the local router can receive in UPDATE from this peer. This value is configured through the **ip bgp neighbor maximum-prefix** command.
Neighbor max prefixes warning	Indicates whether a warning will be issued when this peer exceeds 80 percent of the maximum prefix value. This value is configured through the **ip bgp neighbor update-source** command.
# of prefixes received	Displays the total number of prefixes received by this neighbor.
Neighbor MD5 key [32- 47]	When present, shows an encrypted version of the MD5 password. When not present, and MD5 password has not been configured. This value is configured through the **ip bgp neighbor md5 key** command.
Neighbor local port	The TCP port used for the session with this peer.
Neighbor TCP window size	The size of the TCP window for this BGP session. This value will always be 32768 as that is the maximum size of a BGP message.

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp neighbor	Creates or deletes a BGP peer.

MIB Objects

```
alabgpMIBPeerGroup
   alaBgpPeerAddr
   alaBgpPeerAS
   alaBgpPeerPassive
   alaBgpPeerName
   alaBgpPeerMultiHop
   alaBgpPeerMaxPrefix
   alaBgpPeerMaxPrefixWarnOnly
   alaBgpPeerNextHopSelf
   alaBgpPeerSoftReconfig
   alaBgpPeerInSoftReset
   alaBgpPeerIpv4Unicast
   alaBgpPeerIpv4Multicast
   alaBgpPeerRcvdRtRefreshMsgs
   alaBgpPeerSentRtRefreshMsgs
   alaBgpPeerRouteMapOut
   alaBgpPeerRouteMapIn
   alaBgpPeerLocalAddr
   alaBgpPeerLastDownReason
   alaBgpPeerLastDownTime
   alaBgpPeerLastReadTime
   alaBgpPeerRcvdNotifyMsgs
   alaBgpPeerSentNotifyMsgs
   alaBgpPeerLastSentNotifyReason
   alaBgpPeerLastRecvNotifyReason
   alaBgpPeerRcvdPrefixes
   alaBgpPeerDownTransitions
   alaBgpPeerType
   alaBgpPeerAutoReStart
   alaBgpPeerClientStatus
   alaBgpPeerConfedStatus
   alaBgpPeerRemovePrivateAs
   alaBgpPeerClearCounter
   alaBgpPeerTTL
   alaBgpPeerAspathListOut
   alaBgpPeerAspathListIn
   alaBgpPeerPrefixListOut
   alaBgpPeerPrefixListIn
   alaBgpPeerCommunityListOut
   alaBgpPeerCommunityListIn
   alaBgpPeerRestart
   alaBgpPeerDefaultOriginate
   alaBgpPeerReconfigureInBound
   alaBgpPeerReconfigureOutBound
   alaBgpPeerMD5Key
   alaBgpPeerMD5KeyEncrypt
   alaBgpPeerRowStatus
   alaBgpPeerUpTransitions
   alaBgpPeerLocalIntfName
```

show ip bgp neighbors policy

Displays BGP peer policy information.

show ip bgp neighbors policy [*ip_address*]

Syntax Definitions

ip_address	A 32-bit IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

This command displays all of the configured policies for the switch, or the polices configured for a specific peer.

Example

```
-> show ip bgp neighbors policy
Neighbor address  =  0.0.0.0,
  Neighbor autonomous system          = 1,
  Neighbor output policy map name     = <none>,
  Neighbor input policy map name      = <none>,
  Neighbor output aspath-list name    = <none>,
  Neighbor input aspath-list name     = <none>,
  Neighbor output prefix-list name    = <none>,
  Neighbor input prefix-list name     = <none>,
  Neighbor output community-list name = <none>,
  Neighbor input community-list name  = <none>,
  Neighbor soft reconfiguration       = enabled
Neighbor address  =  0.0.0.1,
  Neighbor autonomous system          = 1,
  Neighbor output policy map name     = <none>,
  Neighbor input policy map name      = <none>,
  Neighbor output aspath-list name    = <none>,
  Neighbor input aspath-list name     = <none>,
  Neighbor output prefix-list name    = <none>,
  Neighbor input prefix-list name     = <none>,
  Neighbor output community-list name = <none>,
  Neighbor input community-list name  = <none>,
  Neighbor soft reconfiguration       = enabled
```

output definitions

Neighbor autonomous system	The AS to which the peer is assigned. This can be assigned by using the **ip bgp neighbor remote-as** command.
Neighbor output policy map name	The outbound route map policy for the peer. This can be assigned by using the **ip bgp neighbor route-map** command.
Neighbor input policy map name	The inbound route map policy for the peer. This can be assigned by using the **ip bgp neighbor route-map** command.
Neighbor output aspath-list name	The outbound AS path list policy for the peer. This can be assigned by using the **ip bgp neighbor out-aspathlist** command.
Neighbor input aspath-list name	The inbound AS path list policy for the peer. This can be assigned by using the **ip bgp neighbor in-aspathlist** command.
Neighbor output prefix-list name	The outbound prefix list policy for the peer. This can be assigned by using the **ip bgp neighbor out-prefixlist** command.
Neighbor input prefix-list name	The inbound prefix list policy for the peer. This can be assigned by using the **ip bgp neighbor in-prefixlist** command.
Neighbor output community-list name	The outbound community list policy for the peer. This can be assigned by using the **ip bgp neighbor out-communitylist** command.
Neighbor input community-list name	The inbound community list policy for the peer. This can be assigned by using the **ip bgp neighbor in-communitylist** command.
Neighbor soft reconfiguration	Lists whether soft reconfigurations are enabled or disabled for this peer. This is configured using the **ip bgp neighbor soft-reconfiguration** command.

Release History

Release 5.1; command was introduced.

Related Commands

show ip bgp neighbors	Displays BGP peer main status.

show ip bgp neighbors timer

Displays BGP peer timer statistics.

show ip bgp neighbors timer [*ip_address*]

Syntax Definitions

ip_address	A 32-bit IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

This command displays the timer values for all peer associated with this speaker, or for a specific peer.

Example

```
-> show ip bgp neighbors timer
Legends: Nbr     = Neighbor
         As      = Autonomous System
         RtAdv   = Route Advertisement
         Kalive  = Keep Alive (actual)
         Ka(C)   = Configured Keep Alive
Nbr address     As    Hold  Hold(C) RtAdv Retry Kalive Ka(C)
---------------+-----+-----+-------+-----+-----+------+-----
192.40.4.29     3     90    90      30    120   30     30
192.40.4.121    5     0     90      30    120   0      30
```

output definitions

Nbr address	The IP address for this BGP peer. Assign this address through the **ip bgp neighbor** command.
As	The autonomous system to which this peer belongs. A peer's AS number is assigned through the **ip bgp neighbor remote-as** command.
Hold	The current count for the holdtime value.
Hold(C)	The holdtime value configured through the **ip bgp neighbor timers** command.
RtAdv	The route advertisement interval, in seconds, for updates between external BGP peers. This value is configured through the **ip bgp neighbor advertisement-interval** command.
Retry	The interval, in seconds, between retries by this peer to set up a connection via TCP with another peer. This value is configured through the **ip bgp neighbor timers** command.

output definitions (continued)

Kalive	The current count, in seconds, between keepalive messages. Keepalive messages do not contain route or status updates; they serve only to tell other peers that the connection is still live and this peer is reachable.
Ka(C)	The keepalive interval as configured through the **ip bgp neighbor timers** command.

Release History

Release 5.1; command was introduced.

Related Commands

show ip bgp neighbors	Displays BGP peer main status.

show ip bgp neighbors statistics

Displays BGP peer message statistics.

show ip bgp neighbors statistics [*ip_address*]

Syntax Definitions

ip_address	A 32-bit IP address of the peer.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

This command displays message statistics for all peers associated with this speaker, or with a specific peer.

Example

```
-> show ip bgp neighbors statistics
Legends: RMSGS = number of received messages, SMSGS = number of sent messages
         RUPDS = number of Update messages received,
         SUPDS = number of Update messages sent,
         RNOFY = number of Notify messages received,
         SNOFY = number of Notify messages sent
         RPFXS = number of prefixes received
         UPTNS = number of UP transitions
         DNTNS = number of DOWN transitions

 Nbr address    As    RMSGS SMSGS RUPDS SUPDS RNOFY SNOFY RPFXS UPTNS DNTNS
---------------+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----
192.40.4.29     3     110   123   5     0     0     1     8     2     2
192.40.4.121    5     0     0     0     0     0     0     0     0     0
```

output definitions

Nbr address	The IP address for this peer. This value is configured through the **ip bgp neighbor** command.
As	The autonomous system to which this peer belongs. This value is configured through the **ip bgp neighbor remote-as** command.
RMSGS	Total number of messages (UPDATE, NOTIFY, OPEN, KEEPALIVE) received by this peer.
SMSGS	Total number of messages (UPDATE, NOTIFY, OPEN, KEEPALIVE) sent by this peer.

output definitions (continued)

RUPDS	The number of route UPDATE messages received by this peer. UPDATE messages contain route reachability information, BGP attributes, and route feasibility information.
SUPDS	The number of route UPDATE messages sent by this peer. UPDATE messages contain route reachability information, BGP attributes, and route feasibility information.
RNOFY	The number of NOTIFY messages received by this peer. NOTIFY messages contain error information, such as unsupported parameters, invalid attributes, and holdtime expirations.
SNOFY	The number of NOTIFY messages sent by this peer. NOTIFY messages contain error information, such as unsupported parameters, invalid attributes, and holdtime expirations.
RPFXS	The number of unique route prefixes received by this peer.
UPTNS	The number of times this peer has come up, operationally.
DNTNS	Number of times this peer has gone down, operationally.

```
-> show ip bgp neighbors statistics 0.0.0.1
Neighbor address                  = 0.0.0.1,
# of UP transitions               = 0,
Time of last UP transition        = 00h:00m:00s,
# of DOWN transitions             = 0,
Time of last DOWN transition      = 00h:00m:00s,
Last DOWN reason                  = none,
# of msgs rcvd                    = 0,
# of Update msgs rcvd             = 0,
# of prefixes rcvd                = 0,
# of Route Refresh msgs rcvd      = 0,
# of Notification msgs rcvd       = 0,
Last rcvd Notification reason     = none [none]
Time last msg was rcvd            = 00h:00m:00s,
# of msgs sent                    = 0,
# of Update msgs sent             = 0,
# of Route Refresh msgs sent      = 0
# of Notification msgs sent       = 0,
Last sent Notification reason     = none [none]
Time last msg was sent            = 00h:00m:00s,
```

output definitions

Neighbor address	The IP address for this peer. This value is configured through the **ip bgp neighbor** command.
# of UP transitions	The number of times this peer has come up, operationally.
Time of last UP transition	The duration that this peer has been up.
# of DOWN transitions	Number of times this peer has gone down, operationally.
Time of last DOWN transition	The duration since this peer last went down.

output definitions (continued)

Last DOWN reason	Provides a message as the last reason why a peer went down. The possible reasons for going down are: user_request - user initiated conn_timeout - connection timer expired hold_timeout - hold timer expired bad_msg - received a bad message from neighbor fsm_blink - BGP FSM error peer_closed - neighbor closed connection peer_notify - neighbor sent fatal notification tcp_error - Fatal TCP error none - None
# of msgs rcvd	Total number of messages (UPDATE, NOTIFY, OPEN, KEEPALIVE) received from this peer.
# of Update msgs rcvd	The number of route UPDATE messages received from this peer. UPDATE messages contain route reachability information, BGP attributes, and route feasibility information.
# of prefixes rcvd	The number of unique route prefixes received by this peer.
# of Route Refresh msgs rcvd	The number of route refresh requests this peer has received. Route refresh requests request all routes learned be a peer.
# of Notification msgs rcvd	The number of NOTIFY messages received from this peer. NOTIFY messages contain error information, such as unsupported parameters, invalid attributes, and holdtime expirations.

output definitions (continued)

Last rcvd Notification reason	NOTIFY messages include errors codes. These error codes are listed in this field. They apply to the last NOTIFY message received from this peer. The notification reasons are listed in two parts separated by a dash (-). The following are possible notification reasons: message header error - synchronization loss message header error - bad length message header error - bad type open message error - unsupported version open message error - bad peer autonomous system open message error - bad peer bgp id open message error - unsupported option open message error - authentication failure open message error - unacceptable hold time open message error - unsupported capability update message error - malformed attribute update message error - unknown attribute update message error - missing wellknown attribute update message error - attribute flags error update message error - attribute length error update message error - invalid origin update message error - as loop update message error - invalid nexthop update message error - optional attribute error update message error - invalid network update message error - malformed aspath cease - maximum number of prefixes reached cease - administrative shutdown cease - peer de-configured cease- administrative reset cease- connection rejected cease - other configuration change cease - connection collision resolution cease - out of resources hold time out - none fsm error - none cease - none none - none
Time last msg was rcvd	The duration since a message was received from this peer.
# of msgs sent	Total number of messages (UPDATE, NOTIFY, OPEN, KEEPALIVE) sent to this peer.
# of Update msgs sent	The number of route UPDATE messages sent to this peer. UPDATE messages contain route reachability information, BGP attributes, and route feasibility information.
# of Route Refresh msgs sent	The number of route refresh requests this peer has sent. Route refresh requests request all routes learned be a peer.
# of Notification msgs sent	The number of NOTIFY messages sent to this peer. NOTIFY messages contain error information, such as unsupported parameters, invalid attributes, and holdtime expirations.

output definitions (continued)

Last sent Notification reason	NOTIFY messages include errors codes. These error codes are listed in this field. They apply to the last NOTIFY message sent by this peer. The notification reasons are listed in two parts separated by a dash (-). See the list of possible notification reasons under the description for the **Peer last received notification reason** field above.
Time last msg was sent	The duration since a message was sent to this peer.

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp neighbor	Creates or deletes a BGP peer.

show ip bgp policy aspath-list

Displays AS path list parameters.

show ip bgp policy aspath-list [*name***] [***"regular_expression"***]**

Syntax Definitions

name	An AS path name.
regular_expression	A regular expression. The regular expression must be enclosed by quotation marks.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- This command displays a list of all of the AS path policies for the switch, or a single policy selected by the list name or regular expression.
- Regular expressions are defined in the **ip bgp policy aspath-list** command on page 31-95.
- When using regular expressions in the CLI, the regular expression must be enclosed by quotation marks.

Example

```
-> show ip bgp policy aspath-list
Aspath List Name          Aspath regular expression
------------------------+-------------------------------------------------
aspl1                     (500 | 400) ? 300$
aspl2                     (500 | 400)

-> show ip bgp policy aspath-list aspl1
Aspath List name = aspl1
Aspath Regexp    = (500 | 400) ? 300$
  Admin state      = disabled,
  Priority         = 1,
  Action           = deny,
  Primary index    = 0,
```

output definitions

Aspath List name	The name of the AS path list. This is defined using the **ip bgp policy aspath-list** command.
Aspath regular expression	The regular expression that defines the AS path list. This is defined using the **ip bgp policy aspath-list** command.

output definitions (continued)

Admin state	The administration state of the AS path policy. It is either enabled or disable.
Priority	The AS path list priority. This defined using the **ip bgp policy aspath-list priority** command.
Action	The AS path list action, either permit or deny. This is defined using the **ip bgp policy aspath-list action**command.
Primary index	The instance identifier for the AS path list. This value is not configurable.

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp policy aspath-list	Creates or removes an AS path list.

MIB Objects

```
alabgpMIBAspathListGroup
   alaBgpAspathMatchListId
   alaBgpAspathMatchListRegExp
   alaBgpAspathMatchListPriority
   alaBgpAspathMatchListAction
   alaBgpAspathMatchListRowStatus
```

show ip bgp policy community-list

Displays community list parameters.

show ip bgp policy community-list [*name***] [***string***]**

Syntax Definitions

name	Community name.
string	Community match list string

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

This command displays a list of the community policies for the speaker, or a specific policy defined by its name or community match string.

Example

```
-> show ip bgp policy community-list
Community list name       Community string
--------------------------+--------------------------------------------------
adfasdf                   0:0

-> show ip bgp policy community-list coml1
Community List name = coml1
Community string    = 600:1
  Admin state               = disabled,
  Match type                = exact,
  Priority                  = 1,
  Action                    = deny,
  Primary index             = 0
```

output definitions

Community List name	The community list name. This is defined using the **ip bgp policy community-list** command.
Community string	The community list definition. This is defined using the **ip bgp policy community-list** command.
Admin state	The administration state of the community list policy, either enabled or disabled.
Match type	The match type of the community list. This is defined using the **ip bgp policy community-list match-type** command.

output definitions

Priority	The community list priority. This is defined using the **ip bgp policy community-list priority** command.
Action	The community list action. This is defined using the **ip bgp policy community-list action** command.
Primary index	The instance indentifier for the community list. This value is not configurable.

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp policy community-list	Creates or deletes a community list.

MIB Objects

```
alabgpMIBCommunityListGroup
   alaBgpCommunityMatchListId
   alaBgpCommunityMatchListString
   alaBgpCommunityMatchListPriority
   alaBgpCommunityMatchListType
   alaBgpCommunityMatchListAction
   alaBgpCommunityMatchListRowStatus
```

show ip bgp policy prefix-list

Displays prefix list parameters.

show ip bgp policy prefix-list [*name***] [***ip_address ip_mask***]**

Syntax Definitions

name	A prefix list name.
ip_address	A prefix list IP address.
ip_mask	An IP address mask.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

This command displays the list of prefix-list policies configured for the speaker, or a specific list determined by the list name or IP address and mask.

Example

```
-> show ip bgp policy prefix-list
Prefix List name          Prefix address  Prefix mask
--------------------------+---------------+---------------
pfxl1                     155.132.33.0    255.255.255.0
pfxl2                     155.148.32.0    255.255.255.0

-> show ip bgp policy prefix-list pfxl1
Prefix List name = pfxl1
Address          = 155.132.33.0
Mask             = 255.255.255.0
  Admin state        = disabled,
  Match Mask >= (GE) = 0,
  Match Mask <= (LE) = 0,
  Action             = deny
```

output definitions

Prefix List name	The name of the prefix list. This is defined using the **ip bgp policy prefix-list** command.
Address	The IP address of the prefix list. This is defined using the **ip bgp policy prefix-list** command.
Mask	The mask of the prefix list. This is defined using the **ip bgp policy prefix-list** command.
Admin state	The administrative state of the prefix list, either enabled or disabled.

output definitions (continued)

Match Mask >= (GE)	The GE match mask of the prefix list. This is defined using the **ip bgp policy prefix-list ge** command.
Match Mask <= (LE)	The GE match mask of the prefix list. This is defined using the **ip bgp policy prefix-list le** command.
Action	The action of the prefix list. This is defined using the **ip bgp policy prefix-list action** command.

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp policy prefix-list	Creates or deletes a prefix match list.

MIB Objects

```
alabgpMIBPrefixListGroup
   alaBgpPrefixMatchListId
   alaBgpPrefixMatchListAddr
   alaBgpPrefixMatchListMask
   alaBgpPrefixMatchListGE
   alaBgpPrefixMatchListLE
   alaBgpPrefixMatchListAction
   alaBgpPrefixMatchListRowStatus
```

show ip bgp policy route-map

Displays policy route map parameters.

show ip bgp policy route-map [*name***] [***sequence_number***]**

Syntax Definitions

name	Route map name.
sequence_number	A sequence number. The valid range is 1–255.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

The route map is displayed as a summary table by entering only the route map name, or as a detailed list by specifying the sequence number.

Example

```
-> show ip bgp policy route-map
RouteMap name             Instance
--------------------------+--------
rmap1                     1
rmap1                     2
rmap2                     1

-> show ip bgp policy route-map rmap1
RouteMap name     = rmap1
RouteMap instance = 1
  Admin state               = disabled,
  Local pref (mode/value)   = <none> / 0,
  Route map action          = permit,
  Origin                    = <none>,
  MED (mode/value)          = <none> / 0,
  Weight                    = 0,
  Aspath-List name          = aspl1,
  Aspath prepend            = <none>,
  Aspath match primitive    = 500 .* 400$,
  Prefix-List name          = <none>,
  Prefix match primitive    = 0.0.0.0 0.0.0.0,
  Community-List name       = coml2,
  Community match primitive = <none>,
  Community string [mode]   =  [Additive]
```

output definitions

RouteMap name	The name of the route map policy. This is determined using the **ip bgp policy route-map** command.
RouteMap instance	The instance of the route map policy. This is determined using the **ip bgp policy route-map** command.
Admin state	The administrative state of the route map policy, either enabled or disabled.
Local pref (mode/value)	The local preference of the route map policy. This is determined using the **ip bgp policy route-map lpref** command.
Route map action	The action of the route map policy. This is determined using the **ip bgp policy route-map action** command.
Origin	The origin of the route map policy. This is determined using the **ip bgp policy route-map origin** command.
MED (mode/value)	The MED of the route map policy. This is determined using the **ip bgp policy route-map med** command.
Weight	The weight of the route map policy. This is determined using the **ip bgp policy route-map weight** command.
Aspath-List name	The name of the AS path list attached to this route map.This is set using the **show ip bgp policy aspath-list** command.
Aspath prepend	The value to prepend to the AS_PATH attribute of the routes matched by this RouteMap instance (Empty quotes indicates no AS_PATH prepending is to be done).
Aspath match primitive	The regular expression used to match AS Path for this route map.
Prefix-List name	The name of the prefix list attached to this route map. This is set using the **show ip bgp policy prefix-list** command.
Prefix match primitive	The prefix to match for this route map.
Community-List name	The name of the community list attached to this route map. This is set using the **show ip bgp policy community-list** command.
Community match primitive	The community string to match for this route map.
Community string [mode]	The name of the community mode attached to this route map. This is set using the **ip bgp policy route-map community-mode** command.

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp policy route-map	Creates or deletes a policy route map.

MIB Objects

```
alabgpMIBRouteMapGroup
   alaBgpRouteMapName
   alaBgpRouteMapInst
   alaBgpRouteMapAsPathMatchListId
   alaBgpRouteMapPrefixMatchListId
   alaBgpRouteMapCommunityMatchListId
   alaBgpRouteMapOrigin
   alaBgpRouteMapLocalPref
   alaBgpRouteMapLocalPrefMode
   alaBgpRouteMapMed
   alaBgpRouteMapMedMode
   alaBgpRouteMapAsPrepend
   alaBgpRouteMapSetCommunityMode
   alaBgpRouteMapCommunity
   alaBgpRouteMapMatchAsRegExp
   alaBgpRouteMapMatchPrefix
   alaBgpRouteMapMatchMask
   alaBgpRouteMapMatchCommunity
   alaBgpRouteMapWeight
   alaBgpRouteMapAction
   alaBgpRouteMapRowStatus
```

show ip bgp redist-filter

Displays redistribution filter parameters for all protocols or a specific protocol.

show ip bgp redist-filter [local] [static] [rip] [ospf]

Syntax Definitions

local	Shows the redistributed local routes.
static	Shows the redistributed static routes.
rip	Shows the redistributed routes using the RIP protocol.
ospf	Shows the redistributed routes using the OSPF protocol.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

This command displays the redistributed routes for the speaker, or a select group of redistributed routes based on a protocol.

Example

```
-> show ip bgp redist-filter
Protocol   Address         Mask            Metric     Subnets  Effect Admin
----------+---------------+---------------+----------+--------+------+-----------
STATIC     1.2.3.4         255.255.255.255 0          enabled  permit disabled
RIP        155.132.0.0     255.255.0.0     0          enabled  permit disabled
OSPF       192.40.0.0      255.255.0.0     0          enabled  permit disabled

-> show ip bgp redist-filter rip
Addr            Mask            Metric     Subnets  Effect Admin state
--------------+---------------+----------+--------+------+-----------
155.132.0.0     255.255.0.0     0          enabled  permit disabled

-> show ip bgp redist-filter rip 155.132.0.0 255.255.0.0
Filter protocol         = OSPF,
Filter address          = 155.132.0.0,
Filter mask             = 255.255.0.0,
Filter admin state      = disabled,
Filter metric           = 0,
Filter local preference = 0,
Filter community string = <none>,
Filter subnet           = enabled,
Filter effect           = deny
```

output definitions

Protocol	The protocol type of the route redistribution, which is one of the following: static, local, RIP, or OSPF.
Address	The destination address of the route.
Mask	The destination mask of the route.
Metric	The assigned metric of the redistributed route. This command is set using the **ip bgp redist-filter metric** command.
Subnets	Shows whether the redistribution of subnets is enabled of disabled. This is set using the **ip bgp redist-filter subnets** command.
Effect	The effect of the redistribution on this route. This is set using the **ip bgp redist-filter effect** command.
Admin	The administrative state of the redistribution filter. This is set using the **ip bgp redist-filter** command.
Filter local preference	The value to override the default local preference sent to internal peers. If 0, then no override is applied.
Filter community string	The value to set the community attribute when advertising this network.

Release History

Release 5.1; command was introduced.

Related Commands

ip bgp redist-filter	Creates or deletes a local redistribution filter.

MIB Objects

```
alabgpMIBRedistRouteGroup
   alaBgpRedistRouteProto
   alaBgpRedistRouteDest
   alaBgpRedistRouteMask
   alaBgpRedistRouteMetric
   alaBgpRedistRouteLocalPref
   alaBgpRedistRouteCommunity
   alaBgpRedistRouteSubnetMatch
   alaBgpRedistRouteEffect
   alaBgpRedistRouteRowStatus
   alaBgpRedistRouteSubnetMatch
```

32 PIM-SM Commands

Protocol-Independent Multicast (PIM) is an IP multicast routing protocol that uses routing information provided by unicast routing protocols such as RIP and OSPF. Note that PIM is not dependent on any particular unicast routing protocol. Sparse mode PIM (PIM-SM) contrasts with flood-and-prune dense mode multicast protocols such as DVMRP and PIM Dense Mode (PIM-DM) in that multicast forwarding in PIM-SM is initiated only via specific requests.

Downstream routers must explicitly join PIM-SM distribution trees in order to receive multicast streams on behalf of directly-connected receivers or other downstream PIM-SM routers. This paradigm of receiver-initiated forwarding makes PIM-SM ideal for network environments where receiver groups are thinly populated and bandwidth conservation is a concern such as in wide area networks (WANs).

Note. Omni Switch/Router software supports PIM-SM version 2 and is not compatible with older implementations.

MIB information for the PIM-SM commands is as follows:

Filename: AlcatelIND1Pimsm.mib
Module: ALCATEL-IND1-PIMSM-MIB

Filename: IETF_PIM.mib
Module: PIM-MIB

A summary of the available commands is listed here:

ip load pimsm
ip pimsm status
ip pimsm cbsr-masklength
ip pimsm static-rp status
ip pimsm static-rp
ip pimsm rp-candidate
ip pimsm rp-threshold
ip pimsm crp-address
ip pimsm crp-expirytime
ip pimsm crp-holdtime
ip pimsm crp-interval
ip pimsm crp-priority
ip pimsm data-timeout
ip pimsm joinprune-interval
ip pimsm max-rps
ip pimsm probe-time
ip pimsm register checksum
ip pimsm registersuppress-timeout
ip pimsm spt status
ip pimsm interface
ip pimsm interface hello-interval
ip pimsm interface joinprune-interval
ip pimsm interface cbsr-preference
ip pimsm interface dr-priority
ip pimsm interface prune-delay status
ip pimsm interface prune-delay
ip pimsm interface override-interval
ip pimsm interface triggered-hello
ip pimsm interface hello-holdtime
ip pimsm interface genid
ip pimsm interface joinprune-holdtime
ip pimsm debug-level
ip pimsm debug-type
show ip pimsm
show ip pimsm neighbor
show ip pimsm rp-candidate
show ip pimsm rp-set
show ip pimsm interface
show ip pimsm nexthop
show ip pimsm mroute
show ip pimsm static-rp
show ip pimsm debug

ip load pimsm

Dynamically loads PIM-SM to memory.

ip load pimsm

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- This command must be executed before PIM-SM can run on the switch.
- The advanced routing image file (**Fadvrout.img** on OmniSwitch 7700/7800, **Eadvrout.img** on OmniSwitch 8800) file must be loaded before the feature will work on the switch.

Examples

```
-> ip load pimsm
```

Release History

Release 5.1; command was introduced.

Related Commands

ip pimsm status	Globally enables or disables PIM-SM protocol on the switch.
show ip pimsm	Displays global parameters for the PIM-SM domain.

MIB Objects

```
alaDrcTmConfig
   alaDrcTmIPPimsmStatus
```

ip pimsm status

Globally enables or disables PIM-SM protocol on the switch.

ip pimsm status {enable | disable}

Syntax Definitions

enable	Globally enables PIM-SM on the switch.
disable	Globally disables PIM-SM on the switch.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- This command must be set to **enable** before PIM-SM can run on the switch. In addition, the **ip load pimsm** command must be executed. Refer to page 32-3 for more information.
- The **Fadvrout.img** file must be loaded to flash before the feature will work on the switch.
- To enable or disable PIM-SM for a particular interface, refer to the **ip pimsm interface** command on page 32-25.

Examples

```
-> ip pimsm status enable
-> ip pimsm status disable
```

Release History

Release 5.1; command was introduced.

Related Commands

ip pimsm interface	Enables or disables PIM-SM protocol on a specific interface.
ip load pimsm	Dynamically loads PIM-SM to memory.
show ip pimsm	Displays global parameters for the PIM-SM domain.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmAdminStatus
```

ip pimsm cbsr-masklength

Configures the length of the mask used in the hash function when computing the Rendezvous Point (RP) for a multicast group.

ip pimsm cbsr-masklength *bits*

Syntax Definitions

bits	Specifies the mask length, in bits (1–32).

Defaults

parameter	default
bits	30

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> ip pimsm cbsr-masklength 30
```

Release History

Release 5.1; command was introduced.

Related Commands

ip pimsm interface cbsr-preference	Configures the preference value for a local interface as a candidate bootstrap router.
show ip pimsm	Displays global parameters for the PIM-SM domain.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmAdminBSRHashmasklen
```

ip pimsm static-rp status

Enables or disables static RP configuration for use with group-to-RP mapping.

ip pimsm static-rp status {enable | disable}

Syntax Definitions

enable	Enables static RP configuration for group-to-RP mapping. If static RP configuration is enabled, the Bootstrap Mechanism will be automatically disabled.
disable	Disables static RP configuration for group-to-RP mapping.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Although the **ip pimsm static-rp status** command enables the switch for static RP configuration, actual static RPs must be added via the **ip pimsm static-rp** command.
- As mentioned above, if static RP configuration is enabled, the bootstrap mechanism will be automatically disabled. When the bootstrap mechanism is disabled, no bootstrap messages or C-RP advertisements are sent from the switch; any bootstrap or C-RP advertisements received are ignored.
- If static RP configuration is enabled, the same static RP configuration setting must be defined on all PIM-SM switches within the domain. This will ensure that the PIM-SM switches have the same RP set information.
- To view whether static RP configuration is currently enabled or disabled (default), use the **show ip pimsm** command. To display the static RP table, use the **show ip pimsm static-rp** command.

Examples

```
-> ip pimsm static-rp status enable
-> ip pimsm static-rp status disable
```

Release History

Release 5.1; command was introduced.

Related Commands

ip pimsm static-rp	Adds, modifies, or deletes a static RP group.
show ip pimsm	Displays global parameters for the PIM-SM domain.
show ip pimsm rp-set	Displays the list of reachable C-RPs for an IP multicast group.
show ip pimsm static-rp	Displays the PIM Static RP table, which includes group address/ mask, the static Rendezvous Point (RP) address, and the current status of Static RP configuration (i.e., enabled or disabled).

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmAdminStaticRPConfig
```

ip pimsm static-rp

Adds, modifies, or deletes a static RP group (“modifies” applies only to the RP Address, since the table is indexed from group address and mask parameters). This group will be used in the group-to-RP mapping algorithm if the static RP configuration status is enabled.

ip pimsm static-rp *group_address mask rp_address*

no ip pimsm static-rp *group_address mask rp_address*

Syntax Definitions

group_address	Specifies a 32-bit group address.
mask	Specifies a 32-bit group mask.
rp_address	Specifies a 32-bit Rendezvous Point (RP) address.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to delete a static RP group.
- Changes will take effect only if the global static RP status is enabled. For information on enabling global static RP status, refer to the **ip pimsm static-rp status** command on page 32-6.
- To view current static RP configuration settings, use the **show ip pimsm static-rp** command.

Examples

```
-> ip pimsm static-rp 224.0.0.0 240.0.0.0 10.1.1.1
```

Release History

Release 5.1; command was introduced.

Related Commands

ip pimsm static-rp status	Enables or disables static RP configuration for use with group-to-RP mapping.
show ip pimsm	Displays global parameters for the PIM-SM domain.
show ip pimsm rp-set	Displays the list of reachable C-RPs for an IP multicast group.
show ip pimsm static-rp	Displays the PIM Static RP table, which includes group address/mask, the static Rendezvous Point (RP) address, and the current status of Static RP configuration (i.e., enabled or disabled).

MIB Objects

```
alaPimsmStaticRPTable
   alaPimsmStaticRPGroupAddress
   alaPimsmStaticRPGroupMask
   alaPimsmStaticRPAddress
   alaPimsmStaticRPRowStatus
```

ip pimsm rp-candidate

Adds, modifies, or deletes a multicast range for C-RP advertisements (“modifies” applies only to the RP Address since the table is indexed from group address and mask parameters).

ip pimsm rp-candidate *group_address mask rp_address*

no ip pimsm rp-candidate *group_address mask rp_address*

Syntax Definitions

group_address	Specifies a 32-bit group address.
mask	Specifies a 32-bit group mask.
rp_address	Specifies a 32-bit Rendezvous Point (RP) address.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to delete a multicast range for C-RP advertisements.
- Bootstrap Routers (BSRs) in PIM-SM support RP-specific expiry timers. As a result, disabling or deleting individual C-RP entries requires that PIM-SM status be disabled on the corresponding interface until former RP entries are aged in the domain. PIM-SM status for the interface can then be re-enabled. New or re-enabled C-RP entries do not require a change in C-RP or BSR status.
- To change the PIM-SM status for a specific interface, refer to the **ip pimsm interface** command on page 32-25.

Examples

```
-> ip pimsm rp-candidate 224.0.0.0 240.0.0.0 10.1.1.1
```

Release History

Release 5.1; command was introduced.

Related Commands

ip pimsm crp-address	Specifies the IP address used as the source in candidate rendezvous point (C-RP) advertisements.
show ip pimsm rp-candidate	Displays the PIM RP Candidate Table.

MIB Objects

```
pimCandidateRPTable
   pimCandidateRPGroupAddress
   pimCandidateRPGroupMask
   pimCandidateRPAddress
   pimCandidateRPRowStatus
```

ip pimsm rp-threshold

Specifies the data rate, in bits per second (Bps), at which the Rendezvous Point (RP) will attempt to switch to native forwarding by issuing a source-specific (S, G) join message toward the source.

ip pimsm rp-threshold *bps*

Syntax Definitions

bps	The data rate value, in bits per second, at which the RP will attempt to switch to native forwarding (0–2147483647).

Defaults

parameter	default
bps	65536

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- To disable the RP threshold feature, specify a bits per second value of 0. When the RP threshold is disabled, the RP will never initiate an (S, G) Join message toward the source; the packets will be register-encapsulated to the RP.
- To view the current RP threshold, use the **show ip pimsm** command.

Examples

```
-> ip pimsm rp-threshold 131072
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip pimsm	Displays global parameters for the PIM-SM domain.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmRPThreshold
```

ip pimsm crp-address

Specifies the IP address used as the source in Candidate Rendezvous Point (C-RP) advertisements.

ip pimsm crp-address *ip_address*

no ip pimsm crp-address

Syntax Definitions

ip_address	Specifies the 32-bit source IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a C-RP advertisement source address. (You can also specify a zero (0) value for the IP address to remove a C-RP advertisement source address.)
- If the IP address value is non-zero, the router is configured to be a C-RP. If the IP address value is zero, the router is *not* configured to be a C-RP.
- If static RP configuration is enabled, the switch will not act as a C-RP—even if the C-RP address is defined.

Examples

```
-> ip pimsm crp-address 0.0.0.0
-> no ip pimsm crp-address
-> ip pimsm crp-address 172.2.1.21
```

Release History

Release 5.1; command was introduced.

Related Commands

ip pimsm rp-candidate	Adds, modifies, or deletes a multicast range for C-RP advertisements.
show ip pimsm	Displays global parameters for the PIM-SM domain.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmCRPAddress
```

ip pimsm crp-expirytime

Configures the maximum time a PIM-SM router considers the current candidate rendezvous point (C-RP) active.

ip pimsm crp-expirytime *seconds*

Syntax Definitions

seconds	Specifies the expiry time, in seconds (1–300).

Defaults

parameter	default
seconds	300

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> ip pimsm crp-expirytime 10
```

Release History

Release 5.1; command was introduced.

Related Commands

ip pimsm crp-holdtime	Configures the holdtime of the component when it is a C-RP in the local domain.
ip pimsm crp-interval	Configures the interval at which a C-RP router's advertisements are sent to the bootstrap router.
ip pimsm crp-priority	Configures C-RP router's priority.
show ip pimsm	Displays global parameters for the PIM-SM domain.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmCRPExpiryTime
```

ip pimsm crp-holdtime

Configures the Candidate Rendezvous Point (C-RP) holdtime. The C-RP holdtime is the amount of time, in seconds, the C-RP advertisement is considered valid. This value is specified in C-RP advertisement messages if the router is configured to be a C-RP.

ip pimsm crp-holdtime *seconds*

Syntax Definitions

seconds	Specifies the holdtime value, in seconds (0–255).

Defaults

parameter	default
seconds	150

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

A value of zero (0) turns off the C-RP mechanism. When the C-RP mechanism is turned off, the switch will not act as a C-RP.

Examples

```
-> ip pimsm crp-holdtime 120
-> ip pimsm crp-holdtime 0
```

Release History

Release 5.1; command was introduced.

Related Commands

ip pimsm crp-address	Configures the IP address used as the source in CRP advertisements.
ip pimsm crp-interval	Configures the interval at which a C-RP router's advertisements are sent to the bootstrap router.
ip pimsm crp-priority	Configures C-RP router's priority.
show ip pimsm	Displays global parameters for the PIM-SM domain.

MIB Objects

```
pimComponentTable
   pimComponentCRPHoldTime
```

ip pimsm crp-interval

Configures the interval at which a C-RP router's advertisements are sent to the bootstrap router.

ip pimsm crp-interval *seconds*

Syntax Definitions

seconds	Specifies the interval time, in seconds (1–300).

Defaults

parameter	default
seconds	60

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

The **ip pimsm crp-interval** command is applicable only if the switch is configured to be a C-RP (i.e., the C-RP address is set to a non-zero value). Refer to page 32-13 for C-RP address information.

Examples

```
-> ip pimsm crp-interval 60
```

Release History

Release 5.1; command was introduced.

Related Commands

ip pimsm crp-address	Configures the IP address used as the source in CRP advertisements.
ip pimsm crp-holdtime	Configures the holdtime of the component when it is a C-RP in the local domain.
ip pimsm crp-priority	Configures C-RP router's priority.
show ip pimsm	Displays global parameters for the PIM-SM domain.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmCRPInterval
```

ip pimsm crp-priority

Configures C-RP router's priority.

ip pimsm crp-priority *priority*

Syntax Definitions

priority	Specifies the router priority (0–128). The lower the value, the higher the priority.

Defaults

parameter	default
priority	0

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- The priority value is included in the C-RP advertisements sent by the switch (if the switch is configured to be a C-RP).
- This priority value is used in determining which RP maps to a particular multicast group.

Examples

```
-> ip pimsm crp-priority 0
```

Release History

Release 5.1; command was introduced.

Related Commands

ip pimsm crp-address	Configures the IP address used as the source in CRP advertisements.
ip pimsm crp-holdtime	Configures the holdtime of the component when it is a C-RP in the local domain.
ip pimsm crp-interval	Configures the interval at which a C-RP router's advertisements are sent to the bootstrap router.
show ip pimsm	Displays global parameters for the PIM-SM domain.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmCRPPriority
```

ip pimsm data-timeout

Configures the time after which Source, Group (S,G) state will be deleted for a source that is no longer transmitting.

ip pimsm data-timeout *seconds*

Syntax Definitions

seconds	Specifies the data timeout value, in seconds (1–300).

Defaults

parameter	default
seconds	210

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> ip pimsm data-timeout 210
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip pimsm	Displays global parameters for the PIM-SM domain.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmDataTimeout
```

ip pimsm joinprune-interval

Configures the default interval at which periodic PIM-SM join/prune messages are sent.

ip pimsm joinprune-interval *seconds*

Syntax Definitions

seconds	Default interval, in seconds (1–300).

Defaults

parameter	default
seconds	60

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

The value specified by this command will be used by default on *all* PIM-SM-enabled interfaces unless the **ip pimsm interface joinprune-interval** command is used to change the value for a specific interface. For information on using the **ip pimsm interface joinprune-interval** command, see page 32-28.

Examples

```
-> ip pimsm joinprune-interval 60
```

Release History

Release 5.1; command was introduced.

Related Commands

ip pimsm interface joinprune-interval	Configures the frequency at which periodic join/prune messages are transmitted on a specified interface.
show ip pimsm	Displays global parameters for the PIM-SM domain.

MIB Objects

```
pim
   pimJoinPruneInterval
```

ip pimsm max-rps

Configures the maximum number of C-RP routers allowed in the PIM-SM domain.

ip pimsm max-rps *number*

Syntax Definitions

number	The maximum number of C-RP routers allowed in the PIM-SM domain (1–100).

Defaults

parameter	default
number	32

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

PIM-SM must be globally disabled before changing the maximum number of C-RP routers. To globally disable PIM-SM, refer to the **ip pimsm status** command on page 32-4.

Examples

```
-> ip pimsm max-rps 32
```

Release History

Release 5.1; command was introduced.

Related Commands

ip pimsm status	Globally enables or disables PIM-SM protocol on the switch.
show ip pimsm	Displays global parameters for the PIM-SM domain.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmMaxRPs
```

ip pimsm probe-time

Configures the amount of time before the register suppression timer expires, at which point the Designated Router (DR) sends a Null Register message to the Rendezvous Point (RP). This allows the RP to refresh the Register Stop. If the Register Suppression timer expires, the DR will resume encapsulating packets from the source to the RP.

ip pimsm probe-time *seconds*

Syntax Definitions

seconds	The probe time, in seconds (1–300).

Defaults

parameter	default
seconds	5

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> ip pimsm probe-time 5
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip pimsm	Displays global parameters for the PIM-SM domain.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmProbeTime
```

ip pimsm register checksum

Configures the application of the checksum function on sent and received register messages in the domain.

ip pimsm register checksum {header | full}

Syntax Definitions

header	Specifies that the checksum for registers is done only on the PIM header.
full	Specifies that the checksum is done over the entire PIM register message.

Defaults

parameter	default
header | full	**header**

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- The **full** option may be required for compatibility with older implementations of PIM-SM v2.
- This parameter setting must be consistent across the PIM-SM domain.

Examples

```
-> ip pimsm register checksum header
-> ip pimsm register checksum full
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip pimsm	Displays global parameters for the PIM-SM domain.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmOldRegisterMessageSupport
```

ip pimsm registersuppress-timeout

Specifies the period during which a Designated Router (DR) stops sending Register-encapsulated packets to the Rendezvous Point (RP) after receiving a Register-Stop.

ip pimsm registersuppress-timeout *seconds*

Syntax Definitions

seconds	The timeout value, in seconds (1–300).

Defaults

parameter	default
seconds	60

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> ip pimsm registersuppress-timeout 10
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip pimsm	Displays global parameters for the PIM-SM domain.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmRegisterSuppressionTimeout
```

ip pimsm spt status

Enables or disables last hop Designated Router (DR) switching to the Shortest Path Tree (SPT). If enabled, last hop DR switching to the SPT begins once the first data packet is received.

ip pimsm spt status {enable | disable}

Syntax Definitions

enable	Enables last hop DR switching to the SPT.
disable	Disables last hop DR switching to the SPT.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- As mentioned above, if SPT status is enabled, last hop DR switching to the SPT begins once the first data packet is received.
- To view whether SPT status is currently enabled (default) or disabled, use the **show ip pimsm** command.

Examples

```
-> ip pimsm spt status enable
-> ip pimsm spt status disable
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip pimsm	Displays global parameters for the PIM-SM domain.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmAdminSPTConfig
```

ip pimsm interface

Enables or disables the PIM-SM protocol on a specific interface.

ip pimsm interface *ip_address*

no ip pimsm interface *ip_address*

Syntax Definitions

ip_address	The 32-bit IP address for the interface on which PIM-SM is being enabled or disabled.

Defaults

By default, PIM-SM is disabled on all interfaces.

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

PIM-SM must be enabled globally on the switch before PIM-SM will begin running on the interface. To globally enable or disable PIM-SM on the switch, refer to the **ip pimsm status** command on page 32-4.

Examples

```
-> ip pimsm interface 172.22.2.115
```

Release History

Release 5.1; command was introduced.

Related Commands

ip pimsm status	Globally enables or disables PIM-SM protocol on the switch.
ip pimsm interface hello-interval	Configures the frequency at which PIM-SM hello messages are transmitted on a specified interface.
ip pimsm interface joinprune-interval	Configures the frequency at which periodic join/prune messages are transmitted on a specified interface.
ip pimsm interface cbsr-preference	Configures the preference value for the local interface as a candidate bootstrap router.
ip pimsm interface dr-priority	Specifies the Designated Router priority inserted into the DR priority option on a specified interface.
ip pimsm interface prune-delay status	Enables or disables the LAN prune-delay option on a specified interface.
ip pimsm interface prune-delay	Specifies the value, in milliseconds, inserted into the LAN Prune Delay field of a LAN Prune Delay option on a specified interface.
ip pimsm interface override-interval	Specifies the value inserted into the Override Interval field of a LAN Prune Delay option on this interface if the prune-delay status is enabled.
ip pimsm interface triggered-hello	Specifies the maximum time, in seconds, before a triggered PIM Hello message is transmitted on the corresponding interface.
ip pimsm interface hello-holdtime	Specifies the value, in seconds, to be set in the Holdtime field of Hello messages transmitted on the specified interface.
ip pimsm interface genid	Enables or disables the Generation ID option on a specified interface.
ip pimsm interface joinprune-holdtime	Specifies the value inserted into the Holdtime field of a Join/Prune message sent on the corresponding interface.
show ip pimsm interface	Displays detailed PIM-SM settings for a specific interface, or general PIM-SM settings for all interfaces.

MIB Objects

```
pimInterfaceTable
   pimInterfaceIfIndex
   pimInterfaceStatus
```

ip pimsm interface hello-interval

Configures the frequency at which PIM-SM Hello messages are transmitted on a specified interface.

ip pimsm interface *ip_address* **hello-interval** *seconds*

Syntax Definitions

ip_address	The 32-bit IP address for the interface on which the hello interval is being set.
seconds	The Hello interval, in seconds. Values may range from 1–300.

Defaults

parameter	default
seconds	30

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

A PIM-SM interface must be created via the **ip pimsm interface** command before the Hello interval value can be configured.

Examples

```
-> ip pimsm interface 172.22.2.115 hello-interval 30
```

Release History

Release 5.1; command was introduced.

Related Commands

ip pimsm interface	Enables or disables PIM-SM protocol on a specific interface.
ip pimsm interface hello-holdtime	Specifies the value, in seconds, to be set in the Holdtime field of Hello messages transmitted on the specified interface.
ip pimsm interface triggered-hello	Specifies the maximum time, in seconds, before a triggered PIM Hello message is transmitted on the corresponding interface.
show ip pimsm	Displays global parameters for the PIM-SM domain.

MIB Objects

```
pimInterfaceTable
   pimInterfaceIfIndex
   pimInterfaceHelloInterval
```

ip pimsm interface joinprune-interval

Configures the frequency at which periodic join/prune messages are transmitted on a specified interface.

ip pimsm interface *ip_address* **joinprune-interval** *seconds*

Syntax Definitions

ip_address	The 32-bit IP address for the interface on which the join/prune interval is being set.
seconds	The join/prune interval, in seconds (1–300).

Defaults

The default value for the join/prune interval matches the interval specified by the **ip pimsm joinprune-interval** command. The switch's default **ip pimsm joinprune-interval** command setting is 60 seconds.

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- A PIM-SM interface must be created via the **ip pimsm interface** command before the Join/Prune interval can be configured.
- To view the current join/prune interval for an interface, refer to the **show ip pimsm interface** command on page 32-61.

Examples

```
-> ip pimsm interface 172.22.2.115 joinprune-interval 60
```

Release History

Release 5.1; command was introduced.

Related Commands

ip pimsm interface	Enables or disables PIM-SM protocol on a specific interface.
ip pimsm joinprune-interval	Configures the default interval at which periodic PIM-SM join/prune messages are sent.
ip pimsm interface joinprune-holdtime	Specifies the value inserted into the Holdtime field of a Join/Prune message sent on the corresponding interface.
show ip pimsm interface	Displays the current PIM-SM status for a specific interface or for all interfaces.

MIB Objects

```
pimInterfaceTable
   pimInterfaceIfIndex
   pimInterfaceJoinPruneInterval
```

ip pimsm interface cbsr-preference

Configures the preference value for a local interface as a candidate bootstrap router.

ip pimsm interface *ip_address* **cbsr-preference** *value*

Syntax Definitions

ip_address	The 32-bit IP address for the interface on which the C-BSR preference is being set.
value	The C-BSR preference value (0–255). The higher the value, the higher the priority.

Defaults

parameter	default
value	0

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- A value of -1 is used to specify that the interface is *not* to be considered as a C-BSR. If all interfaces have a C-BSR preference of -1, the switch will not act as a C-BSR.
- If all PIM-SM interfaces are enabled and currently running (i.e., each IP interface is up), the interface with the highest priority becomes the C-BSR for the switch. If the priority levels are equal across all interfaces, the interface with the highest IP address will become the C-BSR for the switch.
- A PIM-SM interface must be created via the **ip pimsm interface** command before the C-BSR preference can be specified.

Examples

```
-> ip pimsm interface 172.22.2.115 cbsr-preference 0
```

Release History

Release 5.1; command was introduced.

Related Commands

ip pimsm interface	Enables or disables PIM-SM protocol on a specific interface.
show ip pimsm	Displays global parameters for the PIM-SM domain.
show ip pimsm interface	Displays detailed PIM-SM settings for a specific interface, or general PIM-SM settings for all interfaces.

MIB Objects

```
pimInterfaceTable
   pimInterfaceIfIndex
   pimInterfaceCBSRPreference
```

ip pimsm interface dr-priority

Specifies the Designated Router priority inserted into the DR priority option on a specified interface. This value is used in determining the Designated Router on an interface.

ip pimsm interface *ip_address* **dr-priority** *priority*

Syntax Definitions

ip_address	The 32-bit IP address of a PIM-enabled VLAN on which the priority value is being defined.
priority	The DR priority option value (1–128). A higher numeric value denotes a higher priority.

Defaults

parameter	default
priority	1

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Higher priority values are preferred when choosing the Designated Router.
- Priority-based DR election is only enabled when all neighbors on an interface advertise that they are capable of using the DR election priority option.
- A PIM-SM interface must be created via the **ip pimsm interface** command before the DR priority can be configured.
- To view the current Designated Router (DR) priority, use the **show ip pimsm interface** command.

Examples

```
-> ip pimsm interface 172.22.2.120 dr-priority 20
```

Release History

Release 5.1; command was introduced.

Related Commands

ip pimsm interface	Enables or disables the PIM-SM protocol on a specific interface.
show ip pimsm neighbor	Displays a list of active PIM-SM neighbors.
show ip pimsm interface	Displays detailed PIM-SM settings for a specific interface, or general PIM-SM settings for all interfaces.

MIB Objects

```
pimInterfaceTable
   pimInterfaceIfIndex
   pimInterfaceDRPriority
```

ip pimsm interface prune-delay status

Enables or disables the LAN prune-delay option on a specified interface. The LAN prune-delay option expresses the expected message propagation delay on the link. It is used by upstream routers to determine how long to wait for a Join override message before pruning an interface.

ip pimsm interface *ip_address* **prune-delay status {enable | disable}**

Syntax Definitions

ip_address	The 32-bit IP address of a PIM-enabled VLAN on which the LAN Prune Delay status is being defined.
enable	Enables the LAN prune-delay option on the specified interface.
disable	Disables the LAN prune-delay option on the specified interface.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- This option controls whether or not the LAN prune-delay option is included in hello messages sent out on the interface. This information is not used unless all neighbors on the interface advertise the option. To determine whether the LAN prune-delay option is currently used by all neighbors on the interface, use the **show ip pimsm interface** command.
- A PIM-SM interface must be created via the **ip pimsm interface** command before the prune-delay status can be configured.
- To view whether the LAN prune-delay option is currently enabled or disabled (default) on an interface, use the **show ip pimsm interface** command. When using the **show ip pimsm interface** command to view LAN prune-delay status, be sure to specify the interface IP address in the command line. Refer to page 32-61 for details.

Examples

```
-> ip pimsm interface 172.22.2.120 prune-delay status enable
-> ip pimsm interface 168.140.14.2 prune-delay status disable
```

Release History

Release 5.1; command was introduced.

Related Commands

ip pimsm interface	Enables or disables the PIM-SM protocol on a specific interface.
ip pimsm interface prune-delay	Specifies the value, in milliseconds, inserted into the LAN Prune Delay field of a LAN Prune Delay option on a specified interface.
show ip pimsm neighbor	Displays a list of active PIM-SM neighbors.
show ip pimsm interface	Displays detailed PIM-SM settings for a specific interface, or general PIM-SM settings for all interfaces.

MIB Objects

```
pimInterfaceTable
   pimInterfaceIfIndex
   pimInterfaceLanPruneDelay
```

ip pimsm interface prune-delay

Specifies the value, in milliseconds, inserted into the LAN prune-delay option of the Hello message. This value expresses the expected message propagation delay on the link and is used by upstream routers to determine how long they must wait for a Join override message before pruning an interface.

ip pimsm interface *ip_address* **prune-delay** *milliseconds*

Syntax Definitions

ip_address	The 32-bit IP address of a PIM-enabled VLAN on which the prune-delay value is being defined.
milliseconds	The value to be inserted into the LAN Prune Delay field, in milliseconds (0–32767).

Defaults

parameter	default
milliseconds	500

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- The LAN prune-delay option must be *enabled* before these parameters can take effect. For information on enabling the prune-delay option, refer to the **ip pimsm interface prune-delay status** command on page 32-34.
- A PIM-SM interface must be created via the **ip pimsm interface** command before the prune-delay can be configured.
- To view the current prune-delay value for an interface, use the **show ip pimsm interface** command. When using the **show ip pimsm interface** command to view the prune-delay value, be sure to specify the interface IP address in the command line. Refer to page 32-61 for details.

Examples

```
-> ip pimsm interface 172.22.2.120 prune-delay 2000
```

Release History

Release 5.1; command was introduced.

Related Commands

ip pimsm interface	Enables or disables the PIM-SM protocol on a specific interface.
ip pimsm interface prune-delay status	Enables or disables the LAN prune-delay option on a specified interface.
show ip pimsm neighbor	Displays a list of active PIM-SM neighbors.
show ip pimsm interface	Displays detailed PIM-SM settings for a specific interface, or general PIM-SM settings for all interfaces.

MIB Objects

```
pimInterfaceTable
   pimInterfaceIfIndex
   pimInterfacePropagationDelay
```

ip pimsm interface override-interval

Specifies the value inserted into the Override Interval field of a LAN prune-delay option on this interface if the prune-delay status is enabled. This option is used to avoid synchronization of override messages when multiple downstream routers share a multi-access link. Sending of the override messages is delayed by a small random amount of time. The router's view of the amount of randomization necessary is expressed in the Override Delay field of the LAN prune-delay option.

ip pimsm interface *ip_address* **override-interval** *milliseconds*

Syntax Definitions

ip_address	The 32-bit IP address of a PIM-enabled VLAN on which the override interval value, in milliseconds, is being defined.
milliseconds	The value to be inserted into the Override Interval field, in milliseconds (0–65535).

Defaults

parameter	default
milliseconds	2500

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- The LAN prune-delay option must be *enabled* before these parameters can take effect. For information on enabling the prune-delay option, refer to the **ip pimsm interface prune-delay status** command on page 32-34.
- A PIM-SM interface must be created via the **ip pimsm interface** command before the override interval can be configured.
- To view the current override interval for an interface, use the **show ip pimsm interface** command. When using the **show ip pimsm interface** command to view the override interval, be sure to specify the interface IP address in the command line. Refer to page 32-61 for details.

Examples

```
-> ip pimsm interface 11.11.11.1 override-interval 3000
```

Release History

Release 5.1; command was introduced.

Related Commands

ip pimsm interface	Enables or disables the PIM-SM protocol on a specific interface.
ip pimsm interface prune-delay status	Enables or disables the LAN prune-delay option on a specified interface.
show ip pimsm neighbor	Displays a list of active PIM-SM neighbors.
show ip pimsm interface	Displays detailed PIM-SM settings for a specific interface, or general PIM-SM settings for all interfaces.

MIB Objects

```
pimInterfaceTable
   pimInterfaceIfIndex
   pimInterfaceOverrideInterval
```

ip pimsm interface triggered-hello

Specifies the maximum time, in seconds, before a triggered PIM Hello message is transmitted on the corresponding interface.

ip pimsm interface *ip_address* **triggered-hello** *seconds*

Syntax Definitions

ip_address	The 32-bit IP address of a PIM-enabled VLAN on which the triggered Hello value is being defined.
seconds	The amount of time, in seconds, before a triggered PIM Hello message is transmitted on the corresponding interface (1–65535).

Defaults

parameter	default
seconds	5

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- A PIM-SM interface must be created via the **ip pimsm interface** command before the triggered Hello value can be configured.
- To view the current triggered Hello value for an interface, use the **show ip pimsm interface** command. When using the **show ip pimsm interface** command to view the triggered Hello value, be sure to specify the interface IP address in the command line. Refer to page 32-61 for details.

Examples

```
-> ip pimsm interface 120.25.1.1 triggered-hello 120
```

Release History

Release 5.1; command was introduced.

Related Commands

ip pimsm interface	Enables or disables the PIM-SM protocol on a specific interface.
ip pimsm interface hello-interval	Configures the frequency at which PIM-SM Hello messages are transmitted on a specified interface.
ip pimsm interface hello-holdtime	Specifies the value, in seconds, to be set in the Holdtime field of Hello messages transmitted on the specified interface.
show ip pimsm interface	Displays detailed PIM-SM settings for a specific interface, or general PIM-SM settings for all interfaces.

MIB Objects

```
pimInterfaceTable
   pimInterfaceIfIndex
   pimInterfaceTrigHelloInterval
```

ip pimsm interface hello-holdtime

Specifies the amount of time a neighbor is considered valid—i.e., the Hello holdtime is used to timeout the neighbor state. A timer is reset to Hello holdtime whenever a Hello message containing the holdtime option is received. If the timer expires, the neighbor state is deleted.

ip pimsm interface *ip_address* **hello-holdtime** *seconds*

Syntax Definitions

ip_address	The 32-bit IP address of a PIM-enabled VLAN on which the Hello message holdtime value is being defined.
seconds	The amount of time, in seconds, for the interface's new Hello message holdtime value (0–65535).

Defaults

parameter	default
seconds	105

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- The specified holdtime should be 3.5 times the value of the Hello interval defined for the interface. To view the current Hello interval for an interface, use the **show ip pimsm interface** command. When using the **show ip pimsm interface** command to view the Hello interval, be sure to specify the interface IP address in the command line. Refer to page 32-61 for details.
- If the holdtime options are not used in the Hello messages, then a default Hello holdtime value of 105 seconds is used to timeout neighbors.
- A PIM-SM interface must be created via the **ip pimsm interface** command before the triggered Hello holdtime can be configured.
- For information on modifying the current Hello interval, refer to the **ip pimsm interface hello-interval** command on page 32-27.
- To view the current Hello holdtime for an interface, use the **show ip pimsm interface** command.

Examples

```
-> ip pimsm interface 120.120.2.10 hello-holdtime 560
```

Release History

Release 5.1; command was introduced.

Related Commands

ip pimsm interface	Enables or disables the PIM-SM protocol on a specific interface.
ip pimsm interface triggered-hello	Specifies the maximum time, in seconds, before a triggered PIM Hello message is transmitted on the corresponding interface.
ip pimsm interface hello-interval	Configures the frequency at which PIM-SM Hello messages are transmitted on a specified interface.
show ip pimsm interface	Displays the current PIM-SM status for a specific interface or for all interfaces.

MIB Objects

```
pimInterfaceTable
   pimInterfaceIfIndex
   pimInterfaceHelloHoldtime
```

ip pimsm interface genid

Enables or disables the Generation ID option on a specified interface.

ip pimsm interface *ip_address* **genid {enable | disable}**

Syntax Definitions

ip_address	The 32-bit IP address of a PIM-enabled VLAN on which the Generation ID status is being enabled or disabled.
enable	Enables the Generation ID option on the specified interface.
disable	Disables the Generation ID option on the specified interface.

Defaults

parameter	default
enable | **disable**	enable

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- A PIM-SM interface must be created via the **ip pimsm interface** command before the Generation ID status can be configured.
- To view whether the Generation ID option is currently enabled (default) or disabled, use the **show ip pimsm interface** command. Be sure to specify the corresponding interface IP address when entering the command.

Examples

```
-> ip pimsm interface 120.120.2.10 genid enable
-> ip pimsm interface 120.120.2.10 genid disable
```

Release History

Release 5.1; command was introduced.

Related Commands

ip pimsm interface	Enables or disables the PIM-SM protocol on a specific interface.
show ip pimsm interface	Displays detailed PIM-SM settings for a specific interface, or general PIM-SM settings for all interfaces.

MIB Objects

```
pimInterfaceTable
   pimInterfaceIfIndex
   pimInterfaceGenerationID
```

ip pimsm interface joinprune-holdtime

Specifies the value inserted into the holdtime field of a Join/Prune message sent on the corresponding interface. This value indicates the amount of time a Join/Prune message is considered valid.

ip pimsm interface *ip_address* **joinprune-holdtime** *seconds*

Syntax Definitions

ip_address	The 32-bit IP address of a PIM-enabled VLAN on which the Join/Prune holdtime is being defined.
seconds	The amount of time, in seconds, for the interface's new Join/Prune message holdtime value (0–65535).

Defaults

parameter	default
seconds	210

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- The specified holdtime should be 3.5 times the value of the Join/Prune interval defined for the interface. For information on viewing the current Join/Prune interval for an interface, refer to the **show ip pimsm interface** command on page 32-61.
- A PIM-SM interface must be created via the **ip pimsm interface** command before the Join/Prune holdtime can be configured.
- For information on modifying the current Join/Prune interval, refer to the **ip pimsm interface joinprune-interval** command on page 32-28.
- To view the current Join/Prune holdtime for an interface, use the **show ip pimsm interface** command. When using the **show ip pimsm interface** command to view the Join/Prune holdtime, be sure to specify the interface IP address in the command line. Refer to page 32-61 for details.

Examples

```
-> ip pimsm interface 120.120.2.10 joinprune-holdtime 350
```

Release History

Release 5.1; command was introduced.

Related Commands

ip pimsm interface	Enables or disables the PIM-SM protocol on a specific interface.
ip pimsm interface joinprune-interval	Configures the frequency at which periodic Join/Prune messages are transmitted on a specified interface.
show ip pimsm interface	Displays the current PIM-SM status for a specific interface or for all interfaces.

MIB Objects

```
pimInterfaceTable
   pimInterfaceIfIndex
   pimInterfaceJoinPruneHoldtime
```

ip pimsm debug-level

Defines the level of PIM-SM debug messages that are generated.

ip pimsm debug-level *level*

Syntax Definitions

level	Specifies the PIM-SM debug level (0–255). Higher debug-levels will include all messages that correspond to a lower value. For example, a debug-level of 1 will display only those messages that are defined with a level of 1; however, a debug level of 2 will display all messages of level 1 and level 2, etc. Higher levels will display detailed messages; lower levels will display basic messages.

Defaults

parameter	default
level	1

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

When the debug level is set to 0, PIM-SM debug logging is turned off.

Examples

```
-> ip pimsm debug-level 2
```

Release History

Release 5.1; command was introduced.

Related Commands

ip pimsm debug-type	Configures the type(s) of PIM-SM debug messages to display.
show ip pimsm debug	Displays the current PIM-SM debug levels and types.

MIB Objects

```
alaPimsmDebugConfig
   alaPimsmDebugLevel
```

ip pimsm debug-type

Configures the type(s) of PIM-SM debug messages to display.

ip pimsm debug-type *message_list*

no ip pimsm debug-type *message_list*

Syntax Definitions

message_list Specifies the type(s) of PIM-SM messages to be debugged. Select supported PIM-SM message types from the list below. You may enter multiple message types in any order. For example, **ip pimsm debug-type time bootstrap init**.

supported message types	descriptions
all	Enables or disables PIM-SM debugging for all items listed below. The syntax **all** can be used to easily turn debugging for all message types on or off.
assert	Enables or disables debugging for Assert processing.
bootstrap	Enables or disables debugging for Bootstrap Router (BSR) messages.
crp	Enables or disables debugging for Candidate Rendezvous Point (C-RP) messages.
error	Enables or disables debugging for PIM-SM Error handling.
hello	Enables or disables debugging for PIM-SM Hello messages.
igmp	Enables or disables debugging for Internet Group Management Protocol (IGMP) messages.
ipmrm	Enables or disables debugging for messages exchanged with IP Multicast Routing Manager (IPMRM).
init	Enables or disables debugging related to PIM-SM initialization code.
joinprune	Enables or disables debugging related to Join/Prune messages.
mip	Enables or disables debugging related to MIP (Management Internal Protocol).
misc	Enables or disables miscellaneous debugging of PIM-SM.
nbr	Enables or disables debugging for PIM-SM Neighbor processing.
route	Enables or disables debugging for PIM-SM Route processing.
spt	Enables or disables debugging related to Shortest-Path Tree (SPT).
time	Enables or disables debugging for PIM-SM Timer processing.
tm	Enables or disables debugging for PIM-SM Task Manager interaction.

Defaults

Debugging for error handling is *enabled* by default; all other options are disabled.

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- The message-types specified in the command line will only be displayed if the debug level has been set to a number greater than zero (i.e., 1–255). For information on specifying the debug level, refer to the **ip pimsm debug-level** command on page 32-48.
- The syntax **all** can be used to easily turn on/off all message types (e.g., **ip pimsm debug-type all** or **no ip pimsm debug-type all**).

Examples

```
-> ip pimsm debug-type all
-> ip pimsm debug-type bootstrap assert
-> no ip pimsm debug-type all
```

Release History

Release 5.1; command was introduced.

Related Commands

ip pimsm debug-level	Defines the level of PIM-SM messages that are generated.
show ip pimsm debug	Displays the current PIM-SM debug levels and types.

MIB Objects

```
alaPimsmDebugConfig
   alaPimsmDebugAll
   alaPimsmDebugAssert
   alaPimsmDebugBootstrap
   alaPimsmDebugCRP
   alaPimsmDebugError
   alaPimsmDebugHello
   alaPimsmDebugIgmp
   alaPimsmDebugInit
   alaPimsmDebugIpmrm
   alaPimsmDebugJoinPrune
   alaPimsmDebugMip
   alaPimsmDebugMisc
   alaPimsmDebugNbr
   alaPimsmDebugRoute
   alaPimsmDebugSpt
   alaPimsmDebugTime
   alaPimsmDebugTm
```

show ip pimsm

Displays global parameters for the PIM-SM domain.

show ip pimsm

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show ip pimsm
Status                     = enabled,
BSR Address                = 192.168.89.9,
BSR Expiry Time            = 00h:00m:00s,
CBSR Address               = 192.168.89.9,
CBSR Mask Length           = 30,
CBSR Priority              = 0,
CRP Address                = 0.0.0.0,
CRP Hold Time              = 0,
CRP Expiry Time            = 00h:05m:00s,
CRP Interval               = 60,
CRP Priority               = 0,
Data Timeout               = 210,
Join/Prune Interval        = 60,
Max RPs                    = 32,
Probe Time                 = 5,
Register Checksum          = header,
Register Suppress Timeout  = 60,
RP Threshold               = 65536,
SPT Status                 = enabled,
Static RP Configuration    = disabled
```

output definitions

Status	The current global (i.e., switch-wide) status of PIM-SM. Options include **enabled** and **disabled**. To change the current PIM-SM global status, refer to the **ip pimsm status** command on page 32-4.
BSR Address	The 32-bit IP address of the PIM domain's Bootstrap Router (BSR). For more information on BSRs, refer to the "Configuring PIM-SM" chapter of the applicable *OmniSwitch Advanced Routing Configuration Guide*.
BSR Expiry Time	The amount of time remaining before the BSR times out.
CBSR Address	A 32-bit IP address for the Candidate Bootstrap Router (C-BSR). This IP address is used to advertise the bootstrap message. Note that this IP address will be the interface address of a *PIM-enabled* VLAN.
CBSR Mask Length	The mask length, in bits, used in the hash function when computing the Rendezvous Point (RP) for a multicast group (1–32). The default value is 30.
CBSR Priority	The current candidate boostrap router (C-BSR) priority. The priority level of C-BSRs can be used to force the selection of a particular C-BSR. A higher numeric value denotes a higher priority (0–128). The default value is 0.
CRP Address	The IP address used as the source in candidate rendezvous point (C-RP) advertisements. If the IP address value is non-zero, the router is configured to be a C-RP. If the IP address value is zero, the router is *not* configured to be a C-RP.
CRP Hold Time	The amount of time, in seconds, the C-RP advertisement is considered valid. This value is specified in C-RP advertisement messages if the router is configured to be a C-RP (0–255). If the switch is acting as a C-RP, the default value is 150. If the switch is *not* acting as a C-RP, the default value is 0.
CRP Expiry Time	The amount of time until the PIM-SM router will consider the current candidate rendezvous point (C-RP) inactive, displayed in hours, minutes, and seconds.
CRP Interval	The interval at which the C-RP router's advertisements are sent to the bootstrap router (0–300). The default value is 60.
CRP Priority	The C-RP router's priority. The lower the value, the higher the priority (0–128). The default value is 0.
Data Timeout	The time after which (S,G) state will be deleted for a source that is no longer transmitting (0–300). The default value is 210.
Join/Prune Interval	The default interval at which periodic PIM-SM Join/Prune messages are sent (1–300). The default value is 60.
Max RPs	The maximum number of Rendezvous Points (RPs) allowed in the PIM-SM domain (1–100). The default value is 32.
Probe Time	The amount of time before the register suppression timer expires, at which point the Designated Router (DR) sends a Null Register message to the Rendezvous Point (RP). This allows the RP to refresh the Register Stop. If the Register Suppression timer expires, the DR will resume encapsulating packets from the source to the RP. Values may range from 1–300. The default value is 5.

output definitions (continued)

Register Checksum	The current application of the checksum function on register messages in the domain. Options include **header** and **full**. The default setting is **header**. To change the current checksum function, refer to the **ip pimsm register checksum** command on page 32-22.
Register Suppress Timeout	The amount of time, in seconds, the Designated Router (DR) will stop sending registers to the Rendezvous Point (RP) once a Register-Stop is received (1–300). The default value is 60.
RP Threshold	Displays the current RP data rate threshold. This value indicates the rate, in bits per second (Bps), at which the Rendezvous Point (RP) will attempt to switch to native forwarding by issuing a (S, G) join message toward the source. Values may range from 0–2147483647. The default value is 65536. A value of 0 indicates that the feature is currently disabled. To change the current RP threshold, refer to the **ip pimsm rp-threshold** command on page 32-12.
SPT Status	The current status of last hop Designated Router (DR) switching to the Shortest Path Tree (SPT). Options include **enabled** and **disabled**. The default setting is **enabled**. To change the current status, refer to the **ip pimsm spt status** command on page 32-24.
Static RP Configuration	Displays whether static RP configuration is currently enabled or disabled. Options include **enabled** and **disabled**. The default setting is **disabled**. To change the current status, refer to the **ip pimsm static-rp status** command on page 32-6.

Release History

Release 5.1; command was introduced.

Related Commands

show ip pimsm interface	Displays the PIM-SM protocol status for a specific interface.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmAdminStatus
   alaPimsmAdminBSRAddress
   alaPimsmBSRHashmasklen
   alaPimsmAdminBSRPriority
   alaPimsmAdminCRPExpiryTime
   alaPimsmAdminCRPInterval
   alaPimsmAdminCRPAddress
   alaPimsmAdminCRPPriority
   alaPimsmDataTimeout
   alaPimsmMaxRPs
   alaPimsmProbeTime
   alaPimsmOldRegisterMessageSupport
   alaPimsmRegisterSuppressionTimeout
   alaPimsmAdminStaticRPConfig
   alaPimsmAdminSPTConfig
   alaPimsmRPThreshold
```

```
pimComponentTable
   pimComponentBSRExpiryTime
   pimComponentCRPHoldTime
   pimComponentBSRAddress
pim
   pimJoinPruneInterval
```

show ip pimsm neighbor

Displays a list of active PIM-SM neighbors.

show ip pimsm neighbor [*ip_address***]**

Syntax Definitions

ip_address	The 32-bit IP address for a current PIM-SM neighbor. If an IP address is not specified, the entire PIM Neighbor Table is displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

To view more detailed information about a particular neighbor, specify the neighbor's IP address in the command line. Additional information includes LAN Prune Delay, Override Interval, TBit field, and Designated Router option status.

Examples

If a specific neighbor IP address is specified in the command line, *detailed information for the corresponding neighbor only* displays:

```
-> show ip pimsm neighbor 192.168.89.6
Neighbor IP Address        = 192.168.89.6,
Vlan ID                    = 89,
Uptime                     = 00h:36m:31s,
Expires                    = 00h:01m:15s,
Mode                       = Sparse,
Lan Prune Delay            = 0,
Override Interval          = 0.
TBit field                 = 0,
Designated Router Option   = true
```

If no neighbor IP address is specified in the command line, a *general table that includes all neighbors* displays, as shown:

```
-> show ip pimsm neighbor

Neighbor Address  Vlan     Uptime      Expires     Mode
-----------------+--------+-----------+-----------+-----------
192.168.89.6      89       00h:36m:31s 00h:01m:15s Sparse
```

output definitions

Neighbor (IP) Address	The 32-bit IP address of the active PIM-SM neighbor.
Vlan (ID)	The PIM-enabled VLAN associated with the PIM-SM neighbor's IP address.
Uptime	The amount of time since this PIM neighbor last became a neighbor of the local router, displayed in hours, minutes, and seconds.
Expires	The minimum amount of time remaining before the PIM neighbor will be aged out, displayed in hours, minutes, and seconds.
Mode	The current active PIM mode of the neighbor. Options include **Sparse** and **Sparse (DR)**. The syntax, (DR), indicates that the neighbor is currently the Designated Router on this interface.
Lan Prune Delay	The value of LAN Prune Delay field of the LAN Prune Delay option received from this neighbor. A value of 0 indicates that no LAN Prune Delay Option was received from this neighbor.
Override Interval	The current Override Interval of the LAN Prune Delay option received from this neighbor. This value is used to avoid synchronization of override messages when multiple downstream routers share a multi-access link. The sending of override messages is delayed at random time intervals. The amount of randomization used by the neighboring router is dictated by this number. Values may range from 0–65535. A value of 0 indicates that no LAN Prune Delay option was received from this neighbor.
TBit field	The value of the Tbit field of the LAN Prune Delay Option received from this neighbor. The Tbit specifies the ability of the neighbor to disable Join suppression.
Designated Router Option	Displays whether the neighbor is using the Designated Router option. Options include **true** or **false**.

Release History

Release 5.1; command was introduced.

Related Commands

N/A

MIB Objects

```
pimNeighborTable
   pimNeighborAddress
   pimNeighborIfIndex
   pimNeighborUpTime
   pimNeighborExpiryTime
   pimNeighborMode
   pimNeighborLanPruneDelay
   pimNeighborOverrideInterval
   pimNeighborTBit
   pimNeighborDRPresent
```

show ip pimsm rp-candidate

Displays the PIM RP Candidate Table.

show ip pimsm rp-candidate

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show ip pimsm rp-candidate

Group Address      RP Address      Status
-----------------+---------------+--------
224.10.10.10/32    143.209.92.177  enabled
```

output definitions

Group Address	The 32-bit IP address for a multicast group, along with the mask length, shown in bits. The group IP address and mask are separated by a slash (/).
RP Address	A 32-bit IP address of the Rendezvous Point (RP).
Status	The current status of the candidate RP.

Release History

Release 5.1; command was introduced.

Related Commands

ip pimsm rp-candidate	Adds, modifies, or deletes a multicast range for C-RP advertisements.

MIB Objects

```
pimCandidateRPTable
   pimCandidateRPGroupAddress
   pimCandidateRPGroupMask
   pimCandidateRPAddress
   pimCandidateRPRowStatus
```

show ip pimsm rp-set

Displays the list of reachable C-RPs for an IP multicast group.

show ip pimsm rp-set

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- If static RP configuration is being used, this information is obtained from those static RP addresses that are defined via the **ip pimsm static-rp** command. As long as the RP addresses defined in the static RP set are reachable, they will be added to the RP set.
- If the bootstrap mechanism is being used, this information is obtained from received Candidate-RP advertisements (when the local router is the BSR; when the local router is not the BSR, this information is obtained from received RP-Set messages).

Examples

```
-> show ip pimsm rp-set

Group Address      Address         Holdtime Expires
-----------------+---------------+--------+-----------
240.240.240.240/32 1.1.1.1         1        00h:00m:00s
```

output definitions

Group Address	The 32-bit multicast address for a multicast group, along with the mask length, shown in bits. The group IP address and mask are separated by a slash (/).
Address	The 32-bit IP address for a corresponding C-RP router.
HoldTime	The maximum amount of time, in seconds, a C-RP router's advertisement is considered valid. Values may range from 0–255. The default value is 0.
Expires	The amount of time remaining before the C-RP expires, displayed in hours, minutes, and seconds.

Release History

Release 5.1; command was introduced.

Related Commands

N/A

MIB Objects

```
pimRPSetTable
   pimRPSetGroupAddress
   pimRPSetGroupMask
   pimRPSetAddress
   pimRPSetHoldTime
   pimRPSetExpiryTime
```

show ip pimsm interface

Displays detailed PIM-SM settings for a specific interface, or general PIM-SM settings for all interfaces.

show ip pimsm interface [*ip_address***]**

Syntax Definitions

ip_address	The 32-bit IP address for a specific interface to be displayed. When an IP address is specified, detailed information for the corresponding interface only displays. If an IP address is *not* specified, a general interface table that includes all interfaces displays.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

To view more detailed information about a particular interface, specify the interface's IP address in the command line. Additional information includes VLAN ID, Triggered Hello Interval, Hello Holdtime, Prune Delay status and value, Override Interval, LAN Delay status, Generation ID status, and Join/Prune Holdtime.

Examples

If a specific interface IP address is specified in the command line, *detailed information for the corresponding interface only* displays:

```
-> show ip pimsm interface 192.168.9.9
IP Address                = 192.168.9.9,
Vlan ID                   = 9,
Designated Router         = 192.168.9.9,
Hello Interval            = 30,
Triggered Hello Interval  = 5
Hello HoldTime            = 105
Prune Delay Option        = disabled,
Prune Delay Value         = 500
Override Interval Value   = 2500,
Lan Delay Enabled         = false,
Generation ID Option      = on,
Join/Prune Interval       = 60,
Join/Prune Holdtime       = 210,
CBSR Preference           = 0,
DR Priority               = 1,
Operational Status        = enabled
```

If no interface IP address is specified in the command line, a *general interface table that includes all interfaces* displays, as shown:

```
-> show ip pimsm interface
Address         Designated      Hello    Join/Prune  CBSR   DR       Oper
                Router          Interval Interval    Pref   Priority Status
--------------+---------------+--------+-----------+------+--------+--------
192.168.9.9     192.168.9.9     30       60          0      1        enabled
192.168.59.9    192.168.59.9    30       60          0      1        disabled
192.168.61.9    192.168.61.9    30       60          0      1        enabled
192.168.89.9    192.168.89.9    30       60          0      1        enabled
```

(IP) Address	The 32-bit IP address assigned to a PIM-SM interface.
Designated Router	The 32-bit IP address for the Designated Router (DR). The DR acts on behalf of any directly-connected hosts with respect to the PIM-SM protocol. Only one router in the LAN will act as the DR.
Hello Interval	The frequency at which PIM-SM hello messages are transmitted on a specified interface. Values may range from 1–300. The default value is 30.
Triggered Hello Interval	The current Triggered Hello Interval. This value indicates the maximum time, in seconds, before a triggered PIM Hello message is transmitted on the corresponding interface. Values may range from 1–65535. The default value is 5. To change the current Triggered Hello Interval, refer to the **ip pimsm interface triggered-hello** command on page 32-40.
Hello Holdtime	The current Hello Holdtime value. This value indicates the maximum amount of time, in seconds, Hello messages will be held before they are considered invalid. Values may range from 0–65535. The default value is 105. The Hello Holdtime value should be 3.5 times the value of the Hello Interval defined for the interface. To change the current Hello Holdtime value, refer to the **ip pimsm interface hello-holdtime** command on page 32-42. For information on modifying the current Hello Interval, refer to the **ip pimsm interface hello-interval** command on page 32-27.
Prune Delay Option	The current status of the LAN prune-delay option on the interface. The LAN prune-delay option expresses the expected message propagation delay on the link. When enabled, it is used by upstream routers to determine how long to wait for a Join override message before pruning an interface. Options include **enabled** and **disabled**. The default setting is **disabled**. To enable or disable the LAN prune-delay option, refer to the **ip pimsm interface prune-delay status** command on page 32-34.
Prune Delay Value	The maximum amount of time, in milliseconds, that upstream routers will wait for a Join override message before pruning an interface. Values may range from 0–32767. The default value is 500. To change the current prune-delay value, refer to the **ip pimsm interface prune-delay** command on page 32-36.

Override Interval	The current Override Interval. This value is used to avoid synchronization of override messages when multiple downstream routers share a multi-access link. The sending of override messages is delayed at random time intervals. The amount of randomization used by a router is dictated by this number. Values may range from 0–65535. The default value is 2500. To change the current Override Interval, refer to the **ip pimsm interface override-interval** command on page 32-38.
Lan Delay Enabled	Options include **true** and **false**. The value will be true if all neighbors on the interface are using the LAN Prune Delay option. Otherwise, the setting will be false.
Generation ID Option	The current status of the Generation ID option on the interface. Options include **on** and **off**. The default setting is **on**. To enable or disable the Generation ID option, refer to the **ip pimsm interface genid** command on page 32-44.
Join/Prune Interval	The Join/Prune interval for the associated interface. The Join/Prune interval is the interval at which periodic PIM-SM Join/Prune messages are sent. Values may range from 1–300. The default value for the Join/Prune interval matches the interval specified by the **ip pimsm join-prune-interval** command. To change the interval for a specific interface, see the **ip pimsm interface joinprune-interval** command on page 32-28.
Join/Prune Holdtime	The current Join/Prune Holdtime value. This value indicates the maximum amount of time, in seconds, Join/Prune messages will be held before they are considered invalid. Values may range from 0–65535. The default value is 210. The Join/Prune Holdtime value should be 3.5 times the value of the Join/Prune Interval defined for the interface. To change the current Join/Prune Holdtime value, refer to the **ip pimsm interface joinprune-holdtime** command on page 32-46. For information on modifying the current Join/Prune Interval, refer to the **ip pimsm interface joinprune-interval** command on page 32-28.
CBSR Pref(erence)	The preference value for a local interface as a candidate bootstrap router. A value of -1 indicates the interface will *not* be considered a C-BSR. Values may range from 0–255. The default value is 0.
DR Priority	Displays the Designated Router priority for each interface. This value is used in determining the Designated Router on an interface. Values may range from 1–128. A higher numeric value denotes a higher priority. Note that priority-based election is used only if all routers on the interface are using the DR priority option. The default value is 1.To change the DR priority for a specific interface, see the **ip pimsm interface dr-priority** command on page 32-32.
Oper(ational) Status	The current operational status of the corresponding interface. Options include **enabled** and **disabled**. This value indicates whether the IP interface is operationally up. For example, if PIM-SM is enabled on the interface, but the IP interface is currently down, this field will display as disabled. The default setting is **disabled**. To enable or disable PIM-SM on an interface, refer to the **ip pimsm interface** command on page 32-25. To globally enable or disable PIM-SM on the switch, refer to the **ip pimsm status** command on page 32-4.

Release History

Release 5.1; command was introduced.

Related Commands

ip pimsm interface	Enables or disables the PIM-SM protocol on a specific interface.
show ip pimsm	Displays global parameters for the PIM-SM domain.

MIB Objects

```
pimInterfaceTable
   pimInterfaceAddress
   pimInterfaceDR
   pimInterfaceHelloInterval
   pimInterfaceHelloHoldtime
   pimInterfaceLanDelayEnabled
   pimInterfaceLanPruneDelay
   pimInterfaceOverrideInterval
   pimInterfaceGenerationID
   pimInterfaceJoinPruneInterval
   pimInterfaceJoinPruneHoldtime
   pimInterfaceCBSRPreference
   pimInterfaceDRPriority
   pimInterfaceStatus
   pimInterfaceIfIndex
   pimInterfaceTrigHelloInterval
   pimInterfacePropagationDelay
```

show ip pimsm nexthop

Displays the PIM-SM Next Hop Table.

show ip pimsm nexthop [*group_address source_address mask nexthop_address***]**

Syntax Definitions

group_address	A 32-bit multicast address. If an IP address is not specified, the current PIM-SM status for all next hop entries displays.
source_address	The 32-bit IP address for a specific multicast source.
mask	The mask value for the specified multicast source.
nexthop_address	The 32-bit IP address for the next hop address.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

If optional address, mask information, and next-hop address are not specified, the entire PIM-SM Next Hop Table is displayed.

Examples

```
-> show ip pimsm nexthop

Group Address   Src Address        Vlan   Next Hop Address
--------------+------------------+------+---------------
224.16.16.16    143.209.92.12/32   2      224.16.16.16
224.20.20.0     143.209.92.12/24   2      224.20.20.0
```

output definitions

Group Address	The 32-bit multicast address for a multicast group.
Src Address	The 32-bit source IP address, along with the mask length, shown in bits. The source IP address and mask are separated by a slash (/).
Vlan	The associated VLAN ID.
Next Hop Address	The 32-bit Next Hop multicast address.

Release History

Release 5.1; command was introduced.

Related Commands

show ip pimsm mroute	Displays the PIM-SM Multicast Routing table.
show ip mroute	Displays multicast routing information for IP datagrams sent by particular sources to the IP multicast groups known to this router.

MIB Objects

```
ipMRouteNextHopTable
   ipMRouteNextHopSource
   ipMRouteNextHopSourceMask
   ipMRouteNextHopIfIndex
   ipMRouteNextHopAddress
```

show ip pimsm mroute

Displays the PIM-SM Multicast routing table.

show ip pimsm mroute [*group_address source_address mask***]**

Syntax Definitions

group_address	A 32-bit multicast address. If an IP address is not specified, the current PIM-SM status for all multicast route entries displays.
source_address	The 32-bit IP address for a specific multicast source.
mask	The mask value for the specified multicast source.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

If optional address and mask information is not specified, the entire table is displayed.

Examples

If no Multicast route information is specified in the command line, a *table showing basic information* displays, as shown:

```
-> show ip pimsm mroute

Group Address   Src Address        Assert Assert      Assert Flags
                                   Metric expires     Pref
---------------+------------------+------+-----------+------+-----
225.0.0.1      192.168.9.1/32     0      00h:00m:00s 0      spt
```

If specific interface Multicast route information (i.e., group address, source address, and mask) is specified in the command line, *detailed information for the corresponding route* displays:

```
-> show ip pimsm mroute 225.0.0.1 192.168.9.1 255.255.255.255
Group IP Multicast Address  = 225.0.0.1,
Source IP Address           = 192.168.9.1/32,
RPF Neighbor                = 192.168.89.6,
Assert Metric               = 0,
Assert expires              = 00h:00m:00s,
Assert Preference           = 0,
Assert RPT Bit              = false,
Flags                       = spt
```

output definitions

Group (IP Multicast) Address	The 32-bit address for a multicast group.
Source (IP) Address	The 32-bit source IP address, along with the mask length, shown in bits. The source IP address and mask are separated by a slash (/).
RPF Neighbor	The IP Address of the current RPF neighbor. If there is an upstream assert winner, it will be designated as the RPF neighbor. Otherwise, the RPF neighbor will be the next hop, as determined by unicast routing.
Assert Metric	The current assert metric value advertised by the assert winner on the upstream interface. A value of 0 indicates that no such assert has been received. The metric value is essentially used to determine the most cost-effective way to pass data through the network. The higher the metric value, the higher the cost.
Assert expires	The time remaining before the router changes its upstream neighbor back to its RPF neighbor. A value of 0 indicates that no assert has changed the upstream neighbor away from the RPF neighbor. This value is displayed in hours, minutes, and seconds.
Assert Preference	The preference advertised by the assert winner on the upstream interface. A value of 0 indicates that no such assert is in effect.
Assert RPT Bit	The value of the RPT-bit advertised by the assert winner on the upstream interface. Options include **true** and **false**. False indicates either that the RPT bit is not set or that no such assert is in effect.
Flags	PIM-specific flags related to a multicast state entry. Options include **rpt** (RP-Tree) and **spt** (Shortest-Path Tree).

Release History

Release 5.1; command was introduced.

Related Commands

show ip pimsm nexthop	Displays the PIM-SM Next Hop Table.
show ip mroute-nexthop	Displays next-hop information on outgoing interfaces for routing IP multicast datagrams.
show ip mroute	Displays multicast routing information for IP datagrams sent by particular sources to the IP multicast groups known to this router.

MIB Objects

```
ipMRouteTable
   ipMRouteGroup
   ipMRouteSource
   ipMRouteSourceMask
pimIpMRouteTable
   pimIpMRouteRPFNeighbor
   pimIpMRouteAssertMetric
   pimIpMRouteUpstreamAssertTimer
   pimIpMRouteAssertMetricPref
   pimIpMRouteAssertRPTBit
   pimIpMRouteFlags
```

show ip pimsm static-rp

Displays the PIM Static RP table, which includes group address/mask, the static Rendezvous Point (RP) address, and the current status of Static RP configuration (i.e., enabled or disabled).

show ip pimsm static-rp

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show ip pimsm static-rp

Group Address      RP Address      Status
-----------------+---------------+--------
225.0.0.0/8        192.168.89.6    enabled
```

output definitions

Group Address	The 32-bit IP address for a multicast group, along with the mask length, shown in bits. The group IP address and mask are separated by a slash (/). To change the current multicast group address and mask, refer to the **ip pimsm static-rp** command on page 32-8.
RP Address	A 32-bit IP address of the Rendezvous Point (RP). To change the current RP address, refer to the **ip pimsm static-rp** command on page 32-8.
Status	Displays whether static RP configuration is currently enabled or disabled. Options include **enabled** and **disabled**. The default setting is **disabled**. To change the current status, refer to the **ip pimsm static-rp status** command on page 32-6.

Release History

Release 5.1; command was introduced.

Related Commands

ip pimsm static-rp status	Enables or disables static RP configuration for use with group-to-RP mapping.
ip pimsm static-rp	Adds, modifies, or deletes a static RP group.

MIB Objects

```
alaPimsmStaticRPTable
   alaPimsmStaticRPGroupAddress
   alaPimsmStaticRPGroupMask
   alaPimsmStaticRPAddress
alaPimsmGlobalConfig
   alaPimsmAdminStaticRPConfig
```

show ip pimsm debug

Displays the current PIM-SM debug levels and types.

show ip pimsm debug

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

The debug types displayed in the table are determined by the **ip pimsm debug-type** command on page 32-49. To configure debug levels, refer to the **ip pimsm debug-level** command on page 32-48.

Examples

```
-> show ip pimsm debug

Debug Level   = 1,
assert        = off,
bootstrap     = off,
crp           = off,
error         = off,
hello         = off,
igmp          = off,
init          = off,
ipmrm         = off,
joinprune     = off,
mip           = off,
misc          = off,
nbr           = off,
route         = off,
spt           = off,
time          = off,
tm            = off
```

output definitions

Debug Level	The current debug level value. For information on setting this parameter, see the **ip pimsm debug-level** command on page 32-48.
assert	The current debug setting for assert processing. Options include **on** or **off**.
bootstrap	The current debug setting for bootstrap. Options include **on** or **off**.
crp	The current debug setting for Candidate Rendezvous Point (C-RP). Options include **on** or **off**.

output definitions (continued)

error	The current debug setting for error handling. Options include **on** or **off**.
hello	The current debug setting for hello messages. Options include **on** or **off**.
igmp	The current debug setting for Internet Group Management Protocol (IGMP) packet processing. Options include **on** or **off**.
init	The current debug setting for initialization code. Options include **on** or **off**.
ipmrm	The current debug setting for IP Multicast Routing Manager (IPMRM). Options include **on** or **off**.
joinprune	The current debug setting for Join/Prune messages. Options include **on** or **off**.
mip	The current debug setting for MIP (Management Internal Protocol). Options include **on** or **off**.
misc	The current debug setting for miscellaneous message handling. Options include **on** or **off**.
nbr	The current debug setting for neighbors. Options include **on** or **off**.
route	The current debug setting for routes. Options include **on** or **off**.
spt	The current debug setting for Shortest-Path Tree (SPT).
time	The current debug setting for time. Options include **on** or **off**.
tm	The current debug setting for Task Manager. Options include **on** or **off**.

Release History

Release 5.1; command was introduced.

Related Commands

ip pimsm debug-level	Defines the level of PIM-SM debug messages that are generated.
ip pimsm debug-type	Configures the type(s) of PIM-SM debug messages to display.

MIB Objects

```
alaPimsmDebugConfig
   alaPimsmDebugLevel
   alaPimsmDebugAssert
   alaPimsmDebugBootstrap
   alaPimsmDebugCRP
   alaPimsmDebugError
   alaPimsmDebugHello
   alaPimsmDebugIgmp
   alaPimsmDebugInit
   alaPimsmDebugIpmrm
   alaPimsmDebugJoinPrune
   alaPimsmDebugMip
   alaPimsmDebugMisc
   alaPimsmDebugNbr
   alaPimsmDebugRoute
   alaPimsmDebugSpt
   alaPimsmDebugTime
   alaPimsmDebugTm
```

33 DVMRP Commands

This chapter includes CLI command descriptions for Distance Vector Multicast Routing Protocol (DVMRP), version 3.

DVMRPv3 is a dense-mode multicast routing protocol that enables routers to efficiently propagate IP multicast traffic through a network. Multicast traffic consists of a data stream that originates from a single source and is sent to hosts that have subscribed to that stream. Live video broadcasts, video conferencing, corporate communications, distance learning, distribution of software, stock quotes, and news services are examples of multicast traffic.

For more information about configuring DVMRP, see the applicable *OmniSwitch Advanced Routing Configuration Guide*.

MIB information for the DVMRP commands is as follows:

Filename: AlcatelIND1Dvmrp.MIB
Module: ALCATEL-IND1-DVMRP-MIB

Filename: IETF_DVMRP_STD_DRAFT.MIB
Module: DVMRP-STD-MIB

A summary of the available commands is listed here:

ip load dvmrp
ip dvmrp status
ip dvmrp flash-interval
ip dvmrp graft-timeout
ip dvmrp interface
ip dvmrp interface metric
ip dvmrp neighbor-interval
ip dvmrp neighbor-timeout
ip dvmrp prune-lifetime
ip dvmrp prune-timeout
ip dvmrp report-interval
ip dvmrp route-holddown
ip dvmrp route-timeout
ip dvmrp subord-default
ip dvmrp tunnel
ip dvmrp tunnel ttl
ip dvmrp debug-level
ip dvmrp debug-type
show ip dvmrp
show ip dvmrp interface
show ip dvmrp neighbor
show ip dvmrp nexthop
show ip dvmrp prune
show ip dvmrp route
show ip dvmrp tunnel
show ip dvmrp debug

ip load dvmrp

Dynamically loads DVMRP to memory.

ip load dvmrp

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command must be executed before DVMRP can be configured in the switch. In addition, DVMRP must be administratively enabled before you can run the protocol on the switch. For more information, refer to the **ip dvmrp status** command on page 33-3.
- The advanced routing image file (**Hadvrout.img** on OmniSwitch 6600 Family, **Fadvrout.img** on OmniSwitch 7700/7800, and **Eadvrout.img** on OmniSwitch 8800) must be loaded before the feature works in the switch.

Examples

```
-> ip load dvmrp
```

Release History

Release 5.1; command was introduced.

Related Commands

ip dvmrp status	Globally enables or disables DVMRP on the switch.

MIB Objects

```
alaDrcTmConfig
   alaDrcTmIPDvmrpStatus
```

ip dvmrp status

Globally enables or disables DVMRP on the switch.

ip dvmrp status {enable | safe-enable| unrestricted-enable | disable}

Syntax Definitions

enable	Administratively enables DVMRP on OmniSwitch 7700, 7800, and 8800 switches. This option is not valid in OmniSwitch 6600 Family switches.
safe-enable	Specifies that DVMRP will operate on safe-enable mode. This option is not valid in OmniSwitch 7700, 7800, and 8800 switches.
unrestricted-enable	Administratively enables DVMRP on OmniSwitch 6600 Family switches (i.e., unrestricted-enable mode). This option is not valid in OmniSwitch 7700, 7800, and 8800 switches.
disable	Administratively disables DVMRP on the switch.

Defaults

parameter	default
enable | safe-enable | unrestricted-enable |disable	**disable**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- In OmniSwitch 7700, 7800, and 8800 switches this command must be set to **enable** before DVMRP can run. In addition, the **ip load dvmrp** command must be issued. For more information, refer to the **ip load dvmrp** command on page 33-2.
- In the OmniSwitch 6600 Family switches this command must be set to **safe-enable** or **unrestricted-enable** before DVMRP can run. In addition, the **ip load dvmrp** command must be issued. For more information, refer to the **ip load dvmrp** command on page 33-2.
- The advanced routing image file (**Hadvrout.img** on OmniSwitch 6600 Family, **Fadvrout.img** on OmniSwitch 7700/7800, and **Eadvrout.img** on OmniSwitch 8800) must be loaded to flash before the feature works in the switch.
- To enable or disable DVMRP for a particular interface, refer to the **ip dvmrp interface** command on page 33-7.
- Use the safe-enable mode on OmniSwitch 6600 Family switches to eliminate potential problems with duplicate packets and routing loops in the network.
- Depending on the exact network setup, unrestricted-enable mode on OmniSwitch 6600 Family switches may cause potential networking problems by introducing duplicate packets and creating routing loops in the network.

Examples

OmniSwitch 7700, 7800, and 8800 switches:

```
-> ip dvmrp status enable
-> ip dvmrp status disable
```

OmniSwitch 6600 Family switches:

```
-> ip dvmrp status safe-enable
-> ip dvmrp status unrestricted-enable
-> ip dvmrp status disable
```

Release History

Release 5.1; command was introduced.
Release 5.4.1; **safe-enable** and **unrestricted-enable** parameters were added for OmniSwitch 6600 Family switches only.

Related Commands

ip dvmrp interface	Enables or disables DVMRP on a specified interface.
ip load dvmrp	Dynamically loads DVMRP to memory.
show ip dvmrp	Displays global DVMRP parameters, including current status.

MIB Objects

```
alaDvmrpGlobalConfig
   alaDvmrpAdminStatus
```

ip dvmrp flash-interval

Configures the minimum flash update interval value. The flash update interval defines how often routing table change messages are sent to neighboring DVMRP routers.

ip dvmrp flash-interval *seconds*

Syntax Definitions

seconds	Specifies the interval value, in seconds (5–86400).

Defaults

parameter	default
seconds	5

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Because routing table change messages are sent between the transmission of complete routing tables, the flash update interval value must be lower than the route report interval.

Examples

```
-> ip dvmrp flash-interval 5
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip dvmrp	Displays global DVMRP parameters.

MIB Objects

```
alaDvmrpGlobalConfig
   alaDvmrpFlashUpdateInterval
```

ip dvmrp graft-timeout

Configures the graft message retransmission value. The graft message retransmission value is the duration of time that the routing switch will wait before retransmitting a graft message if it has not received an acknowledgement from its neighbor.

ip dvmrp graft-timeout *seconds*

Syntax Definitions

seconds	Specifies the graft message retransmission value, in seconds (5–86400).

Defaults

parameter	default
seconds	5

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> ip dvmrp graft-timeout 5
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip dvmrp	Displays global DVMRP parameters.

MIB Objects

```
alaDvmrpGlobalConfig
   alaDvmrpGraftRetransmission
```

ip dvmrp interface

Enables or disables DVMRP on a specified interface.

ip dvmrp interface {*ip_address* | *interface_name***}**

no ip dvmrp interface {*ip_address* | *interface_name***}**

Syntax Definitions

ip_address	Specifies the IP address for the interface on which DVMRP is being enabled or disabled.
interface_name	The name of the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **no** form of the command to delete an interface.

Examples

```
-> ip dvmrp interface 172.22.2.115
-> ip dvmrp interface vlan-10
-> no ip dvmrp interface 172.22.2.115
-> no ip dvmrp interface vlan-10
```

Release History

Release 5.1; command was introduced.
Release 5.1.6; *interface_name* parameter added.

Related Commands

ip dvmrp status	Globally enables or disables DVMRP on the switch.
ip dvmrp interface metric	Configures the distance metric for an interface, which is used to calculate distance vectors.
show ip dvmrp interface	Displays information for all multicast-capable interfaces.

MIB Objects

```
dvmrpInterfaceTable
   dvmrpInterfaceLocalAddress
   dvmrpInterfaceStatus
```

ip dvmrp interface metric

Configures the distance metric for an interface, which is used to calculate distance vectors. DVMRP uses the distance metric value to determine the most cost-effective way to pass data through the network.

ip dvmrp interface {*ip_address* | *interface_name***} metric** *value*

Syntax Definitions

ip_address	Specifies the IP address of the interface on which the distance metric is being defined.
interface_name	The name of the interface.
value	Specifies the metric value (1–31).

Defaults

parameter	default
value	1

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

DVMRP uses the distance metric value to determine the most cost-effective way to pass data through the network. The higher the distance metric value, the higher the cost.

Examples

```
-> ip dvmrp interface 172.22.2.115 metric 1
-> ip dvmrp interface vlan-2 metric 1
```

Release History

Release 5.1; command was introduced.
Release 5.1.6; *interface_name* parameter was added.

Related Commands

ip dvmrp interface	Enables or disables DVMRP on a specified interface.
show ip dvmrp interface	Displays the DVMRP interface table.

MIB Objects

```
dvmrpInterfaceTable
   dvmrpInterfaceLocalAddress
   dvmrpInterfaceMetric
```

ip dvmrp neighbor-interval

Configures the neighbor probe interval time. The neighbor probe interval time specifies how often probes are transmitted on DVMRP-enabled interfaces.

ip dvmrp neighbor-interval *seconds*

Syntax Definitions

seconds	Specifies the probe interval time, in seconds (5–30).

Defaults

parameter	default
seconds	10

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> ip dvmrp neighbor-interval 10
```

Release History

Release 5.1; command was introduced.

Related Commands

ip dvmrp neighbor-timeout	Configures the neighbor timeout.
show ip dvmrp neighbor	Displays the DVMRP neighbor table.
show ip dvmrp	Displays the global DVMRP parameters.

MIB Objects

```
alaDvmrpGlobalConfig
   alaDvmrpNeighborProbeInterval
```

ip dvmrp neighbor-timeout

Configures the neighbor timeout. This value specifies how long the switch will wait for activity from a neighboring DVMRP router before assuming the inactive router is down.

ip dvmrp neighbor-timeout *seconds*

Syntax Definitions

seconds	Specifies the neighbor timeout, in seconds (5–86400).

Defaults

parameter	default
seconds	35

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> ip dvmrp neighbor-timeout 35
```

Release History

Release 5.1; command was introduced.

Related Commands

ip dvmrp neighbor-interval	Configures the neighbor probe interval time.
show ip dvmrp neighbor	Displays the DVMRP neighbor table.
show ip dvmrp	Displays the global DVMRP parameters.

MIB Objects

```
alaDvmrpGlobalConfig
   alaDvmrpNeighborTimeout
```

ip dvmrp prune-lifetime

Indicates the length of time a prune will be in effect (i.e., its *lifetime)*. When the prune lifetime expires, the interface rejoins the multicast delivery tree. If unwanted multicast datagrams continue to arrive, the prune mechanism will be re-initiated and the cycle will continue.

ip dvmrp prune-lifetime *seconds*

Syntax Definitions

seconds	Specifies the prune lifetime, in seconds (180–86400).

Defaults

parameter	default
seconds	7200

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> ip dvmrp prune-lifetime 7200
```

Release History

Release 5.1; command was introduced.

Related Commands

ip dvmrp prune-timeout	Configures the prune packet retransmission value.
show ip dvmrp prune	Displays the DVMRP prune entries, including the router's upstream prune state.
show ip dvmrp	Displays the global DVMRP parameters.

MIB Objects

```
alaDvmrpGlobalConfig
   alaDvmrpPruneLifetime
```

ip dvmrp prune-timeout

Configures the prune packet retransmission value. This value is the time duration that the routing switch will wait if it continues to receive unwanted multicast traffic before retransmitting a prune message.

ip dvmrp prune-timeout *seconds*

Syntax Definitions

seconds	Specifies retransmission time, in seconds (30–86400).

Defaults

parameter	default
seconds	30

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> ip dvmrp prune-timeout 30
```

Release History

Release 5.1; command was introduced.

Related Commands

ip dvmrp prune-lifetime	Indicates the length of time a prune will be in effect.
show ip dvmrp prune	Displays the DVMRP prune entries, including the router's upstream prune state.
show ip dvmrp	Displays the global DVMRP parameters.

MIB Objects

```
alaDvmrpGlobalConfig
   alaDvmrpPruneRetransmission
```

ip dvmrp report-interval

Configures the route report interval. This value defines how often the switch will send its complete routing table to neighboring routers running DVMRP.

ip dvmrp report-interval *seconds*

Syntax Definitions

seconds	Specifies the report interval, in seconds (10–2000).

Defaults

parameter	default
seconds	60

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> ip dvmrp report-interval 60
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip dvmrp route	Displays the DVMRP routes that are being advertised to other routers.
show ip dvmrp	Displays the global DVMRP parameters.

MIB Objects

```
alaDvmrpGlobalConfig
   alaDvmrpRouteReportInterval
```

ip dvmrp route-holddown

Configures the time during which DVMRP routes are kept in a hold-down state. A hold-down state refers to the time that a route to an inactive network continues to be advertised.

ip dvmrp route-holddown *seconds*

Syntax Definitions

seconds	Specifies the hold-down time, in seconds (1–86400).

Defaults

parameter	default
seconds	120

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> ip dvmrp route-holddown 120
```

Release History

Release 5.1; command was introduced.

Related Commands

ip dvmrp route-timeout	Configures the route expiration timeout value.
show ip dvmrp	Displays the global DVMRP parameters.
show ip dvmrp route	Displays the DVMRP routes that are being advertised to other routers.

MIB Objects

```
alaDvmrpGlobalConfig
   alaDvmrpRouteHoldDown
```

ip dvmrp route-timeout

Configures the route expiration timeout value. The route expiration timeout value specifies how long the switch will wait before aging out a route. When the route expiration timeout expires, the route is advertised as being in hold-down until either its activity resumes or it is deleted from the route table.

ip dvmrp route-timeout *seconds*

Syntax Definitions

seconds	Specifies the timeout value, in seconds (20–4000).

Defaults

parameter	default
seconds	140

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> ip dvmrp route-timeout 140
```

Release History

Release 5.1; command was introduced.

Related Commands

ip dvmrp route-holddown	Configures the time during which DVMRP routes are kept in a hold-down state.
show ip dvmrp	Displays the global DVMRP parameters.

MIB Objects

```
alaDvmrpGlobalConfig
   alaDvmrpRouteExpirationTimeout
```

ip dvmrp subord-default

Changes the initial default assumption on a neighbor's subordinate or non-subordinate status. When the status value is true, DVMRP neighbors are assumed to be subordinate and traffic is automatically forwarded to the neighbor upon initial discovery. When the value is false, traffic is not forwarded to the neighbor until route reports have been exchanged and the neighbor has explicitly expressed dependency.

ip dvmrp subord-default {true | false}

Syntax Definitions

true	DVMRP neighbors are assumed subordinate; traffic is automatically forwarded to the neighbor on initial discovery.
false	DVMRP neighbors are *not* assumed to be subordinate; traffic is not forwarded until route reports have been exchanged and the neighbor has explicitly expressed dependency.

Defaults

parameter	default
true | false	**true**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- However, if neighbors in the DVMRP domain have difficulty handling large initial bursts of traffic, it is recommended that the neighbor's default status as a suboridinate be changed to false.
- To view the current subordinate neighbor status, use the **show ip dvmrp** command. For more information, refer to page 33-25.

Examples

```
-> ip dvmrp subord-default false
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip dvmrp	Displays the global DVMRP parameters.

MIB Objects

```
alaDvmrpGlobalConfig
   alaDvmrpInitNbrAsSubord
```

ip dvmrp tunnel

Adds or deletes a DVMRP tunnel.

ip dvmrp tunnel {*local_address* **|** *local_name***} {***remote_address* **|** *remote_name***}**

no ip dvmrp tunnel {*local_address* **|** *local_name***} {***remote_address* **|** *remote_name***}**

Syntax Definitions

local_address	The 32-bit IP address of the local router interface. The local router interface IP address serves as an identifier for the local end of the DVMRP tunnel.
remote_address	The 32-bit IP address of the remote router interface. The remote router interface IP address serves as an identifier for the remote end of the DVMRP tunnel.
local_name	The name of the local router interface.
remote_name	The name of the remote router interface.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The local IP address of the tunnel must match the IP address of an existing DVMRP interface.
- Routing (via RIP, OSPF, etc.) must first be set up in order for the remote tunnel endpoint to be accessible.
- Use the **no** form of the command to delete a tunnel.

Examples

```
-> ip dvmrp tunnel 172.22.2.115 168.22.2.120
-> ip dvmrp tunnel vlan-2 vlan-10
-> ip dvmrp tunnel vlan-2 168.22.2.120
-> ip dvmrp tunnel 172.22.2.115 vlan-10
-> no ip dvmrp tunnel 172.22.2.115 168.22.2.120
-> no ip dvmrp tunnel vlan-2 vlan-10
-> no ip dvmrp tunnel vlan-2 168.22.2.120
-> no ip dvmrp tunnel 172.22.2.115 vlan-10
```

Release History

Release 5.1; command was introduced.
Release 5.1.6; *local_name* and *remote_name* parameters were added.

Related Commands

ip dvmrp tunnel ttl	Configures the TTL value for the tunnel defined for the specified local address and remote address.
show ip dvmrp interface	Displays the DVMRP interface table.
show ip dvmrp tunnel	Displays the DVMRP tunnel entries.

MIB Objects

```
tunnelConfigTable
   tunnelConfigLocalAddress
   tunnelConfigRemoteAddress
   tunnelConfigStatus
```

ip dvmrp tunnel ttl

Configures the TTL value for the tunnel defined for the specified local address and remote address. The TTL value is added to the TTL field of the IP header for outgoing packets destined for the remote tunnel endpoint.

ip dvmrp tunnel {*local_address remote_address* **|** *interface_name***} ttl** *value*

Syntax Definitions

local_address	Local IP address of the tunnel.
remote_address	Remote IP address of the tunnel.
interface_name	The name of the interface.
value	The Time to Live (TTL) value (0–255).

Defaults

parameter	default
value	255

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The local IP address of the tunnel must match the IP address of an existing DVMRP tunnel.
- A value of 0 indicates that the value is copied from the payload's header.

Example

```
-> ip dvmrp tunnel 172.22.2.115 172.22.2.120 ttl 0
-> ip dvmrp tunnel vlan-2 ttl 0
```

Release History

Release 5.1; command was introduced.
Release 5.1.6; *interface_name* parameter was added.

Related Commands

ip dvmrp tunnel	Adds or deletes a DVMRP tunnel for the specified local and remote addresses.
show ip dvmrp tunnel	Displays the DVMRP tunnel entries.

MIB Objects

```
tunnelIfTable
   tunnelIfLocalAddress
   tunnelIfRemoteAddress
   tunnelIfHopLimit
```

ip dvmrp debug-level

Defines the level of debugging for DVMRP in the switch.

ip dvmrp debug-level *level*

Syntax Definitions

level	Specifies the DVMRP debug level (0–255). Higher debug-levels will include all messages that correspond to a lower value. For example, a debug level of 2 will display all messages for level 1 and level 2. As a rule of thumb, higher levels will display more detailed messages, while lower levels will display more basic messages.

Defaults

parameter	default
level	1

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

When the debug level is set to 0, DVMRP debug logging is turned off.

Examples

```
-> ip dvmrp debug-level 2
```

Release History

Release 5.1; command was introduced.

Related Commands

ip dvmrp debug-type	Enables or disables DVMRP debugging for a specified message type, or for all message types.
show ip dvmrp debug	Displays the current level of debugging for DVMRP in the switch, as well as the current status for all debugging types.

MIB Objects

```
alaDvmrpDebugConfig
   alaDvmrpDebugLevel
```

ip dvmrp debug-type

Enables or disables DVMRP debugging for a specified message type, or for all message types.

Note. Debugging for a specified message type will only be enabled if its debug level is a value greater than zero (i.e., 1–255). For information on specifying the debug level, refer to the **ip dvmrp debug-level** command on page 33-22.

ip dvmrp debug-type *message_type*

no ip dvmrp debug-type *message_type*

Syntax Definitions

message_type Enables or disables DVMRP debugging for the specified item. Select from the list below. You may enter multiple message types in any order. For example, **ip dvmrp debug-type time flash init**.

supported message types	descriptions
all	Enables or disables DVMRP debugging for all items listed below. The syntax **all** can be used to easily turn debugging for all message types on or off.
error	Enables or disables debugging for DVMRP Error messages.
flash	Enables or disables debugging for DVMRP Flash processing.
graft	Enables or disables debugging for DVMRP Graft processing.
igmp	Enables or disables debugging for DVMRP Internet Group Management Protocol (IGMP) packet processing.
ipmrm	Enables or disables debugging for DVMRP IP Multicast Routing Manager (IPMRM) interaction.
init	Enables or disables debugging related to DVMRP initialization code.
mip	Enables or disables debugging for MIP (Management Internal Protocol) processing. Includes CLI and SNMP.
misc	Enables or disables miscellaneous debugging of DVMRP.
nbr	Enables or disables debugging for DVMRP Neighbor processing.
probes	Enables or disables debugging for DVMRP Probe processing.
prunes	Enables or disables debugging for DVMRP Prune processing.
routes	Enables or disables debugging for DVMRP Route processing.
time	Enables or disables debugging for DVMRP Timer processing.
tm	Enables or disables debugging for DVMRP Task Manager interaction.

Defaults

parameter	default
message_type	error

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to disable debugging for the specified item.
- Reminder: Debugging for a specified message type will only be enabled if its debug level is a value greater than zero (i.e., 1–255). For information on specifying the debug level, refer to the **ip dvmrp debug-level** command on page 33-22.
- The syntax **all** can be used to easily turn debugging for all message types on or off (e.g., **ip dvmrp debug-type all** or **no ip dvmrp debug-type all**).

Examples

```
-> ip dvmrp debug-type all
-> ip dvmrp debug-type tm igmp flash
-> no ip dvmrp debug-type misc
-> no ip dvmrp debug-type all
```

Release History

Release 5.1; command was introduced.

Related Commands

ip dvmrp debug-level	Defines the level of debugging for DVMRP in the switch.
show ip dvmrp debug	Displays the current level of debugging for DVMRP in the switch, as well as the current status for all debugging types.

MIB Objects

```
alaDvmrpDebugConfig
   alaDvmrpDebugAll
   alaDvmrpDebugError
   alaDvmrpDebugFlash
   alaDvmrpDebugGrafts
   alaDvmrpDebugIgmp
   alaDvmrpDebugInit
   alaDvmrpDebugIpmrm
   alaDvmrpDebugMip
   alaDvmrpDebugNbr
   alaDvmrpDebugProbes
   alaDvmrpDebugPrunes
   alaDvmrpDebugRoutes
   alaDvmrpDebugTime
   alaDvmrpDebugTm
```

show ip dvmrp

Displays the global DVMRP parameters.

show ip dvmrp

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

On OmniSwitch 7700, 7800, and 8800 switches:

```
-> show ip dvmrp

DVMRP Admin Status = enabled,
Flash Interval     = 5,
Graft Timeout      = 5,
Neighbor Interval  = 10,
Neighbor Timeout   = 35,
Prune Lifetime     = 7200,
Prune Timeout      = 30,
Report Interval    = 60,
Route Holddown     = 120,
Route Timeout      = 140,
Subord Default     = true,

Number of Routes           = 2,
Number of Reachable Routes = 2
```

On OmniSwitch 6600 Family switches:

```
-> show ip dvmrp

DVMRP Admin Status = enabled (safe mode),
Flash Interval     = 5,
Graft Timeout      = 5,
Neighbor Interval  = 10,
Neighbor Timeout   = 35,
Prune Lifetime     = 7200,
Prune Timeout      = 30,
Report Interval    = 60,
Route Holddown     = 120,
Route Timeout      = 140,
Subord Default     = true,

Number of Routes           = 2,
Number of Reachable Routes = 2
```

output definitions

DVMRP Admin Status	The current global (i.e., switch-wide) status of DVMRP, which can be **enabled** or **disabled**. On OmniSwitch 6600 Family switches only this field displays the operational mode also, which can be either **safe mode** or **unrestricted mode**. To change the current DVMRP global status, refer to the **ip dvmrp status** command on page 33-3.
Flash Interval	The current minimum flash update interval value, in seconds. The flash interval defines how often routing table change messages are sent to neighboring DVMRP routers. Because routing table change messages are sent between the transmission of complete routing tables, the flash update interval must be shorter than the route report interval. The default value is 5.
Graft Timeout	The graft message retransmission value, in seconds. The graft message retransmission value defines the duration of time that the routing switch will wait before retransmitting a graft message if it has not received an acknowledgement from its neighbor. Values may range from 5–86400. The default value is 5.
Neighbor Interval	The current neighbor probe interval time, in seconds. The neighbor probe interval time specifies how often probes are transmitted to interfaces with attached DVMRP neighbors. Values may range from 5–30. The default value is 10.
Neighbor Timeout	The current neighbor timeout value, in seconds. This value specifies how long the routing switch will wait for activity from a neighboring DVMRP router before assuming the inactive router is down. Values may range from 5–86400. The default value is 35.
Prune Lifetime	The length of time, in seconds, a prune will be in effect. When the prune lifetime expires, the interface is joined back onto the multicast delivery tree. If unwanted multicast datagrams continue to arrive, the prune mechanism will be re-initiated and the cycle will continue. Values may range from 180–86400. The default value is 7200.
Prune Timeout	The current prune packet retransmission value, in seconds. This value indicates the duration of time that the routing switch will wait if it continues to receive unwanted multicast traffic before retransmitting a prune message. Values range from 30–86400. The default value is 30.

output definitions (continued)

Report Interval	The current route report interval, in seconds. The route report interval defines how often routers will send their complete routing tables to neighboring routers running DVMRP. Values may range from 10–2000. The default value is 60.
Route Holddown	The current hold-down time, in seconds. This value indicates the time during which DVMRP routes are kept in a hold-down state. A hold-down state refers to the time that a route to an inactive network continues to be advertised. Values may range from 1–120. The default value is 120.
Route Timeout	The current route expiration timeout value, in seconds. The route expiration timeout value specifies how long the routing switch will wait before aging out a route. Values may range from 20–4000. The default value is 140.
Subord Default	Displays the initial default assumption on a neighbor's subordinate or non-subordinate status. When the status value is true, DVMRP neighbors are assumed to be subordinate and traffic is automatically forwarded to the neighbor upon initial discovery. When the value is false, traffic is not forwarded to the neighbor until route reports have been exchanged and the neighbor has explicitly expressed dependency. To change the current subordinate neighbor status, refer to the **ip dvmrp subord-default** command on page 33-16. Options include true and false. The default value is true.
Number of Routes	The number of entries in the routing table. This number can be used to monitor the routing table size and detect illegal advertisements of unicast routes.
Number of Reachable Routes	The total number of reachable routes. The number of entries in the routing table with non-infinite metrics. This number can be used to detect network partitions by observing the ratio of reachable routes to total routes. Routes with unreachable metrics, routes in a hold-down state, and routes that have aged out are not considered reachable.

Release History

Release 5.1; command was introduced.

Related Commands

ip dvmrp status	Globally enables or disables DVMRP in the switch.
ip dvmrp flash-interval	Configures the minimum flash update interval value.
ip dvmrp graft-timeout	Configures the graft message retransmission value.
ip dvmrp neighbor-timeout	Configures the neighbor timeout.
ip dvmrp prune-lifetime	Indicates the length of time a prune will be in effect.
ip dvmrp prune-timeout	Configures the prune packet retransmission value.
ip dvmrp report-interval	Configures the route report interval.
ip dvmrp route-holddown	Configures the time during which DVMRP routes are kept in a hold-down state.
ip dvmrp route-timeout	Configures the route expiration timeout value.
ip dvmrp subord-default	Configures the neighbor probe interval time.

MIB Objects

```
alaDvmrpConfigMIBGroup
   alaDvmrpAdminStatus
   alaDvmrpRouteReportInterval
   alaDvmrpFlashUpdateInterval
   alaDvmrpNeighborTimeout
   alaDvmrpRouteExpirationTimeout
   alaDvmrpRouteHoldDown
   alaDvmrpNeighborProbeInterval
   alaDvmrpPruneLifetime
   alaDvmrpPruneRetransmission
   alaDvmrpGraftRetransmission
   alaDvmrpInitNbrAsSubord
dvmrpGeneralGroup
   dvmrpNumRoutes
   dvmrpReachableRoutes
```

show ip dvmrp interface

Displays information for all multicast-capable interfaces *or* for a specified interface. This command provides options to display only DVMRP-enabled or DVMRP-disabled interfaces also.

show ip dvmrp interface [{*ip_address* | *interface_name* **} | enabled | disabled]**

Syntax Definitions

ip_address	Specifies a particular interface IP address.
interface_name	The name of the interface.
enabled	Displays a list of all interfaces (i.e., VLAN router ports) on which DVMRP is currently *enabled*.
disabled	Displays a list of all interfaces (i.e., VLAN router ports) on which DVMRP is currently *disabled*.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If no optional syntax is specified in the command line, the entire interface table is displayed.
- For an interface to show as *enabled* in the **show ip dvmrp interface** or **show ip dvmrp interface enabled** output, the interface must be both administratively *and* operationally enabled. Although the interface does not have to be passing traffic, at least one VLAN router port must be operational on the corresponding DVMRP-enabled VLAN.
- To view the Generation ID being used on a particular interface, you must include the interface IP address in the command line.

Examples

The following are sample displays for OmniSwitch 6600, 7700, 7800, and 8800 switches:

```
-> show ip dvmrp interface
 Interface Name       Vlan   Metric  Admin-Status  Oper-Status
--------------------+-----+--------+-------------+-------------
 vlan-1                 1      1      Disabled     Disabled
 vlan-2                 2      1      Enabled      Enabled
-> show ip dvmrp interface enabled
 Interface Name       Vlan   Metric  Admin-Status  Oper-Status
--------------------+-----+--------+-------------+-------------
 vlan-2                 2      1      Enabled      Enabled
```

output definitions

Interface Name	The name of the interface. This field is displayed on OmniSwitch 7700, 7800, and 8800 switches only.
Vlan	The associated VLAN ID.
Metric	The current metric value. A metric is essentially used to determine the most cost-effective way to pass data through the network. The higher the metric value, the higher the cost.
Admin-Status	The current administrative status of the corresponding interface. Options include **Enabled** or **Disabled**. An interface can be configured for DVMRP without being operational. To change the DVMRP Admin-status for an individual interface, refer to the **ip dvmrp interface** command on page 33-7.
Oper-Status	The current operational status of the corresponding multicast-capable interface. Options include **Enabled** or **Disabled**. For an interface to be DVMRP-operational, the global DVMRP status must be enabled and the individual interface must be DVMRP-enabled. To change the global DVMRP status, refer to the **ip dvmrp status** command on page 33-3.

Release History

Release 5.1; command was introduced.
Release 5.3.1; **Tunnel** field was deleted.
Release 5.1.6; **Interface Name** field was added.

Related Commands

ip dvmrp interface	Enables or disables DVMRP on a specified interface.

MIB Objects

```
dvmrpInterfaceGroup
   dvmrpInterfaceLocalAddress
   dvmrpInterfaceMetric
   dvmrpInterfaceStatus
```

show ip dvmrp neighbor

Displays the DVMRP neighbor table. The DVMRP neighbor table displays either all neighboring DVMRP routers or a specified neighboring DVMRP router.

show ip dvmrp neighbor [*ip_address***]**

Syntax Definitions

ip_address	Specifies a particular IP address for a neighboring DVMRP router.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

If a neighbor IP address is not specified, the entire DVMRP Neighbor table is displayed.

Examples

The following is a sample display for OmniSwitch 6600, 7700, 7800, and 8800 switches:

```
-> show ip dvmrp neighbor

Neighbor Address   Intf Name     Uptime      Expires     GenID     Vers  State
---------------+-------------+-----------+-----------+----------+------+-------
143.209.92.214      vlan-2     00h:09m:12s  00h:00m:06s 546947509  3.255 active
```

output definitions

Neighbor Address	The 32-bit IP address of the DVMRP neighbor's router interface.
Itnf Name	The interface name of the neighbor's router.
Uptime	The amount of time the neighbor has been running, displayed in hours, minutes, and seconds.
Expires	The amount of time remaining before the neighbor expires, displayed in hours, minutes, and seconds.
GenID	The generation ID for the DVMRP neighbor. This value is used by neighboring routers to detect whether the DVMRP routing table should be resent.
Version	The DVMRP version number for the neighbor.
State	The current state of the DVMRP neighbor. Options include **active** and **down**.

Release History

Release 5.1; command was introduced.
Release 5.1.6; **Intf Name** field was added.

Related Commands

ip dvmrp neighbor-interval	Configures the neighbor probe interval time.
ip dvmrp neighbor-timeout	Configures the neighbor timeout.

MIB Objects

```
dvmrpNeighborTable
   dvmrpNeighborAddress
   dvmrpNeighborIfIndex
   dvmrpNeighborUpTime
   dvmrpNeighborExpiryTime
   dvmrpNeighborGenerationId
   dvmrpNeighborMajorVersion
   dvmrpNeighborMinorVersion
   dvmrpNeighborState
```

show ip dvmrp nexthop

Displays DVMRP next hop entries. This command is used to show the list of next hops on outgoing interfaces to which IP multicast datagrams from particular sources are routed.

show ip dvmrp nexthop [*ip_address ip_mask***]**

Syntax Definitions

ip_address	Specifies a source IP address for which DVMRP next hop entries will be displayed.
ip_mask	Specifies a source IP mask for which DVMRP next hop entries will be displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

If an IP address and IP mask are not specified, the entire DVMRP Next Hop Table is displayed.

Examples

The following is a sample display for OmniSwitch 6600, 7700, 7800, and 8800 switches:

```
-> show ip dvmrp nexthop 172.22.2.115 255.255.255.0
Src Address/Mask       Interface Name     Vlan    Hop Type
-------------------+-------------------+-------+----------
143.209.92.0/24           vlan-2            2      branch
```

output definitions

Address/Mask	The 32-bit source IP address, along with the mask length, shown in bits. The source IP address and mask are separated by a slash (/).
Interface Name	The name of the interface.
Vlan	The associated VLAN ID.
Hop Type	The hop type of the associated entry. Options include **leaf** or **branch**. If the next hop VLAN has a DVMRP neighbor attached to it, the hop type will be displayed as **branch**.

Release History

Release 5.1; command was introduced.
Release 5.1.6; **Interface Name** field was added.

Related Commands

N/A

MIB Objects

```
dvmrpRouteNextHopTable
   dvmrpRouteNextHopSource
   dvmrpRouteNextHopSourceMask
   dvmrpRouteNextHopIfIndex
   dvmrpRouteNextHopType
```

show ip dvmrp prune

Displays DVMRP prune entries that have been sent upstream.

show ip dvmrp prune [*group_address source_address source_mask***]**

Syntax Definitions

group_address	Specifies a pruned group address.
source_address	Specifies a source IP address.
source_mask	Specifies a source IP mask.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

If a group address, source address, and source mask are not specified, the entire Prune table is displayed.

Examples

```
-> show ip dvmrp prune

Group Address     Source Address/Mask    Expires
----------------+--------------------+-------------
224.0.0.4           143.209.92.14/24    00h:00m:30s
```

output definitions

Group Address	The 32-bit multicast group address.
Source Address/Mask	The 32-bit source IP address, along with the mask length, shown in bits. The source IP address and mask are separated by a slash (/).
Expires	The amount of time remaining before the current prune state expires, displayed in hours, minutes, and seconds.

Release History

Release 5.1; command was introduced.

Related Commands

ip dvmrp prune-lifetime	Indicates the length of time a prune will be in effect.
ip dvmrp prune-timeout	Configures the prune packet retransmission value.

MIB Objects

```
dvmrpPruneTable
   dvmrpPruneGroup
   dvmrpPruneSource
   dvmrpPruneSourceMask
   dvmrpPruneExpiryTime
```

show ip dvmrp route

Displays the DVMRP routes that are being advertised to other routers.

show ip dvmrp route [*ip_address ip_mask***]**

Syntax Definitions

ip_address	The 32-bit source IP address for a DVMRP-enabled router interface.
ip_mask	A 32-bit number that determines the subnet mask for the IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

If a source IP address and IP mask are not specified, the entire DVMRP route table is displayed.

Examples

```
-> show ip dvmrp route
Legends:  Flags:  L = Local, R = Remote, F = Flash, H = Holddown, I = Invalid
     Address/Mask        Gateway       Metric     Age      Expires  Flags
------------------+-----------------+------+-----------+---------+-----
       11.0.0.0/8     55.0.0.5           2    00h:13m:14s  02m:07s    R
       22.0.0.0/8     44.0.0.4           2    00h:33m:14s  02m:15s    R
       44.0.0.0/8           -            1    05h:24m:59s     -       L
       55.0.0.0/8           -            1    05h:24m:59s     -       L
       66.0.0.0/8     44.0.0.4           2    00h:03m:11s  02m:15s    R
```

output definitions

Address/Mask	The 32-bit IP address for the router interface, along with the corresponding subnet mask. The interface's subnet mask is shown using the CIDR prefix length: 255.0.0.0 equals /8; 255.255.0.0 equals /16; 255.255.255.0 equals /24, etc.
Gateway	The corresponding 32-bit gateway address. Because it is not applicable, no gateway address is displayed for local routes.
Metric	The current metric value. A metric is essentially used to determine the most cost-effective way to pass data through the network. The higher the metric value, the higher the cost.
Age	The current age of the DVMRP route, displayed in hours, minutes, and seconds.

output definitions (continued)

Expires	The expiration time for the corresponding route. Because it is not applicable, no expiration time is displayed for local routes.
Flags	The flag type of a particular DVMRP route. Options include **L** (Local), **R** (Remote), **F** (Flash), **H** (Holddown), and **I** (Invalid).

Release History

Release 5.1; command was introduced.

Related Commands

ip dvmrp report-interval	Configures the route report interval.
ip dvmrp route-holddown	Configures the time during which DVMRP routes are kept in a hold-down state.
ip dvmrp route-timeout	Configures the route expiration timeout value.

MIB Objects

```
dvmrpRouteTable
   dvmrpRouteSource
   dvmrpRouteSourceMask
   dvmrpRouteMetric
   dvmrpRouteExpiryTime
   dvmrpRouteUpTime
```

show ip dvmrp tunnel

Displays DVMRP tunnel entries.

show ip dvmrp tunnel [*local_address remote_address***]**

Syntax Definitions

local_address	The IP address of a particular local router interface. The local router interface IP address is an identifier for the local end of the DVMRP tunnel.
remote_mask	The IP address of a particular remote router interface. The remote router interface IP address is an identifier for the remote end of the DVMRP tunnel.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If optional local and remote IP address information is not specified, the entire DVMRP Tunnels table is displayed.
- The local IP address of the tunnel must match the IP address of an existing DVMRP-enabled IP interface.

Examples

The following is a sample display for OmniSwitch 6600, 7700, 7800, and 8800 switches:

```
-> show ip dvmrp tunnel
Interface Name       Local Address     Remote Address    TTL    Status
-------------------+-----------------+-----------------+-----+----------
vlan-2               143.209.92.203      12.0.0.1        255   Enabled
```

output definitions

Interface Name	The interface name.
Local Address	The 32-bit local IP address for the DVMRP tunnel.
Remote Address	The 32-bit remote IP address for the DVMRP tunnel.

output definitions (continued)

TTL	The current Time to Live (TTL) value. A value of 0 indicates that the value is copied from the payload's header. Values may range from 0–255.
Status	The corresponding interface status. Options include **Enabled** or **Disabled**. If the interface specified by the local address has been configured and is operationally enabled, the status is **Enabled**. If the interface is down, the value displayed is **Disabled**.

Release History

Release 5.1; command was introduced.
Release 5.1.6; **Interface Name** field was added.

Related Commands

ip dvmrp tunnel	Adds or deletes a DVMRP tunnel.
ip dvmrp tunnel ttl	Configures the TTL value for the tunnel defined for the specified local address and remote address.

MIB Objects

```
tunnelIfTable
   tunnelIfLocalAddress
   tunnelIfRemoteAddress
   tunnelIfHopLimit
dvmrpInterfaceGroup
   dvmrpInterfaceStatus
```

show ip dvmrp debug

Displays the current level of debugging for DVMRP in the switch, as well as the current status for all debugging types.

show ip dvmrp debug

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The administrative debugging status for message types displayed in the table are determined by the **ip dvmrp debug-type** command on page 33-23.
- To configure debug levels, refer to the **ip dvmrp debug-level** command on page 33-22.

Examples

```
-> show ip dvmrp debug

Debug Level = 1,
Error       = on,
Flash       = off,
Grafts      = off,
IGMP        = off,
IPMRM       = off,
Init        = off,
MIP         = off,
Misc        = off
Nbr         = on,
Probes      = off,
Prunes      = off,
Routes      = on,
Time        = off,
TM          = off,
```

output definitions

Debug Level	The current debug level value. For information on setting this parameter, see the **ip dvmrp debug-level** command on page 33-22.
error	The current debugging status for DVMRP Error messages. Options include **on** or **off**.
Flash	The current debugging status for DVMRP Flash processing. Options include **on** or **off**.

output definitions (continued)

Grafts	The current debugging status for DVMRP Graft processing. Options include **on** or **off**.
IGMP	The current debugging status for DVMRP Internet Group Management Protocol (IGMP) packet processing. Options include **on** or **off**.
IPMRM	The current debugging status for DVMRP IP Multicast Routing Manager (IPMRM) interaction. Options include **on** or **off**.
Init	The current debugging status for DVMRP Initialization. Options include **on** or **off**.
MIP	The current debugging status for DVMRP MIP (Management Internal Protocol) processing. Includes CLI and SNMP. Options include **on** or **off**.
Misc	The current status of miscellaneous DVMRP debugging. Options include **on** or **off**.
Nbr	The current debugging status for DVMRP Neighbor processing. Options include **on** or **off**.
Probes	The current debugging status for DVMRP Probe processing. Options include **on** or **off**.
Prunes	The current debugging status for DVMRP Prune processing. Options include **on** or **off**.
Routes	The current debugging status for DVMRP Route processing. Options include **on** or **off**.
Time	The current debugging status for DVMRP Timer processing. Options include **on** or **off**.
TM	The current debugging status for DVMRP Task Manager interaction. Options include **on** or **off**.

Release History

Release 5.1; command was introduced.

Related Commands

ip dvmrp debug-level	Defines the level of debugging for DVMRP in the switch.
ip dvmrp debug-type	Enables or disables DVMRP debugging for a specified message type, or for all message types.

MIB Objects

```
alaDvmrpDebugMIBGroup
   alaDvmrpDebugLevel
   alaDvmrpDebugError
   alaDvmrpDebugFlash
   alaDvmrpDebugGrafts
   alaDvmrpDebugIgmp
   alaDvmrpDebugIpmrm
   alaDvmrpDebugInit
   alaDvmrpDebugMip
   alaDvmrpDebugMisc
   alaDvmrpDebugNbr
   alaDvmrpDebugProbes
   alaDvmrpDebugPrunes
   alaDvmrpDebugRoutes
   alaDvmrpDebugTime
   alaDvmrpDebugTm
```

34 Multicast Routing Commands

This chapter describes multicast routing commands. Multicast routing is used in conjunction with IP Multicast Switching (IPMS). IPMS can operate either with or without multicast routing. However, for Multicast Routing to function, IPMS must be configured.

Multicast uses Class D IP addresses in the range 224.0.0.0 to 239.255.255.255. Addresses in the range 239.0.0.0 to 239.255.255.255 are reserved for boundaries, which are used to prevent multicast traffic from being forwarded on a VLAN group or network.

IP multicast routing is a way of controlling multicast traffic across networks. The multicast router discovers which networks want to receive multicast traffic by sending out Internet Group Management Protocol (IGMP) queries and receiving IGMP reports from attached networks. The IGMP reports signal that users want to join or leave a multicast group. If there is more than one multicast router in the network, the router with the lowest IP address is elected the querier router, which is responsible for querying the subnetwork for group members.

MIB information for the multicast routing commands is as follows:

Filename: AlcatelIND1Ipmrm.mib
Module: ALCATEL-IND1-IPMRM-MIB

Filename: IETF_IPMROUTE_STD.mib
Module: IPMROUTE-STD-MIB

A summary of the available commands is listed here:

ip mroute-boundary
ip mroute interface ttl
show ip mroute-boundary
show ip mroute
show ip mroute interface
show ip mroute-nexthop
ip mroute debug-level
ip mroute debug-type
show ip mroute debug

ip mroute-boundary

Adds or deletes scoped multicast address boundaries for a router interface. When a user on the specified interface joins the multicast group as defined by the scoped address—plus the mask length—all multicast traffic will stop being forwarded on that interface. This provides a mechanism for the end user to control multicast traffic from the network.

Refer to the "Configuring Multicast Address Boundaries" chapter in the applicable *OmniSwitch Advanced Routing Guide* for detailed information.

ip mroute-boundary *ip_address scoped_address mask*

no ip mroute-boundary *ip_address scoped_address mask*

Syntax Definitions

ip_address	The IP address of the interface (i.e., router port) on which the boundary is being assigned.
scoped_address	A scoped multicast address identifying the group range for the boundary. Scoped addresses may range from 239.0.0.0–239.255.255.255.
mask	A corresponding Class A, B, or C mask address (e.g., 255.0.0.0).

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> ip mroute-boundary 168.10.1.1 239.0.0.0 255.0.0.0
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip mroute-boundary	Displays scoped multicast address boundaries for the switch's router interfaces

MIB Objects

```
IpMRouteBoundaryTable
   ipMRouteBoundaryIfIndex
   ipMRouteBoundaryAddress
   ipMRouteBoundaryAddressMask
   ipMRouteBoundaryStatus
```

ip mroute interface ttl

Specifies a multicast datagram Time to Live (TTL) threshold for an existing router interface. IP multicast datagrams with a TTL value lower than the specified TTL threshold value will not be forwarded out the interface.

ip mroute interface *ip_address* **ttl** *threshold*

Syntax Definitions

ip_address	The IP address of an interface (i.e., router port) that has one of the Multicast routing protocols running (either DVMRP or PIM-SM).
threshold	The TTL threshold value. Values may range from 0–255. The default value of 0 allows all multicast packets to be forwarded out the interface.

Defaults

parameter	default
threshold	0

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> ip mroute interface 168.10.1.1 ttl 255
```

Release History

Release 5.1; command was introduced.

Related Commands

N/A

MIB Objects

```
IpMRouteInterfaceTable
   ipMRouteInterfaceIfIndex
   ipMRouteInterfaceTtl
```

show ip mroute-boundary

Displays scoped multicast address boundaries for the switch's router interfaces.

show ip mroute-boundary

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show ip mroute-boundary
ifIndex  Vlan     Boundary Address
--------+--------+------------------
13600002 2        239.0.0.0/8
```

output definitions

ifIndex	The ifIndex value for the interface on which the boundary is assigned. This field applies to SNMP MIB information only. Packets with a destination address in the associated address/mask range will not be forwarded from this interface.
Vlan	The VLAN on which the interface (router port) is configured.
Boundary Address	The scoped multicast address that, when combined with the boundary mask, identifies the scoped boundary range. The boundary's subnet mask is shown using the CIDR prefix length: 255.0.0.0 equals /8; 255.255.0.0 equals /16; 255.255.255.0 equals /24.

Release History

Release 5.1; command was introduced.

Related Commands

ip mroute-boundary	Adds or deletes a router's scoped multicast address boundaries.

MIB Objects

```
IpMRouteBoundaryTable
   ipMRouteBoundaryIfIndex
   ipMRouteBoundaryAddress
   ipMRouteBoundaryAddressMask
   ipMRouteBoundaryStatus
```

show ip mroute

Displays multicast routing information for IP datagrams sent by particular sources to the IP multicast groups known to this router.

show ip mroute

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show ip mroute

Group Address   Src Address        Upstream Nbr    Route Addr       Proto
--------------+------------------+--------------+----------------+------
224.16.16.16    143.209.92.12/32   0.0.0.0         143.209.92.12    PIM
224.20.20.0     143.209.92.12/32   0.0.0.0         143.209.92.12    PIM
```

output definitions

Group Address	The IP multicast group address for this entry.
Src Address	The network address which identifies the source for this entry.
Upstream Nbr	The address of the upstream neighbor from which IP datagrams from these sources to this multicast address are received.
Route Addr	The address portion of the route used to find the upstream or parent interface for this multicast forwarding entry.
Proto	The multicast routing protocol through which this multicast forwarding entry was learned (i.e., DVMRP or PIM).

Release History

Release 5.1; command was introduced.

Related Commands

N/A

MIB Objects

```
ipMRouteTable
   ipMRouteGroup
   ipMRouteSource
   ipMRouteSourceMask
   ipMRouteUpstreamNeighbor
   ipMRouteProtocol
   ipMRouteRtAddress
```

show ip mroute interface

Displays IP multicast interface information.

show ip mroute interface

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show ip mroute interface

Vlan     IP Address      TTL      Multicast Protocol
--------+---------------+--------+------------------
1        1.1.1.1         0        PIM-SM
6        2.2.2.2         0        PIM-SM
```

output definitions

Vlan	The VLAN value of the interface for which information is being displayed.
IP Address	The IP address of this interface entry.
TTL	The datagram TTL threshold for the interface. Any IP multicast datagrams with a TTL less than the threshold displayed in the table will not be forwarded out the interface. The default value, 0, specifies that *all* multicast packets are forwarded out the interface.
Multicast Protocol	The multicast routing protocol currently running on this interface. Options include DVMRP and PIM-SM.

Release History

Release 5.1; command was introduced.

Related Commands

N/A

MIB Objects

```
ipMRouteInterfaceTable
   ipMRouteInterfaceIfIndex
   ipMRouteInterfaceTtl
   ipMRouteInterfaceProtocol
```

show ip mroute-nexthop

Displays next-hop information on outgoing interfaces for routing IP multicast datagrams.

show ip mroute-nexthop

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show ip mroute-nexthop

Group Address   Src Address        Vlan   Next Hop        State      Protocol
                                          Address
---------------+------------------+------+---------------+----------+--------
224.16.16.16    143.209.92.12/32   2      224.16.16.16    forwarding PIM
224.20.20.0     143.209.92.12/32   2      224.20.20.0     forwarding PIM
```

output definitions

Group Address	The IP multicast group address for this entry.
Src Address	The network address which identifies the source for this entry.
Vlan	The VLAN (interface) for this next-hop's outgoing interface.
Next Hop Address	The address of the next-hop that is specific to this entry.
State	The current nexthop state. The nexthop state indicates whether the outgoing interface and nexthop represented by this entry are currently being used to forward IP datagrams. Options include **forwarding** and **pruned**. The value, **forwarding**, indicates that the outgoing interface and nexthop are being used to forward IP datagrams; **pruned** indicates that the outgoing interface and nexthop are *not* being used to forward IP datagrams.
Protocol	The routing protocol by which this next-hop was learned (i.e., DVMRP or PIM).

Release History

Release 5.1; command was introduced.

Related Commands

show ip mroute	Displays multicast routing information for IP datagrams sent by particular sources to the IP multicast groups known to this router.

MIB Objects

```
ipMRouteNextHopTable
   ipMRouteNextHopGroup
   ipMRouteNextHopSource
   ipMRouteNextHopSourceMask
   ipMRouteNextHopIfIndex
   ipMRouteNextHopAddress
   ipMRouteNextHopState
   ipMRouteNextHopProtocol
```

ip mroute debug-level

Defines the level of multicast routing debug messages that are generated.

ip mroute debug-level *level*

Syntax Definitions

level	Specifies the multicast routing debug level (0–255). Higher debug-levels will include all messages that correspond to a lower value. For example, a debug-level of 1 will display only those messages that are defined with a level of 1; however, a debug level of 2 will display all messages of level 1 and level 2, etc. Higher levels will display detailed messages; lower levels will display basic messages.

Defaults

parameter	default
level	1

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

When the debug level is set to 0, debug logging for multicast routing is turned off.

Examples

```
-> ip mroute debug-level 2
```

Release History

Release 5.1; command was introduced.

Related Commands

ip mroute debug-type	Configures the type(s) of multicast routing debug messages to display.
show ip mroute debug	Displays the current multicast routing debug levels and types.

MIB Objects

```
alaIpmrmDebugConfig
   alaIpmrmDebugLevel
```

ip mroute debug-type

Configures the type(s) of multicast routing debug messages to display.

ip mroute debug-type *message_list*

no ip mroute debug-type *message_list*

Syntax Definitions

message_list	Specifies the type(s) of multicast routing debug messages to display. Select supported multicast routing message types from the list below. You may enter multiple message types in any order. For example, **ip mroute debug-type tm fib init**.

supported message types	descriptions
all	Specifies all messages. The syntax **all** can be used to easily turn on/off all message types.
aging	Specifies messages related to IPMRM FIB aging entries.
error	Specifies all error handling messages.
fib	Specifies messages related to IPMRM FIB processing.
ipms	Specifies messages related to IP Multicast Switching (IPMS) interaction.
init	Specifies messages related to initialization code.
mip	Specifies messages related to MIP (Management Internal Protocol).
misc	Specifies miscellaneous message handling.
protos	Specifies messages related to multicast routing protocols (e.g., whether they are enabled or disabled on interfaces, which protocols are going up or down, etc.).
tm	Specifies messages related to the Task Manager.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a debug message type.
- The message-types specified in the command line will only be displayed if the debug level has been set to a number greater than zero (i.e., 1–255). For information on specifying the debug level, refer to the **ip mroute debug-level** command on page 34-13.
- The syntax **all** can be used to easily turn on/off all message types (e.g., **ip mroute debug-type all** or **no ip mroute debug-type all**).

Examples

```
-> ip mroute debug-type error aging tm
-> ip mroute debug-type all
```

Release History

Release 5.1; command was introduced.

Related Commands

ip mroute debug-level	Defines the level of multicast routing debug messages that are generated.
show ip mroute debug	Displays the current multicast routing debug levels and types.

MIB Objects

```
alaIpmrmDebugConfig
   alaIpmrmDebugAll
   alaIpmrmDebugError
   alaIpmrmDebugFib
   alaIpmrmDebugAging
   alaIpmrmDebugProtos
   alaIpmrmDebugIpms
   alaIpmrmDebugMip
   alaIpmrmDebugInit
   alaIpmrmDebugTm
   alaIpmrmDebugMisc
```

show ip mroute debug

Displays the current multicast routing debug levels and types.

show ip mroute debug

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

The debug types displayed in the table are determined by the **ip mroute debug-type** command on page 34-14. To configure debug levels, refer to the **ip mroute debug-level** command on page 34-13.

Examples

```
-> show ip mroute debug
    Debug Level   = 1,
    aging         = off,
    error         = on,
    fib           = off,
    init          = off,
    ipms          = off,
    mip           = off,
    misc          = off,
    protos        = off,
    tm            = off
```

output definitions

Debug Level	The current debug level value. For information on setting this parameter, see the **ip mroute debug-level** command on page 34-13.
aging	The current state of messages related to IPMRM FIB aging entries. Options include on or off.
error	The current state of messages related to all error handling. Options include on or off.
fib	The current state of messages related to IPMRM FIB processing. Options include on or off.
init	The current state of messages related to initialization code. Options include on or off.
ipms	The current state of messages related to IPMS interaction. Options include on or off.

output definitions (continued)

mip	The current state of messages related to MIP (Management Internal Protocol). Options include on or off.
misc	The current status of miscellaneous message handling. Options include on or off.
protos	The current state of messages related to multicast routing protocols (e.g., whether they are enabled or disabled on interfaces, which protocols are going up or down, etc.). Options include on or off.
tm	The current state of messages related to the Task Manager. Options include on or off.

Release History

Release 5.1; command was introduced.

Related Commands

ip mroute debug-level	Defines the level of multicast routing debug messages that are generated.
ip mroute debug-type	Configures the type(s) of multicast routing debug messages to display.

MIB Objects

```
alaIpmrmDebugConfig
   alaIpmrmDebugLevel
   alaIpmrmDebugError
   alaIpmrmDebugFib
   alaIpmrmDebugAging
   alaIpmrmDebugProtos
   alaIpmrmDebugIpms
   alaIpmrmDebugMip
   alaIpmrmDebugInit
   alaIpmrmDebugTm
   alaIpmrmDebugMisc
   alaIpmrmDebugAll
```

35 Port Mirroring and Monitoring Commands

The Port Mirroring and Port Monitoring feature are used primarily as diagnostic tools.

The Port Mirroring feature allows you to have all the traffic (inbound and outbound) of an Ethernet port sent to another port on the switch. When you enable port mirroring, the active, or "mirrored," port transmits and receives network traffic normally and the "mirroring" port receives a copy of all transmit and receive traffic to the active port. You can connect an RMON probe or network analysis device to the mirroring port to see an exact duplication of traffic on the mirrored port without disrupting network traffic to and from the mirrored port.

The Port Monitoring feature allows you to examine packets to and from a specific Ethernet port.

MIB information for the Port Mirroring commands is as follows:

Filename: AlcatelIND1portMirMon.mib
Module: ALCATEL-IND1-PORT-MIRRORING-MONITORING-MIB

The following table summarizes the available commands:

Port Mirroring Commands	**port mirroring source destination** **port mirroring** **show port mirroring status**
Port Monitoring Commands	**port monitoring source** **port monitoring** **show port monitoring status** **show port monitoring file**

port mirroring source destination

Defines a port to mirror and the port that is to receive data from the mirrored port, and enables or disables port mirroring status.

port mirroring *port_mirror_sessionid* **[no] source** *slot/port***[-***port2***] [***slot/port***[-***port2***]...]**
destination *slot/port* **[bidirectional |inport |outport] [unblocked** *vlan_id***] [enable | disable]**

Syntax Definitions

port_mirror_sessionid	Mirroring session identifier.
source	Adds a to a port mirroring session.
no source	Removes a port or range of ports from a port mirroring session.
slot	Slot number you want to configure.
port	Port number of the interface you want to configure.
port2	Last port number in a range of ports you want to configure.
[*slot/port***[-***port2***]...]**	Configures multiple source ports.
bidirectional	Specifies bidirectional port mirroring.
inport	Specifies incoming unidirectional port mirroring.
outport	Specifies outgoing unidirectional port mirroring.
vlan_id	VLAN ID number (1–4094) that specifies the VLAN to protect from Spanning Tree changes while port mirroring/monitoring is active. Ports in this VLAN will remain unblocked.
enable	Enables port mirroring status.
disable	Disables port mirroring status.

Defaults

parameter	default
bidirectional | inport | outport	**bidirectional**
enable | disable	disable on OmniSwitch 6600, 7700, 7800, and 8800;

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- On OmniSwitch 7700/7800/8800 switches you can have up to four unidirectional sessions *or* two bidirectional port mirroring sessions are supported.
- One port mirroring session is supported per OmniSwitch 6624, OmniSwitch 6600-U24, OmniSwitch 6600-P24, or OmniSwitch 6602-24 in a stack. Therefore, a stack of four OmniSwitch 6624s could have four port mirroring sessions.
- Up to two port mirroring sessions are supported per OmniSwitch 6648 or OmniSwitch 6602-48 in a stack. Therefore, a stack of four OmniSwitch 6648s could have eight port mirroring sessions.
- On OmniSwitch 6600, 7700, 7800, and 8800 the same destination port can be shared by up to four sessions.
- On OmniSwitch 6600, 7700, 7800, and 8800 link aggregation ports cannot be mirrored in the current release.
- Once you execute the **port mirroring source destination** command to define the mirrored port and enable port mirroring status, the **port mirroring** command must be used to enable the port mirroring session on OmniSwitch 6600, 7700, 7800, and 8800 switches.
- By default, the mirroring port is subject to Spanning Tree changes that could cause it to go into a blocked state. To prevent this, specify the *vlan_id* number of the mirroring port that is to remain **unblocked** when executing the command.

Examples

On OmniSwitch 6600, 7700, 7800, and 8800 switches:

```
-> port mirroring 6 source 2/3 destination 6/4
-> port mirroring 6 source 2/3 destination 6/4 unblocked 750
-> port mirroring 6 source 2/3 destination 6/4 unblocked 750 enable
-> port mirroring 9 source 1/23 destination 1/24 inport
-> port mirroring 9 disable
```

Release History

Release 5.1; command was introduced.

Related Commands

port mirroring	Enables, disables or deletes a port mirroring session.
show port mirroring status	Displays status of mirrored ports. This value may be enabled or disabled.

MIB Objects

```
mirrorTable
   mirrorMirroringIfindex
   mirrorDirection
   mirrorStatus
   mirrorUnblockedVLAN
```

port mirroring

Enables, disables, or deletes a port mirroring session.

port mirroring *port_mirror_sessionid* **{enable | disable}**

no port mirroring *port_mirror_sessionid* **{enable | disable}**

Syntax Definitions

port_mirror_sessionid	Mirroring session identifier.
enable	Enables port mirroring.
disable	Disables port mirroring.
no	Optional syntax. Deletes a previously-configured port mirroring session.

Defaults

parameter	default
enable | **disable**	disabled

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- You must first enter the **port mirroring source destination** command to specify the mirrored and destination ports. Then use this command to enable or disable port mirroring activity on these ports.
- Use the **no** form of the command to delete a port mirroring session.

Examples

```
-> port mirroring 6 enable
-> port mirroring 6 disable
-> no port mirroring 6
```

Release History

Release 5.1; command was introduced.

Related Commands

port mirroring source destination	Defines a port to mirror and the port that is to receive data from the mirrored port, and enables or disables port mirroring status.
show port mirroring status	Displays status of mirrored ports. This value may be enabled or disabled.

MIB Objects

```
mirrorTable
   mirrorMirroringIfindex
   mirrorStatus
```

port monitoring source

Configures a port monitoring session.

port monitoring *port_monitor_sessionid* **source** *slot/port*
[{no file | file *filename* **[size** *filesize***] | [overwrite {on | off}]}]**
[inport | outport | bidirectional] [timeout *seconds***] [enable | disable]**

Syntax Definitions

port_monitor_sessionid	Monitoring session identifier.
slot/port	Enter the slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
file *filename*	Specifies a file name for the monitoring session (e.g., **/flash/port2**).
filesize	Specifies the size of the file in 16K (16384) byte increments. For example, a value of 3 would specify a size of 49152 bytes. The file size can be up to 160 K (163840 bytes).
no file	Specifies that no file will be created for the monitoring session.
on	Specifies that any existing port monitoring file in flash memory will be overwritten if the total data exceeds the specified file size.
off	Specifies that any existing port monitoring file in flash memory will not be overwritten if the total data exceeds the specified file size.
inport	Specifies incoming unidirectional port monitoring.
outport	Specifies outgoing unidirectional port monitoring.
seconds	Specifies the number of seconds how many seconds after which the session gets disabled. The range is 0–2147483647 where 0 is forever.
enable	Enables the port monitoring status.
disable	Disables the port monitoring status.

Defaults

parameter	default
filesize	1
on | off	on
bidirectional | inport | outport	**bidirectional**
seconds	0
enable | disable	**disable**

Platforms Supported

OmniSwitch 6600

Usage Guidelines

- The maximum number of monitoring sessions is limited one per chassis and/or stack.
- You cannot configure port mirroring and monitoring on the same switching ASIC on OmniSwitch 6600 Family switches. OmniSwitch 6624, 6600-P24, 6600-U24, and 6602-24 switches contain one switching ASIC. On OmniSwitch 6648 switches ports 1 through 24 and 49 and 50 are on one switching ASIC while ports 25 through 48 and 51 and 52 are on another switching ASIC. On OmniSwitch 6602-48 switches ports 1 through 24 and 49 and 50 are on one switching ASIC while ports 25 through 48 are on another switching ASIC.
- By default, a file called **pmonitor.enc** is created in the **/flash** directory when you configure and enable a port monitoring session. Use the **file** option to create a user-specified file.
- By default, more-recent frames will overwrite older frames in a port monitoring file if the total data exceeds the specified file size. Use the **overwrite off** option to prevent this from occurring.
- Only the first 64 bytes of the traffic will be captured.
- Link aggregation ports can not be monitored.
- The format of the file created is compliant with the ENC file format (Network General Sniffer Network Analyzer Format).

Examples

```
-> port monitoring 6 source 2/3
-> port monitoring 6 source 2/3 file port3 size 2 enable
```

Release History

Release 5.1.6; command was introduced.

Related Commands

port monitoring	Disables, pauses, resumes, or deletes a port monitoring session.
show port monitoring status	Displays port monitoring status.
show port monitoring file	Displays port monitoring data.

MIB Objects

```
monitorTable
   monitorSessionNumber
   monitorIfindex
   monitorFileStatus
   monitorFileName
   monitorFileSize
   monitorScreenStatus
   monitorScreenLine
   monitorTrafficType
   monitorStatus
   monitorFileOverWrite
   monitorDirection
   monitorTimeout
```

port monitoring

Disables, pauses, resumes, or deletes an existing port monitoring session.

port monitoring *port_monitor_sessionid* **{disable | pause | resume}**

no port monitoring *port_monitor_sessionid*

Syntax Definitions

port_monitor_sessionid	Monitoring session identifier.
disable	Disables the port monitoring session.
pause	Pauses the port monitoring session.
resumes	Resumes the port monitoring session.

Defaults

N/A

Platforms Supported

OmniSwitch 6600

Usage Guidelines

Use the **no** form of the command to delete a port monitoring session.

Examples

```
-> port monitoring 6 pause
-> port monitoring 6 disable
-> port monitoring 6 resume
-> no port monitoring 6
```

Release History

Release 5.1.6; command was introduced.

Related Commands

port monitoring	Configures a port monitoring session.
show port monitoring status	Displays port monitoring status.

MIB Objects

```
monitorTable
   monitorSessionNumber
   monitorScreenStatus
```

show port mirroring status

Displays status of mirrored ports.

show port mirroring status [*port_mirror_sessionid***]**

Syntax Definitions

port_mirror_sessionid	Mirroring session identifier.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

On OmniSwitch 7700/7800/8800 switches if you do not specify a port mirroring session identifier then all port mirroring sessions will be displayed. (Only one session is supported on OmniSwitch 6600 Family switches.)

Examples

On OmniSwitch 6600, 7700, 7800, 8800 switches:

```
-> show port mirroring status 6

 Session   Mirrored   Mirroring      Mirror     Mirroring  Mirroring
           slot/port  slot/port     Direction     Vlan       Status
----------+----------+----------+--------------+----------+----------
 6.          1/23       1/24      bidirectional  NONE       OFF
```

output definitions

Session	The port mirroring session identifier.
Mirrored slot/port	The location of the mirrored port.
Mirroring slot/port	The location of the mirroring port.
Mirror Direction	The direction of the mirroring session, which can be **bidirectional** (the default), **inport**, or **outport**.
Mirroring VLAN	The mirroring VLAN ID number.
Mirroring Status	The current status of Port Mirroring session (on/off).

Release History

Release 5.1; command was introduced.

Related Commands

port mirroring	Enables, disables or deletes a port mirroring session.
port mirroring source destination	Defines a port to mirror and the port that is to receive data from the mirrored port, and enables or disables port mirroring status.

MIB Objects

```
mirrorTable
   mirrorMirroringIfindex
   mirrorDirection
   mirrorStatus
   mirrorUnblockedVLAN
```

show port monitoring status

Displays port monitoring status.

show port monitoring status [*port_monitor_sessionid***]**

Syntax Definitions

port_monitor_sessionid	Monitoring session identifier.

Defaults

N/A

Platforms Supported

OmniSwitch 6600

Usage Guidelines

If you do not specify a port monitoring session identifier then all port monitoring sessions will be displayed.

Examples

```
-> show port monitoring status

Session    Monitor    Monitor    Overwrite     Operating      Admin
           slot/port  Direction                Status        Status
----------+----------+----------+-------------+----------+--------------------
     1.       1/ 9   Bidirectional      ON            ON           ON
```

output definitions

Session	The port monitoring session identifier.
Monitor slot/port	The location of the monitored port.
Monitor Direction	The direction of the monitoring session, which can be **bidirectional** (the default), **inport**, or **outport**.
Overwrite	Whether files created by a port monitoring session can be overwritten. The default is ON.
Operating Status	The current operating status of the port monitoring session (on/off)
Admin Status	The current administrative status of the port monitoring session (on/off).

Release History

Release 5.1.6; command was introduced.

Related Commands

port monitoring source	Configures a port monitoring session.
port monitoring	Disables, pauses, resumes, or deletes a port monitoring session.
show port monitoring file	Displays port monitoring data.

MIB Objects

```
monitorTable
   monitorSessionNumber
   monitorIfindex
   monitorStatus
   monitorFileOverWrite
   monitorDirection
```

show port monitoring file

Displays port monitoring data.

show port monitoring file [*port_monitor_sessionid***]**

Syntax Definitions

port_monitor_sessionid	Monitoring session identifier.

Defaults

N/A

Platforms Supported

OmniSwitch 6600

Usage Guidelines

N/A

Examples

```
-> show port monitoring file

Destination       | Source            |  Type  | Data
------------------------------------------------------------------------------
01:80:C2:00:00:00 | 00:20:DA:8F:92:C6 |  BPDU  | 00:26:42:42:03:00:00:00:00:00
00:20:DA:C7:2D:D6 | 08:00:20:95:F3:89 |  UDP   | 08:00:45:00:00:6B:FE:4A:40:00
00:20:DA:A3:89:F6 | 08:00:20:95:F3:89 |  UDP   | 08:00:45:00:00:6B:CF:89:40:00
00:20:DA:BF:5B:76 | 08:00:20:95:F3:89 |  UDP   | 08:00:45:00:00:6B:CF:85:40:00
00:20:DA:A3:89:F6 | 08:00:20:95:F3:89 |  UDP   | 08:00:45:00:00:6B:CF:8A:40:00
00:20:DA:BF:5B:76 | 08:00:20:95:F3:89 |  UDP   | 08:00:45:00:00:6B:CF:86:40:00
00:20:DA:A3:89:F6 | 08:00:20:95:F3:89 |  UDP   | 08:00:45:00:00:6B:CF:8B:40:00
01:80:C2:00:00:00 | 00:20:DA:8F:92:C6 |  BPDU  | 00:26:42:42:03:00:00:00:00:00
00:20:DA:BF:5B:76 | 08:00:20:95:F3:89 |  UDP   | 08:00:45:00:00:6B:CF:87:40:00
```

output definitions

Destination	The destination MAC address of the packet.
Source	The source MAC address of the packet.
Type	The type of packet.
Data	The packet displayed in hexadecimal format.

Release History

Release 5.1.6; command was introduced.

Related Commands

port monitoring source	Configures a port monitoring session.
port monitoring	Disables, pauses, resumes, or deletes a port monitoring session.
show port monitoring status	Displays port monitoring status.

MIB Objects

```
monitorTable
   monitorSessionNumber
   monitorIfindex
   monitorTrafficType
```

36 RMON Commands

Remote Network Monitoring (RMON) probes can be used to monitor, manage and compile statistical data about network traffic from designated active ports in a LAN segment without negatively impacting network performance. This feature supports basic RMON 4 group implementation compliant with RFC 2819 (Remote Network Monitoring Management Information Base), but does not support RMON 10 group or RMON 2. This chapter includes descriptions of RMON commands used to enable or disable individual (or a group of a certain flavor type) RMON probes, show a list of (or individual) RMON probes and show a list of (or individual) RMON logged events.

MIB information for the RMON commands is as follows:

Filename: IETF_RMON.mib
Module: RMON-MIB

The following table summarizes the available commands:

rmon probes
show rmon probes
show rmon events

rmon probes

This command enables or disables types of RMON probes.

rmon probes {stats | history | alarm} [*entry-number***] {enable | disable}**

Syntax Definitions

stats	Ethernet Statistics Table probe entries.
history	History Control Table probe entries.
alarm	Alarm Table probe entries.
entry-number	The entry number in the list of probes *(optional)*.
enable	Enables the RMON probe.
disable	Disables the RMON probe.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Network activity on subnetworks attached to the RMON probe can be monitored by NMS applications.
- RMON will not monitor activities on the CMM onboard Ethernet Management port.

Examples

```
-> rmon probes stats 4012 enable
-> rmon probes history 10240 disable
-> rmon probes alarm 11235 enable
-> rmon probes stats enable
-> rmon probes history disable
-> rmon probes alarm enable
```

Release History

Release 5.1; command was introduced.

Related Commands

show rmon probes	Displays a list of RMON probes or a single RMON probe.
show rmon events	Displays a list of RMON logged events or a single RMON event.

MIB Objects

```
ETHERSTATSTABLE
   etherStatsStatus
HISTORYCONTROLTABLE
   historyControlStatus
ALARMTABLE
   alarmStatus
```

show rmon probes

Displays a list of RMON probes or single RMON probe.

show rmon probes [stats | history | alarm] [*entry-number***]**

Syntax Definitions

stats	Ethernet Statistics Table probe entries.
history	History Control Table probe entries.
alarm	Alarm Table probe entries.
entry-number	The entry number in the list of probes *(optional)*.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- To display a list of current probes, omit the *entry-number* from the command line.
- To display statistics for a particular probe, include the probe's *entry-number* in the command line.
- The **show rmon probes** command displays the following information: Entry number, Slot/Port, Flavor (whether the probe type is Ethernet, History or Alarm), Status (Active or Inactive), Duration (time since the last change in status, in hours/minutes) and System Resources (the amount of memory allocated to this probe).
- The **show rmon probes** *entry-number* command displays the following information: Probe's Owner (probe type and location), Slot/Port, Entry number, Flavor (whether the probe type is Ethernet, History or Alarm), Status (Active or Inactive), Time since the last change in status (hours/minutes), and System Resources (the amount of memory allocated to this probe). Displayed statistics may vary, depending on whether the probe type is Ethernet, History or Alarm.

Examples

```
-> show rmon probes stats

Entry    Slot/Port   Flavor     Status       Duration          System Resources
-------+-----------+-----------+----------+---------------+---------------------
 4001     4/1        Ethernet    Active      00:25:00          275 bytes
 4008     4/8        Ethernet    Active      00:25:00          275 bytes
 4005     4/5        Ethernet    Active      00:25:00          275 bytes
```

```
-> show rmon probes history

Entry    Slot/Port   Flavor     Status       Duration          System Resources
-------+-----------+-----------+----------+---------------+---------------------
    1     4/1        History     Active      00:25:00          9063 bytes
10240     4/5        History     Active      00:14:00          601 bytes
10325     4/8        History     Active      00:14:00          601 bytes

-> show rmon probes alarm

Entry    Slot/Port   Flavor     Status       Duration          System Resources
-------+-----------+-----------+----------+---------------+---------------------
11235     4/8        Alarm       Active      00:07:00          835 bytes

-> show rmon probes stats 4005

Probe's Owner: Falcon Switch Auto Probe on Slot 4, Port 5
    Entry 4005
      Flavor = History, Status = Active
      Time = 48 hrs 54 mins,
      System Resources (bytes) = 275

-> show rmon probes history 10325

Probe's Owner: Analyzer-p:128.251.18.166 on Slot 4, Port 5
  History Control Buckets Requested  = 2
  History Control Buckets Granted    = 2
  History Control Interval           = 30 seconds
  History Sample Index               = 5859
   Entry 10325
      Flavor = History, Status = Active
      Time = 48 hrs 53 mins,
      System Resources (bytes) = 601

-> show rmon probes alarm 11235

Probe's Owner: Analyzer-t:128.251.18.166 on Slot 4, Port 8
  Alarm Rising Threshold         = 5
  Alarm Falling Threshold        = 0
  Alarm Rising Event Index       = 26020
  Alarm Falling Event Index      = 0
  Alarm Interval                 = 10 seconds
  Alarm Sample Type              = delta value
  Alarm Startup Alarm            = rising alarm
  Alarm Variable = 1.3.6.1.2.1.16.1.1.1.5.4008
   Entry 11235
      Flavor = Alarm, Status = Active
      Time = 48 hrs 48 mins,
      System Resources (bytes) = 1677
```

output definitions

Probe's Owner	Description and interface (location) of the probe.
Slot/Port	The Slot/Port number (interface) that this probe is monitoring.
Entry	The Entry number in the list of probes.
Flavor	Whether the probe type is Ethernet, History or Alarm.
Status	The status of the probe–**Creating** (the probe is under creation), **Active** (the probe is Active) or **Inactive** (the probe is inactive).
Duration	Elapsed time (hours/minutes/seconds) since the last change in status.
System Resources	Amount of memory that has been allocated to this probe.

Release History

Release 5.1; command was introduced.

Related Commands

rmon probes	Enables or disables types of RMON probes.
show rmon events	Displays RMON logged events.

MIB Objects

```
ETHERSTATSTABLE
   etherStatsIndex
HISTORYCONTROLTABLE
   historyControlIndex
ALARMTABLE
   alarmIndex
```

show rmon events

Displays RMON events (actions that take place based on alarm conditions detected by the RMON probe).

show rmon events [*event-number***]**

Syntax Definitions

event-number	The event number *(optional)* in the list of probes.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- To display a list of logged events, omit the *event-number* from the command line.
- To display statistics for a particular event, include the *event-number* in the command line.
- The **show rmon events** command displays the following information for all RMON Logged Events: Entry number, Time (hours/minutes/seconds) since the last change in status and Description (nature of the event).
- The **show rmon events** *event-number* command displays the following information for a particular RMON Logged Event: Entry number, Time (hours/minutes/seconds) since the last change in status and Description (nature of the event).

Examples

```
-> show rmon events

Entry               Time               Description
---------+------------------+-----------------------------------------------------
1               00:08:00       etherStatsPkts.4008: [Falling trap] “Falling Event”
2               00:26:00       etherStatsCollisions.2008: “Rising Event”


-> show rmon events 2

Entry               Time               Description
---------+------------------+-----------------------------------------------------
2               00:26:00       etherStatsCollisions.2008: “Rising Event”
```

output definitions

Entry	The entry number in the list of probes.
Time	Time (hours, minutes, and seconds) since the last change in status.
Description	Description of the Alarm condition detected by the probe.

Release History

Release 5.1; command was introduced.

Related Commands

rmon probes	Enables or disables types of RMON probes.
show rmon probes	Displays RMON probes or a single RMON probe.

MIB Objects

```
EVENTTABLE
   eventIndex
```

37 Health Monitoring Commands

The Health Monitoring function monitors the consumable resources of the switch (e.g., bandwidth usage, CPU usage) and provides a single integrated resource for a Network Management System (NMS). This function monitors the switch, and at fixed intervals, collects the current values for each resource being monitored. Users specify resource threshold limits and traps are sent to an NMS if a value falls above or below a user-specified threshold.

The Health Monitoring commands comply with RFC1212.

MIB information for the Health Monitoring commands is as follows:

Filename: AlcatelIND1Health.mib
Module: healthMIB

A summary of the available commands is listed here:

health threshold
health interval
health statistics reset
show health threshold
show health interval
show health
show health all
show health slice

health threshold

Configures thresholds for input traffic (RX), output/input traffic (TX/RX), memory usage, CPU usage, and chassis temperature.

Input traffic, output/input traffic, memory usage, CPU usage thresholds specify the maximum percentage for each resource that may be consumed before a trap is sent to the user. The temperature threshold specifies the maximum operating temperature, in Celsius, allowed within the chassis before a trap is sent.

health threshold {rx *percent* **| txrx** *percent* **| memory** *percent* **| cpu** *percent* **| temperature** *degrees***}**

Syntax Definitions

rx	Specifies the maximum input (RX) traffic threshold.
txrx	Specifies the maximum output/input (TX/RX) traffic threshold.
memory	Specifies the maximum RAM memory usage threshold.
cpu	Specifies the maximum CPU usage threshold.
percent	The new threshold value, in percent, for the corresponding resource—i.e., **rx**, **txrx**, **memory**, **cpu**—(0–100).
temperature	Specifies the temperature threshold for the chassis.
degrees	The new threshold value, in Celsius, for the chassis temperature threshold (0–100).

Defaults

parameter	default
percentage	80
degrees	50

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- When a resource falls back below the configured threshold, an addition trap is sent to the user. This indicates that the resource is no longer operating beyond its configured threshold limit.
- Changing a threshold value sets the value for all levels of the switch (i.e., switch, module, and port). You cannot set different threshold values for each level.
- For detailed information on each threshold type, refer to page 37-6, or refer to the chapter titled “Diagnosing Switch Problems” in your Network Configuration Guide.

Examples

```
-> health threshold rx 85
-> health threshold txrx 55
-> health threshold memory 95
-> health threshold cpu 85
-> health threshold temperature 40
```

Release History

Release 5.1; command was introduced.

Related Commands

show health threshold	Displays current health threshold settings.

MIB Objects

```
HealthThreshInfo
   healthThreshDeviceRxLimit
   healthThreshDeviceTxRxLimit
   healthThreshDeviceTempLimit
   healthThreshDeviceMemoryLimit
   healthThreshDeviceCpuLimit
```

health interval

Configures the sampling interval between health statistics checks. The sampling interval is the time interval between polls of the switch's consumable resources to see if it is performing within set thresholds.

health interval *seconds*

Syntax Definitions

seconds	Sampling interval (in seconds). Valid entries are 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30.

Defaults

parameter	default
seconds	5

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Decreasing the polling interval may impact switch performance.

Examples

```
-> health interval 6
```

Release History

Release 5.1; command was introduced.

Related Commands

show health interval	Displays the current health sampling interval.

MIB Objects

```
HealthThreshInfo
   healthSamplingInterval
```

health statistics reset

Resets health statistics for the switch.

health statistics reset

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This command clears statistics for the entire switch. You cannot clear statistics for a module or port only.

Examples

```
-> health statistics reset
```

Release History

Release 5.1; command was introduced.

Related Commands

show health	Displays health statistics for the switch.

MIB Objects

```
HealthThreshInfo
   healthSamplingReset
```

show health threshold

Displays current health threshold settings.

show health threshold [rx | txrx | memory | cpu | temperature]

Syntax Definitions

rx	Displays the current input (RX) traffic threshold.
txrx	Displays the current output/input (TX/RX) traffic threshold.
memory	Displays the current RAM memory usage threshold.
cpu	Displays the current CPU usage threshold.
temperature	Displays the current chassis temperature threshold.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Unless a specific resource type (i.e., **rx**, **txrx**, **memory**, **cpu** or **temperature**) is specified, threshold information for *all* resources displays.
- To display only a specific threshold, enter the command, followed by the specific resource type (**rx**, **txrx**, **memory**, **cpu** or **temperature**). For example, to display only the memory threshold, enter the following syntax: **show health threshold memory**.

Examples

```
-> show health threshold
Rx Threshold          = 80
TxRx Threshold        = 80
Memory Threshold      = 80
CPU Threshold         = 80
Temperature Threshold = 50
```

output definitions

`Rx Threshold`	The current device input (RX) threshold. This value displays the maximum percentage of total bandwidth allowed for *incoming traffic* on the switch. The total bandwidth is defined as the Ethernet port capacity for all NI modules currently operating in the switch, in Mbps. For example, a chassis with 48 100Base-T Ethernet ports installed has a total bandwidth of 4800 Mbps. The default value is 80 percent and can be changed via the **health threshold** command.
`TxRx Threshold`	The current device output/input (TX/RX) threshold. This value displays the maximum percentage of total bandwidth allowed for *all incoming and outgoing traffic*. As with the RX threshold described above, the total bandwidth is defined as the Ethernet port capacity for all NI modules currently operating in the switch, in Mbps. The default value is 80 percent and can be changed via the **health threshold** command.
`Memory Threshold`	Displays the current memory usage threshold. Memory usage refers to the total amount of RAM memory currently used by switch applications. The default value is 80 percent and can be changed via the **health threshold** command.
`CPU Threshold`	Displays the current CPU usage threshold. CPU usage refers to the total amount of CPU processor capacity currently used by switch applications. The default value is 80 percent and can be changed via the **health threshold** command.
`Temperature Threshold`	Displays the current chassis temperature threshold, in Celsius. The default value is 50 degrees Celsius and can be changed via the **health threshold** command.

Release History

Release 5.1; command was introduced.

Related Commands

health threshold	Configures thresholds for input traffic (RX), output/input traffic (TX/RX), memory usage, CPU usage, and chassis temperature.

MIB Objects

```
HealthThreshInfo
   healthThreshDeviceRxLimit
   healthThreshDeviceTxRxLimit
   healthThreshDeviceTempLimit
   healthThreshDeviceMemoryLimit
   healthThreshDeviceCpuLimit
```

show health interval

Displays the current health sampling interval.

show health interval

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **health interval** command to set the sampling interval.

Examples

```
-> show health interval

Sampling Interval = 5
```

output definitions

`Sampling Interval`	Currently configured interval between health statistics checks (in seconds).

Release History

Release 5.1; command was introduced.

Related Commands

health interval	Configures the interval between health statistics checks.

MIB Objects

```
HealthThreshInfo
   healthSamplingInterval
```

show health

Displays health statistics for the switch. Statistics are displayed as percentages of total resource capacity and represent data taken from the last sampling interval.

show health [*slot/port*] **[statistics]**

Syntax Definitions

slot/port	To view a specific slot, enter the slot number (e.g., 3). To view a view a specific port, enter the slot and port number (e.g., 3/1).
statistics	Optional command syntax. It displays the same information as the **show health** command.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If no *slot/port* information is specified, aggregate health statistics for *all* ports is displayed.
- Use the **health statistics reset** command to reset health statistics for the switch.

Examples

```
-> show health
* - current value exceeds threshold

Device                              1 Min  1 Hr  1 Hr
Resources              Limit  Curr   Avg    Avg   Max
---------------+-------+-----+------+-----+-----+-------
Receive                80     01     01     01    01
Transmit/Receive       80     01     01     01    01
Memory                 80     66     66     66    66
CPU                    80     41     40     32    30
Temperature Cmm        50     33     33     33    33
Temperature Cmm Cpu    50     32     32     32    32

-> show health 4/3
* - current value exceeds threshold

Port 04/03                    1 Min  1 Hr   1 Hr
Resources        Limit  Curr   Avg    Avg    Max
---------------+-------+-----+-------+-----+-------
Receive          80     01     01     01     01
Transmit/Receive 80     01     01     01     01
```

output definitions

`Receive`	Traffic received by the switch.
`Transmit/Receive`	Traffic transmitted and received by the switch.
`Memory`	Switch memory.
`CPU`	Switch CPU.
`Temperature Cmm`	CMM Chassis Temperature.
`Temperature Cmm Cpu`	CMM CPU Temperature.
`Limit`	Currently configured device threshold levels (percentage of total available bandwidth or temperature measured in degrees Celsius).
`Curr`	Current device bandwidth usage or temperature (measured in degrees Celsius).
`1 Min Avg`	Average device bandwidth usage or temperature (measured in degrees Celsius) over a 1-minute period.
`1 Hr Avg`	Average device bandwidth usage or temperature (measured in degrees Celsius) over a 1-hour period.
`1 Hr Max`	Maximum device bandwidth usage or temperature (measured in degrees Celsius) over a 1-hour period (i.e., the maximum of the 1 minute averages).

Release History

Release 5.1; command was introduced.

Related Commands

health statistics reset	Resets health statistics for the switch.
show health all	Displays health statistics for a specified resource on *all* NIs currently operating in the chassis.

MIB Objects

```
healthModuleTable
   healthModuleSlot
   healthModuleRxLatest
   healthModuleRx1MinAvg
   healthModuleRx1HrAvg
   healthModuleRx1HrMax
   healthModuleRxTxLatest
   healthModuleRxTx1MinAvg
   healthModuleRxTx1HrAvg
   healthModuleRxTx1HrMax
   healthModuleMemoryLatest
   healthModuleMemory1MinAvg
   healthModuleMemory1HrAvg
   healthModuleMemory1HrMax
   healthModuleCpuLatest
   healthModuleCpu1MinAvg
   healthModuleCpu1HrAvg
   healthModuleCpu1HrMax
```

show health all

Displays health statistics for a specified resource on all *active NI modules* installed in the chassis.

show health all {memory | cpu | rx | txrx}

Syntax Definitions

memory	Displays RAM memory health statistics for all active NI modules in the switch.
cpu	Displays CPU health statistics for all active NI modules.
rx	Displays health statistics for traffic *received* on all active NI modules.
txrx	Displays health statistics for traffic both *transmitted and received* on all active NI modules.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show health all memory
* - current value exceeds threshold

                                  1 Min  1 Hr  1 Hr
Memory             Limit   Curr   Avg    Avg   Max
-----------------+-------+------+------+-----+----
01                   80     40     40    40    40
02                   80     40     40    40    40
03                   80     40     40    40    40
04                   80     40     40    40    40
05                   80     40     40    40    40
06                   80     40     40    40    40
07                   80     40     40    40    40
13                   80     40     40    40    40
```

output definitions

`Memory (Cpu, TXRX, RX)`	A list of all currently-active NI modules (i.e., active slots) on the switch. The column header corresponds with the resource keyword entered. For example, if **show health all cpu** is entered, **Cpu** is used as the column header.
`Limit`	Current usage threshold for the specified resource type, on the corresponding slot (in percent). The usage threshold refers to the maximum amount of the resource's total bandwidth that can be used by switch applications before a notification is sent to the user. The default value for all resource types is 80 percent. This threshold can be changed via the **health threshold** command.
`Curr`	Current usage of the resource on the corresponding slot, in percent (i.e., the amount of the resource's total bandwidth actually being used by switch applications).
`1 Min Avg`	Average usage of the resource on the corresponding slot over a one minute period.
`1 Hr Avg`	Average usage of the resource on the corresponding slot over a one hour period.
`1 Hr Max`	The highest average hourly usage for the resource on the corresponding slot.

Release History

Release 5.1; command was introduced.

Related Commands

show health	Displays health statistics for the switch.
health threshold	Configures thresholds for input traffic (RX), output/input traffic (TX/RX), memory usage, CPU usage, and chassis temperature.

MIB Objects

```
healthModuleTable
   healthModuleSlot
   healthModuleRxLatest
   healthModuleRx1MinAvg
   healthModuleRx1HrAvg
   healthModuleRx1HrMax
   healthModuleRxTxLatest
   healthModuleRxTx1MinAvg
   healthModuleRxTx1HrAvg
   healthModuleRxTx1HrMax
   healthModuleMemoryLatest
   healthModuleMemory1MinAvg
   healthModuleMemory1HrAvg
   healthModuleMemory1HrMax
   healthModuleCpuLatest
   healthModuleCpu1MinAvg
   healthModuleCpu1HrAvg
   healthModuleCpu1HrMax
```

show health slice

Displays health statistics for a particular slice. The term *slice* refers to an amount of CPU time and RAM memory allotted for switch applications. By monitoring slice statistics on the switch, users can determine whether there are any potential usage issues with CPU and RAM memory that may affect switch multi-tasking.

show health slice *slot*

Syntax Definitions

slot	A specific physical slot number for which slice statistics are to be displayed (e.g., 3).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show health slice 13
Slot 13     slice
Resources     1
----------+-------
Memory       40
Cpu          21
```

output definitions

Slot	The physical slot number for the corresponding slice.
slice	The on-board slice number (1–64).
Memory	The slice-level RAM memory utilization over the latest sample period, in percent (0–100).
Cpu	The slice-level CPU utilization over the latest sample period, in percent (0–100).

Release History

Release 5.1; command was introduced.

Related Commands

N/A

MIB Objects

```
healthSliceTable
   healthSliceSlot
   healthSliceSlice
   healthSliceMemoryLatest
   healthSliceCpuLatest
```

38 QoS Commands

This chapter describes CLI commands used for Quality of Service (QoS) and policy management in the switch. The QoS software in the switch uses policy rules for classifying incoming flows and deciding how to treat outgoing flows. A policy rule is made up of a policy condition and a policy action. Policy rules may be created on the switch through CLI or SNMP commands, or they may be created through the PolicyView GUI application on an attached LDAP server.

Note. Rules created through PolicyView cannot be modified through the CLI; however, you can create policies in the CLI that take precedence over policies created through PolicyView.

MIB information for the QoS commands is as follows:

Filename: alcatelIND1Qos.mib
Module ALCATEL-IND1-QoS-MIB

Important Note. Some of the commands listed here are not currently supported. See command descriptions in this chapter and check release notes for information about commands that are not supported.

Policy commands	**policy rule** **policy condition** **policy action** **show policy action** **show policy condition** **show policy rule**
Group commands	**policy network group** **policy service** **policy service group** **policy mac group** **policy port group** **policy map group** **show policy network group** **show policy mac group** **show policy port group** **show policy map group** **show policy service** **show policy service group**

Global commands	**qos** **qos trust ports** **qos default queues** **qos forward log** **qos log console** **qos log lines** **qos log level** **qos classifyl3 bridged** **qos classify fragments** **qos flow timeout** **qos fragment timeout** **qos reflexive timeout** **qos nat timeout** **qos default bridged disposition** **qos default routed disposition** **qos default multicast disposition** **qos stats interval** **debug qos** **debug qos internal** **qos clear log** **qos apply** **qos revert** **qos flush** **qos reset** **qos stats reset** **show qos queue** **show qos slice** **show qos log** **show qos config** **show qos statistics**
Port and Slice commands	**qos port** **qos port reset** **qos port default queues** **qos port trusted** **qos port maximum reserve bandwidth** **qos port maximum signal bandwidth** **qos port maximum default depth** **qos port maximum default buffers** **qos port default classification** **qos port default 802.1p** **qos port default dscp** **qos port enqueuing thresholds** **qos port protocol priority** **qos slice** **qos slice dscp** **qos slice servicing mode** **qos slice wred thresholds** **show qos port** **show qos port high-density-module** **show qos slice** **show qos slice high-density-module**

Condition commands	**policy condition** **policy condition source ip** **policy condition destination ip** **policy condition multicast ip** **policy condition source network group** **policy condition destination network group** **policy condition multicast network group** **policy condition source ip port** **policy condition destination ip port** **policy condition source tcp port** **policy condition destination tcp port** **policy condition source udp port** **policy condition destination udp port** **policy condition ethertype** **policy condition service** **policy condition service group** **policy condition ip protocol** **policy condition source mac** **policy condition destination mac** **policy condition source mac group** **policy condition destination mac group** **policy condition source vlan** **policy condition destination vlan** **policy condition source port** **policy condition destination port** **policy condition source port group** **policy condition destination port group** **policy condition source interface type** **policy condition destination interface type**
Command for testing conditions	**show policy classify**
Action commands	**policy action** **policy action disposition** **policy action shared** **policy action priority** **policy action maximum bandwidth** **policy action maximum buffers** **policy action minimum depth** **policy action maximum depth** **policy action tos** **policy action 802.1p** **policy action dscp** **policy action map** **policy action source rewrite ip** **policy action source rewrite network group** **policy action destination rewrite ip** **policy action destination rewrite network group** **policy action load balance group** **policy action alternate gateway ip** **policy action permanent gateway ip**

Types of policies are generally determined by the kind of traffic they classify (policy conditions) and how the policy is enforced (policy actions). Commands used for particular types of policies are listed here. See the *OmniSwitch 6624/6648 Network Configuration Guide* or the *OmniSwitch 7700/7800/8800 Network Configuration Guide* for more information about creating these types of policies and information about valid condition/action combinations.

Access Control Lists	**qos reflexive timeout** **policy condition** **policy action disposition** **policy rule**
Traffic prioritization/shaping	**policy action shared** **policy action priority** **policy action maximum bandwidth** **policy rule**
802.1p/ToS/DSCP tagging or mapping	**policy action tos** **policy action 802.1p** **policy action dscp** **policy action map** **policy rule**
Network Address Translation (NAT)	**policy condition source ip** **policy condition destination ip** **policy action source rewrite ip** **policy action source rewrite network group** **policy action destination rewrite ip** **policy action destination rewrite network group** **policy rule**
Server Load Balancing (SLB)	**policy rule** **policy action load balance group**

qos

Enables or disables QoS. This section describes the base command with a single required option (**enable** or **disable**).

In lieu of these options, the base command (**qos**) may be used with other keywords to set up global QoS configuration. These keywords are listed here and described as separate commands later in this chapter. In addition, some keywords have a **no** form to remove the parameter or return it to its default.

qos {enable | disable}
[trust ports]
[default queues {2 | 4}]
[default servicing mode]
[forward log]
[log console]
[log lines *lines***]**
[log level *level***]**
[classifyl3 bridged]
[classify fragments]
[flow timeout *seconds***]**
[fragment timeout *seconds***]**
[reflexive timeout *seconds***]**
[nat timeout *seconds***]**
[default disposition {accept | deny | drop}]
[default multicast disposition {accept | deny | drop}]
[stats interval *seconds***]**

Syntax Definitions

enable	Enables QoS. The QoS software in the switch classifies flows coming into the switch to attempt to match them to QoS policies. If a match is found, the policy parameters are applied to the flow. The **enable** setting may be used alone or in conjunction with optional command keywords.
disable	Disables QoS. Flows coming into the switch are not matched to policies. The **disable** setting cannot be used with any other command keyword.

Defaults

parameter	default
enable | disable	enable

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- When QoS is disabled, flows coming into the switch are classified but not matched to a policy. Traffic is treated as best effort and assigned to default queues.
- The command keywords may be used with or without **enable**; these keywords cannot be used with **disable**.

Examples

```
-> qos enable classifyl3 bridged
-> qos disable
-> qos enable
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy rule	Configures a policy rule on the switch.
show policy rule	Displays information for policy rules configured on the switch.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigEnable
   alaQoSConfigTrustedPorts
   alaQoSConfigDefaultQueues
   alaQoSConfigAppliedDefaultQueues
   alaQoSConfigLogLines
   alaQoSConfigLogLevel
   alaQoSConfigLogConsole
   alaQoSConfigFlowTimeout
   alaQoSConfigApliedFlowTimeout
   alaQoSConfigFragmentTimeout
   alaQoSConfigAppliedFragmentTimeout
   alaQoSConfigReflexiveTimeout
   alaQoSConfigAppliedReflexiveTimeout
   alaQoSConfigNatTimeout
   alaQoSConfigAppliedNatTimeout
   alaQoSConfigClassifyl3Bridged
   alaQoSConfigAppliedClassifyl3Bridged
   alaQoSConfigClassifyFragments
   alaQoSConfigAppliedClassifyFragments
   alaQoSConfigDefaultMulticastDisposition
   alaQoSConfigAppliedDefaultMulticastDisposition
   alaQoSConfigDefaultDisposition
   alaQoSConfigAppliedDefaultDisposition
```

qos trust ports

Configures the global trust mode for QoS ports. Trusted ports can accept 802.1p and ToS values in incoming packets; untrusted ports will set any 802.1p or ToS bits to zero in packets coming in on the ports.

Any port configured through the **qos port** command will automatically be added in the trust mode specified by this command. See page 38-163 for more information about this command.

qos trust ports

qos no trust ports

Syntax Definitions

N/A

Defaults

By default, 802.1Q-tagged ports and mobile ports are trusted; any other port is untrusted by default.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **qos ports trusted** command to override the default for a particular port.
- The setting only applies to ports with incoming traffic.
- Any port configured for 802.1Q is always trusted, regardless of the global setting.
- Mobile ports are always trusted, regardless of the global setting.

Examples

```
-> qos trust ports
-> qos no trust ports
```

Release History

Release 5.1; command was introduced.

Related Commands

qos port	Configures a physical port for QoS.
qos port trusted	Configures whether or not a particular port is trusted or untrusted.
show qos port	Displays information about QoS ports.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigTrustedPorts
```

qos default queues

Configures the default number of default queues for QoS ports.

qos default queues {2 | 4}

Syntax Definitions

2 | 4	The number of default queues that are created by default for each port at switch startup.

Defaults

parameter	default
2 | 4	4

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Use the **qos port default queues** command to override the default for a particular port.
- QoS queues are created at startup when a flow matches a policy with at least one configured action parameter (other than disposition). A flow that matches a policy which has a disposition of accept but no other action parameters will be placed in a default queue. Any flow that does not match a policy is placed in a default queue.

Examples

```
-> qos default queues 2
```

Release History

Release 5.1; command was introduced.

Related Commands

qos port default queues	Configures the number of default queues for the QoS port.
show qos port	Displays information about QoS ports.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigDefaultQueues
   alaQoSConfigAppliedDefaultQueues
```

qos forward log

Enables the QoS software in the switch to send events to the policy server software in the switch in real time. The policy server software may then be polled by an NMS application for logged events.

qos forward log

qos no forward log

Syntax Definitions

N/A

Defaults

By default, logged events are not sent to the PolicyView application.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

An NMS application may query the Policy Manager in the switch for logged events. Use the **qos forward log** command to forward each event as it happens.

Examples

```
-> qos forward log
```

Release History

Release 5.1; command was introduced.

Related Commands

qos log lines	Configures the number of lines in the QoS log.
show qos log	Displays the log of QoS events.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigForwardLog
```

qos log console

Sends QoS log messages to the output console in real time as they happen.

qos log console

qos no log console

Syntax Definitions

N/A

Defaults

By default, logged events are not sent to the console.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use this command to view log events as they happen on an output console attached to the switch. The entire log may be viewed at any time using the **show qos log** command.

Examples

```
-> qos log console
-> qos no log console
```

Release History

Release 5.1; command was introduced.

Related Commands

qos log lines	Configures the number of lines in the QoS log.
show qos log	Displays the log of QoS events.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigLogConsole
```

qos log lines

Configures the number of lines in the QoS log.

qos log lines *lines*

Syntax Definitions

lines	The number of lines included in the QoS log. A value of zero turns off logging to the console. The range is 0–512.

Defaults

parameter	default
lines	256

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- To turn off logging, enter 0 for the number of log lines. (Note that error messages will still be logged.)
- If you change the number of log lines, you may clear all messages in the QoS log. To avoid clearing all messages in the log, enter the **qos log lines** command in the **boot.cfg** file. The log length will be changed at the next reboot.

Examples

```
-> qos log lines 5
-> qos log lines 0
```

Release History

Release 5.1; command was introduced.

Related Commands

show qos log	Displays the log of QoS events.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigLogLines
```

qos log level

Configures the level of log detail.

qos log level *level*

qos no log level

Syntax Definitions

level	The level of log detail, in the range from 1 (least detail) to 9 (most detail).

Defaults

parameter	default
level	6

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **qos debug** command to change the type of debugging messages that are logged. The **qos log level** command configures the level of detail for these messages.
- If the **qos debug** command is not configured to log any kind of information (this is the default), the **qos log level** command has no effect.
- To log fatal errors only, set the log level to 0.
- Note that a high log level value will impact the performance of the switch.

Examples

```
-> qos log level 4
-> qos log level 0
```

Release History

Release 5.1; command was introduced.

Related Commands

qos log lines	Configures the number of lines in the QoS log.
debug qos	Configures the type of QoS events that will be displayed in the QoS log.
show qos log	Displays the log of QoS events.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigLogLevel
```

qos classifyl3 bridged

Configures the switch to classify bridged traffic using Layer 3 information.

qos classifyl3 bridged

qos no classifyl3 bridged

Syntax Definitions

N/A

Defaults

By default, the switch does not classify bridged traffic as Layer 3.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If this option is enabled, switch performance may be slower.
- Configuring the switch to classify bridged traffic as Layer 3 may result in bridged and routed traffic to the same destination.
- Use the **no** form of the command to set the switch to its default (no classification of bridged traffic as Layer 3).
- When this option is enabled, policy conditions for Layer 3 traffic will be applied to Layer 2 traffic.
- On the OmniSwitch 6624/6648, when **qos classifyl3 bridged** is enabled, Layer 2 ACLs are disabled for IP traffic, and all IP traffic is switched at Layer 3. If the default routed disposition is set to **deny** or **drop** when this command is enabled on the OmniSwitch 6624/6648, all bridged IP packets will be dropped.

Examples

```
-> qos classifyl3 bridged
-> qos no classifyl3 bridged
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a QoS policy condition. The condition determines what parameters the switch uses to classify incoming flows.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigClassifyl3Bridged
   alaQoSConfigAppliedClassifyl3Bridged
```

qos classify fragments

Configures the switch to classify fragments. Normally only the first fragment of a flow is classified. This command forces each fragment to be classified.

qos classify fragments

qos no classify fragments

Syntax Definitions

N/A

Defaults

By default, fragments are not classified.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use this command to force the switch to classify each fragment in the flow. This ensures that each fragment gets the correct QoS; however, it takes up a lot of time and memory on the switch.
- Typically only the first fragment of a flow has enough information for the switch to classify the flow and make a policy decision; when the switch classifies fragments other than the first fragment, it remembers which packet the fragment belongs to and uses the classification from the first fragment.

Examples

```
-> qos classify fragments
-> qos no classify fragments
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
qos fragment timeout	Configures the timeout for packet fragments.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigClassifyFragments
   alaQoSConfigAppliedClassifyFragments
```

qos flow timeout

Configures the timeout for an entry in the flow table. An entry is made in the table whenever a flow is received on the switch. If no packets in the flow are received before the timeout expires, the switch removes the flow entry from the table. Because flow tables take up switch memory, the timeout prevents inactive flow entries from using switch memory.

qos flow timeout *seconds*

Syntax Definitions

seconds	The time, in seconds, that the switch will wait for all packets of a flow to arrive. If the time expires, the switch drops the flow. The range is 2–3600.

Defaults

parameter	default
seconds	300

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Typically the timeout value does not need to be changed.

Examples

```
-> qos flow timeout 20
-> qos no flow timeout
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigFlowTimeout
   alaQoSConfigAppliedFlowTimeout
```

qos fragment timeout

Configures the timeout for packet fragments. *Not supported in the current release*.

qos fragment timeout *seconds*

Syntax Definitions

seconds	The time, in seconds, that the switch will wait for all fragments of a packet to arrive. If the time expires, the switch drops the packet. The range is 2–300.

Defaults

parameter	default
seconds	10

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- This command only takes effect when fragment classification is enabled through the **qos classify fragments** command.
- Typically the timeout does not need to be configured.

Examples

```
-> qos fragment timeout 20
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
qos classify fragments	Configures the switch to classify fragments. Normally only the first fragment of a flow is classified. This command forces each fragment to be classified.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigFragmentTimeout
   alaQoSConfigAppliedFragmentTimeout
```

qos reflexive timeout

Configures the amount of time the switch will wait for anticipated or reflexive flows. Reflexive flows are typically reply packets received back from a TCP session or filtered IP session.

qos reflexive timeout *seconds*

qos no reflexive timeout

Syntax Definitions

seconds	The amount of time the switch waits to receive reply packets, in seconds. If reply packets are not received, the flow is dropped from the switch. The range is 10–3000.

Defaults

parameter	default
seconds	120

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

This command only takes effect if there are policies that have been defined as reflexive using the **policy rule** command.

Examples

```
-> qos reflexive timeout 120
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy rule	Configures a policy rule on the switch. A rule is made up of a condition (for classifying incoming traffic) and an action (to be applied to outgoing traffic).
qos fragment timeout	Configures the timeout for packet fragments.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigReflexiveTimeout
   alaQoSConfigAppliedReflexiveTimeout
```

qos nat timeout

Configures the amount of time the switch will wait for traffic from an address translation flow.

qos nat timeout *seconds*

Syntax Definitions

seconds	The amount of time the switch will wait for traffic from an address translation flow before it drops the connection. The range is 10–10000.

Defaults

parameter	default
seconds	3600

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

This command only takes effect if there are policies that have been defined as network translation policies using the **policy action** command keywords **source rewrite**, **destination rewrite**, **source rewrite group**, or **destination rewrite group**.

Examples

```
-> qos nat timeout 500
```

Release History

Release 5.1; command was introduced.

Related Commands

policy action source rewrite ip	Configures a source IP address that should be used for outgoing flows associated with the specified action.
policy action source rewrite network group	Specifies a source network group that should be used for outgoing flows associated with the specified action.
policy action destination rewrite ip	Configures a destination IP address that should be used for outgoing flows associated with the specified action.
policy action destination rewrite network group	Configures a destination network group that should be used for outgoing flows associated with the specified action.
qos apply	Applies configured QoS and policy settings to the current configuration.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigNatTimeout
   alaQoSConfigAppliedNatTimeout
```

qos default bridged disposition

Configures the default disposition for bridged traffic (Layer 2) that comes into the switch and does not match any policies.

qos default bridged disposition {accept | deny | drop}

Syntax Definitions

accept	Specifies that the switch should accept the flow.
drop	Specifies that the switch should silently drop the flow.
deny	Specifies that the switch should drop the flow and issue an ICMP message indicating the flow was dropped for administrative reasons. Currently this option will provide the same result as **drop**; that is, the flow is silently dropped.

Defaults

By default, the disposition for flows that do match any policies is **accept**.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The disposition for particular flows may be configured through the **policy action disposition** command. The disposition for a particular flow will override the global setting.
- Typically, when configuring IP filtering rules, the global default disposition should be set to **deny**. Filtering rules may then be configured to allow particular types of traffic through the switch.
- If you set the bridged disposition to deny or drop, and you configure rules to allow bridged traffic, each type of allowed traffic must have two rules, one for source and one for destination.

Examples

```
-> qos default bridged disposition deny
```

Release History

Release 5.1; command was introduced.

Related Commands

policy action disposition	Configures a disposition for a policy action.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigDefaultBridgedDisposition
   alaQoSConfigAppliedDefaultBridgedDisposition
```

qos default routed disposition

Configures the default disposition for routed traffic (Layer 3) that comes into the switch and does not match any policies.

qos default routed disposition {accept | deny | drop}

Syntax Definitions

accept	Specifies that the switch should accept the flow.
drop	Specifies that the switch should silently drop the flow.
deny	Specifies that the switch should drop the flow and issue an ICMP message indicating the flow was dropped for administrative reasons. Currently this option will provide the same result as **drop**; that is, the flow is silently dropped.

Defaults

By default, the disposition for flows that do match any policies is **accept**.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The disposition for particular flows may be configured through the **policy action disposition** command. The disposition for a particular flow will override the global setting.
- Typically, when configuring IP filtering rules, the global default disposition should be set to **deny**. Filtering rules may then be configured to allow particular types of traffic through the switch.

Examples

```
-> qos default routed disposition deny
```

Release History

Release 5.1; command was introduced.

Related Commands

policy action disposition	Configures a disposition for a policy action.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigRoutedDefaultDisposition
   alaQoSConfigAppliedRoutedDefaultDisposition
```

qos default multicast disposition

Configures the default disposition for multicast flows coming into the switch that do not match any policies.

qos default multicast disposition {accept | deny | drop}

Syntax Definitions

accept	Specifies that the switch should accept the flow.
drop	Specifies that the switch should silently drop the flow.
deny	Specifies that the switch should drop the flow and issue an ICMP message indicating the flow was dropped for administrative reasons. Currently this option will provide the same result as **drop**; that is, the flow is silently dropped.

Defaults

By default, multicast flows that do not match policies are accepted on the switch.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **policy action multicast** command to specify the disposition for a particular action associated with a multicast condition. The disposition for a particular action will override the global setting.

Examples

```
-> qos default multicast disposition deny
```

Release History

Release 5.1; command was introduced.

Related Commands

policy action disposition	Configures a disposition for a policy action.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigDefaultMulticastDisposition
   alaQoSConfigAppliedDefaultMulticastDisposition
```

qos stats interval

Configures how often the switch polls network interfaces for statistics about QoS events.

qos stats interval *seconds*

Syntax Definitions

seconds	The number of seconds before the switch polls network interfaces for statistics. The range is 10–3600.

Defaults

parameter	default
seconds	60

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Change the statistics interval to a smaller interval if you want to monitor QoS events.
- Change the statistics interval to a larger interval if you want to free some switch memory.

Examples

```
-> qos stats interval 30
```

Release History

Release 5.1; command was introduced.

Related Commands

show qos statistics	Displays statistics about the QoS configuration

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigStatsInterval
```

debug qos

Configures the type of QoS events that will be displayed in the QoS log.

debug qos [info] [config] [rule] [main] [route] [hre] [port] [msg] [sl] [ioctl] [mem] [cam] [mapper] [flows] [queue] [slot] [l2] [l3] [classifier] [nat] [sem] [pm] [ingress] [egress] [rsvp] [balance] [nimsg]

debug no qos

debug no qos [info] [config] [rule] [main] [route] [hre] [port] [msg] [sl] [ioctl] [mem] [cam] [mapper] [flows] [queue] [slot] [l2] [l3] [classifier] [nat] [sem] [pm] [ingress] [egress] [rsvp] [balance] [nimsg]

Syntax Definitions

flows	Logs events for flows on the switch.
queue	Logs events for queues created and destroyed on the switch.
rule	Logs events for rules configured on the switch.
l2	Logs Layer 2 QoS events on the switch.
l3	Logs Layer 3 QoS events on the switch.
nat	Logs events for Network Address Translation policies. *Not supported for the OmniSwitch 6624/6648*.
port	Logs events related to QoS ports.
msg	Logs QoS messages.
classifier	Logs information whenever the switch classifies a flow; more details are provided if the log level is higher.
info	Logs basic information about the switch
config	Logs information about the global configuration.
main	Logs information about basic program interfaces.
route	Logs information about routing.
hre	Logs information about hardware route programming.
sl	Logs information about source learning.
mem	Logs information about memory.
cam	Logs information about CAM operations.
mapper	Logs information about mapping queues.
slot	Logs events related to slots.
sem	Logs information about semaphore, process locking.
pm	Logs events related to the Policy Manager.
ingress	Logs information about packets arriving on the switch.

egress	Logs information about packets leaving the switch.
rsvp	Logs information about RSVP flows. *Currently not supported*.
balance	Logs information about flows that are part of a load balancing cluster. *Not supported for the OmniSwitch 6624/6648.*
nimsg	Logs information about QoS interfaces.

Defaults

By default basic information messages are logged (**info**). Error messages are always logged.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use this command to troubleshoot QoS events on the switch.
- Use the **no** form of the command to change the type of messages that will be logged or to return debugging to its default state.

Examples

```
-> debug qos flows queue
-> qos debug no flows no queue
-> debug no qos
```

Release History

Release 5.1; command was introduced.

Related Commands

qos forward log	Enables the switch to send events to the PolicyView application in real time.
qos log lines	Configures the number of lines in the QoS log.
show qos log	Displays the log of QoS events.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigDebug
```

debug qos internal

Displays debugging information for QoS internal to the switch.

debug qos internal [slice *slot/slice***] [flow] [queue] [port] [l2tree] [l3tree] [vector] [pending] [verbose] [mapper] [pool] [log] [pingonly | nopingonly]**

Syntax Definitions

slot/slice	The slot number and slice for which you want to view debugging information. A *slice* is a logical section of hardware that corresponds to particular ports on a network interface module. On the OmniSwitch 7700/7800, each interface has one slice (slice 0). On the OmniSwitch 8800, each interface may have up to 4 slices (slices 0 to 3).
flow	Displays information about QoS flows.
queue	Displays information about QoS queues.
port	Displays information about QoS ports.
l2tree	Displays information about Layer 2 flows.
l3tree	Displays information about Layer 3 flows.
vector	Displays information about vectors.
pending	Displays information about pending QoS objects.
verbose	Sets the output to verbose mode for more detailed information.
mapper	Displays information about QoS mapping flows to queues.
pool	Displays information about the buffer pool.
log	Displays information about QoS information that is logged.
pingonly	On an OmniSwitch 6624/6648, specifies that any policies configured with an ICMP protocol condition apply only to ICMP echo-requests. On the OmniSwitch 7700/7800/8800, specifies that any policies configured with an ICMP protocol condition apply only to ICMP echo-requests and echo-replies.
nopingonly	Configures the switch so that any policies configured with an ICMP protocol condition apply to any ICMP packets.

Defaults

Debugging is disabled by default.

parameter	default
pingonly | nopingonly	**nopingonly**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **debug qos** command to set the level of log detail in the QoS log.

Examples

```
-> debug qos internal "verbose log"
```

Release History

Release 5.1; command was introduced.

Related Commands

debug qos	Configures the type of QoS events that will be displayed in the QoS log.
policy condition ip protocol	Configures an IP protocol for a policy condition.

MIB Objects

N/A

qos clear log

Clears messages in the current QoS log.

qos clear log

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This command is useful for clearing messages from a large log file so that the file is easier to view. Logs can get large if invalid rules are configured on the switch, or if a lot of QoS events have taken place. Clearing the log makes the file easier to manage.

Examples

```
-> qos clear log
```

Release History

Release 5.1; command was introduced.

Related Commands

qos log lines	Configures the number of lines in the QoS log.
debug qos	Configures the type of QoS events that will be displayed in the QoS log.
show qos log	Displays the log of QoS events.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigClearLog
```

qos apply

Applies configured global QoS and policy settings to the current configuration (changes will be active and stored in flash).

qos apply

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command is required to activate *all* QoS and policy commands. This is the only command that causes current changes to be written to flash.
- Rules are configured through the **policy rule** command, but are not active on the switch until you enter **qos apply**.

Examples

```
-> qos apply
```

Release History

Release 5.1; command was introduced.

Related Commands

qos revert	Removes any policies configured through policy rule but not applied to the current configuration through the **qos apply** command.
qos reset	Resets the QoS configuration to its default values.
qos flush	Deletes all pending policy information.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigApply
```

qos revert

Deletes any QoS configuration that has not been applied to the configuration through the **qos apply** command.

qos revert

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use this command to remove currently configured policies that have not yet been activated through the **qos apply** command.

Examples

```
-> qos revert
```

Release History

Release 5.1; command was introduced.

Related Commands

policy rule	Configures a policy rule and saves it to the current configuration but does not make it active on the switch.
qos apply	Applies all QoS settings configured on the switch to the current configuration.
qos reset	Resets the QoS configuration to its defaults.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigRevert
```

qos flush

Deletes all pending policy information. This command is different from **qos revert**, which returns the pending policy configuration to its last applied settings.

qos flush

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If you enter this command, the pending policy configuration is completely erased. If you then enter **qos apply**, the erased configuration *overwrites the applied policies and you will erase all of your policy configuration.*

Note. Do not use this command unless you want to erase all of your policy configuration and start configuring new policies.

- Use the **qos revert** command to return the pending policy configuration to its last applied value.
- Policy configuration includes the following commands:

base commands	
policy rule	**policy mac group**
policy network group	**policy port group**
policy service	**policy condition**
policy service group	**policy action**

Examples

```
-> qos flush
```

Release History

Release 5.1; command was introduced.

Related Commands

qos revert	Deletes any QoS configuration that has not been applied to the configuration through the **qos apply** command.
qos apply	Applies configured global QoS and policy settings to the current configuration (changes will be active and stored in flash).
policy server flush	Removes all cached LDAP policy data from the switch.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigFlush
```

qos reset

Resets the QoS configuration to its defaults.

qos reset

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use this command to reset QoS configuration that has not yet been applied through the **qos apply** command. The parameters are reset to their defaults.

Examples

```
-> qos reset
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies all QoS settings configured on the switch to the current configuration.
qos revert	Deletes any QoS configuration that has not been applied to the configuration through the **qos apply** command.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigReset
```

qos stats reset

Resets QoS statistic counters to zero.

qos stats reset

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use this command to reset global QoS statistics to zero. Statistics may be displayed with the **show qos statistics** command.

Examples

```
-> qos stats reset
```

Release History

Release 5.1; command was introduced.

Related Commands

show qos statistics	Displays statistics about the QoS configuration.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigStatsReset
```

policy rule

Configures a policy rule on the switch. A rule is made up of a condition (for classifying incoming traffic) and an action (to be applied to outgoing traffic).

policy rule *rule_name* **[enable | disable] [precedence** *precedence***] [condition** *condition***] [action** *action***] [reflexive] [save] [log]**

no policy rule *rule_name*

policy rule *rule_name* **[no reflexive] [no save] [no log]**

Syntax Definitions

rule_name	The name of the policy rule, any alphanumeric string.
enable	Enables the policy rule.
disable	Disables the policy rule.
precedence	The precedence value in the range 0–65535. This value determines the order in which rules are searched for a matching condition. A higher number indicates higher precedence. Typically the range 30000–65535 is reserved for PolicyView.
condition	The condition name that is associated with this rule. Conditions are configured through the **policy condition** command.
action	The name of the action that is associated with this rule. Actions are configured through the **policy action** command.
reflexive	Configures the policy rule to be reflexive, that is, it applies to flows with the reverse source and destination IP addresses and source and destination ports. Used for Access Control Lists (ACLs).
save	Marks the policy rule so that it may be captured as part of the switch configuration.
log	Configures the switch to log messages about specific flows coming into the switch that match this policy rule.

Defaults

By default, rules are not reflexive, but they are saved to the configuration.

parameter	default
enable | disable	**enable**
precedence	0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Any rule configured through this command is not active on the switch until the **qos apply** command is issued.
- A policy rule configured through the PolicyView application may not be edited in the CLI. You may, however, create a rule using the CLI with a higher precedence that will override a rule created through PolicyView.
- Use the **no** form of the command to remove the rule from the configuration. The change will not take effect, however, until the **qos apply** command is issued.
- When a flow comes into the switch, the switch examines Layer 2 source policies first; if no match is found, it examines Layer 2 destination policies; if no match is found it then examines Layer 3 policies. The precedence value only applies within the group of the same type of rules.
- If multiple rules (of the same type; that is, Layer 2 source, Layer 2 destination, or Layer 3) are configured with the same precedence, the switch evaluates the rules in the order they were created.
- The **save** option marks the policy rule so that the rule will be captured in an ASCII text file (using the **configuration snapshot** command), saved to the working directory after the **write memory** command or **copy running-config working** command is entered, or saved after a reboot. Rules are saved by default. If **no save** is entered for the rule, the policy rule will not be written to the configuration. The **save** option should be disabled only if you want to use a policy rule temporarily.
- If the **configuration snapshot** command is entered after the **policy rule** command is configured, the resulting ASCII file will include the following additional syntax for the **policy rule** command:

  from {cli | ldap | blt}

  This syntax indicates how the rule was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in rule, this setting is not configurable.
- The **log** option is useful for determining the source of attacks on the switch firewall.

Examples

```
-> policy rule rule2 precedence 65535
-> no policy rule rule2
-> policy rule rule2 no precedence
```

Release History

Release 5.1; command was introduced.

Related Commands

policy condition	Configures condition parameters.
policy action	Configures action parameters.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy rule	Displays information for policy rules configured on the switch.
show active policy rule	Displays only those policy rules that are currently being enforced on the switch.

MIB Objects

```
alaQoSRuleTable
   alaQoSRuleName
   alaQoSRuleEnabled
   alaQoSRuleSource
   alaQoSRulePrecedence
   alaQoSRuleCondition
   alaQoSRuleAction
   alaQoSRuleReflexive
   alaQoSRuleSave
   alaQoSRuleLog
alaQoSAppliedRuleTable
   alaQoSAppliedRuleName
   alaQoSAppliedRuleEnabled
   alaQoSAppliedRuleSource
   alaQoSAppliedRulePrecedence
   alaQoSAppliedRuleCondition
   alaQoSAppliedRuleAction
   alaQoSAppliedRuleReflexive
   alaQoSAppliedRuleSave
   alaQoSAppliedRuleLog
```

policy network group

Configures a network group name and its associated IP addresses. The group may be used as part of a policy condition. The action associated with any policy using the condition will be applied to all members of the network group.

policy network group *net_group ip_address* **[mask** *net_mask***] [***ip_address2* **[mask** *net_mask2***]...]**

no policy network group *net_group*

policy network group *net_group* **no** *ip_address* **[mask** *netmask***] [***ip_address2* **[mask** *net_mask2***]...]**

Syntax Definitions

net_group	The name of the network group (up to 31 alphanumeric characters).
ip_address	An IP address included in the network group.
net_mask	The mask for the IP address. If no mask is entered, the IP address is assumed to be a host address.
ip_address2	Optional. Another IP address to be included in the network group. Multiple IP addresses may be configured for a network group. Separate each address/mask combination with a space.
net_mask2	Optional mask for the IP address. If no mask is entered, the natural mask for the address will be used.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use this command to configure a group of IP addresses to which you want to apply QoS rules. Rather than create a condition for each IP address, group the addresses together. Use the **policy condition** command to associate a condition with the network group.
- Use the **no** form of the command to remove a network group from the configuration, or to remove an IP address from a network group.
- If the **snapshot** command is entered after the **policy network group** command is configured, the resulting ASCII file will include the following additional syntax for the **policy network group** command:

  from {cli | ldap | blt}

  This syntax indicates how the network group was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in network group, this setting is not configurable.

Examples

```
-> policy network group webgroup1 10.10.12.5 10.50.3.1
-> policy network group webgroup1 no 10.10.12.5
-> no policy network group webgroup1
```

Release History

Release 5.1; command was introduced.

Related Commands

policy condition	Configures a policy condition. A network group may be configured as part of a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy network group	Displays information for policy network groups.

MIB Objects

```
alaQoSNetworkGroupsTable
   alaQoSNetworkGroupsName
   alaQoSNetworkGroupsSource
alaQoSAppliedNetworkGroupsTable
   alaQoSAppliedNetworkGroupsName
   alaQoSAppliedNetworkGroupsSource
alaQoSNetworkGroupTable
   alaQoSNetworkGroupIpAddr
   alaQoSNetworkGroupsIpMask
alaQoSAppliedNetworkGroupTable
   alaQoSAppliedNetworkGroupIpAddr
   alaQoSAppliedNetworkGroupsIpMask
```

policy service group

Configures a service group and its associated services. The group may be used as part of a policy condition. The action associated with any policy using the condition will be applied to all members of the service group.

policy service group *service_group service_name1* **[***service_name2...***]**

no policy service group *service_group*

policy service group *service_group* **no** *service_name1* **[***service_name2...***]**

Syntax Definitions

service_group	The name of the service group (up to 31 alphanumeric characters).
service_name1	The service name is configured through the **policy service** command and includes information about protocol, source port, and destination port.
service_name2...	Optional. Additional service names may be configured for a service group. Separate each service name with a space.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use this command to configure a group of services to which you want to apply QoS rules. Rather than create a condition for each service, group services together. Use the **policy condition** command to associate a condition with the service group.
- Use the **no** form of the command to remove a service group from the configuration, or to remove a service from a service group.
- To drop packets destined to specific TCP and UDP ports, create port services for the traffic that you want dropped and add these services to a service group called DropServices. Then create a condition for this service group and a source port group, which can then be used in a deny rule. Refer to the switch *Network Configuration Guide* for more information about ACL security enhancements.
- If the **snapshot** command is entered after the **policy service group** command is configured, the resulting ASCII file will include the following additional syntax for the **policy service group** command:

  from {cli | ldap | blt}

  This syntax indicates how the service group was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in service group, this setting is not configurable.

Examples

```
-> policy service group servgroup2 telnet ftp
-> policy service group servgroup2 no telnet
-> no policy service group servgroup2
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy service	Configures a service that may be used as part of a policy service group.
policy condition	Configures a policy condition. A network group may be configured as part of a policy condition.
show policy service group	Displays information for policy service groups.

MIB Objects

```
alaQoSServiceGroupsTable
   alaQoSServiceGroupsName
   alaQoSServiceGroupsSource
alaQoSAppliedServiceGroupsTable
   alaQoSAppliedServiceGroupsName
   alaQoSAppliedServiceGroupsSource
alaQoSServiceGroupTable
   alaQoSServiceGroupServiceName
alaQoSAppliedServiceGroupTable
   alaQoSAppliedServiceGroupServiceName
```

policy mac group

Configures a MAC group and its associated MAC addresses. The group may be used as part of a policy condition. The action associated with any policy using the condition will be applied to all members of the MAC group.

policy mac group *mac_group mac_address* **[mask** *mac_mask***] [***mac_address2* **[mask** *mac_mask2***]...]**

no policy mac group *mac_group*

policy mac group *mac_group* **no** *mac_address* **[mask** *mac_mask***] [***mac_address2* **[mask** *mac_mask2***]...]**

Syntax Definitions

mac_group	The name of the MAC group (up to 31 alphanumeric characters).
mac_address	The MAC address associated with the group (for example, 00:20:da:05:f6:23).
mac_mask	The mask of the MAC address, used to identify which bytes in the MAC address are significant when comparing the MAC address in the received frame with the MAC address in the policy condition. If no mask is specified, the switch automatically uses ff:ff:ff:ff:ff:ff.
mac_address2	Optional. Additional MAC addresses may be configured for a MAC group. Separate each address with a space.
mac_mask2	The mask of an additional MAC address, used to identify which bytes in the MAC address are significant when comparing the MAC address in the received frame with the MAC address in the policy condition. If no mask is specified, the switch automatically uses ff:ff:ff:ff:ff:ff.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use this command to configure a group of source or destination MAC addresses to which you want to apply QoS rules. Rather than create a condition for each MAC address, group MAC addresses together. Use the **policy condition** command to associate a condition with the MAC group.
- Use the **no** form of the command to remove a MAC group from the configuration, or to remove a MAC address from a MAC group.

- If the **snapshot** command is entered after the **policy map group** command is configured, the resulting ASCII file will include the following additional syntax for the **policy map group** command:

  from {cli | ldap | blt}

  This syntax indicates how the map group was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.

Examples

```
-> policy mac group mac_group1 00:20:da:05:f6:23 00:20:da:05:f6:24
-> no policy mac group mac_group1
```

Release History

Release 5.1; command was introduced.

Related Commands

policy condition	Configures a policy condition. A MAC group may be configured as part of a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy mac group	Displays information about policy MAC groups.

MIB Objects

```
alaQoSMACGroupsTable
   alaQoSMACGroupsName
   alaQoSMACGroupsSource
alaQoSAppliedMACGroupsTable
   alaQoSAppliedMACGroupsName
   alaQoSAppliedMACGroupsSource
alaQoSMACGroupTable
   alaQoSMACGroupMacAddr
   alaQoSMACGroupMacMask
alaQoSAppliedMACGroupTable
   alaQoSAppliedMACGroupMacAddr
   alaQoSAppliedMACGroupMacMask
```

policy port group

Configures a port group and its associated slot and port numbers. A port group may be attached to a policy condition. The action associated with that policy will be applied to all members of the port group.

policy port group *group_name slot/port***[-***port***] [***slot/port***[-***port***]...]**

no policy port group *group_name*

policy port group *group_name* **no** *slot/port***[-***port***] [***slot/port***[-***port***]...]**

Syntax Definitions

group_name	The name of the port group (up to 31 alphanumeric characters).
*slot/port***[-***port***]**	The slot and port (or port range) to be included in the group. At least one slot/port combination must be specified. Additional combinations may be included in the group; each combination should be separated by a space.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use this command to configure a group of ports to which you want to apply QoS rules. Rather than create a condition for each port, group ports together. Use the **policy condition** command to associate a condition with the port group.
- Use the **no** form of the command to remove a port group from the configuration, or to remove a slot/port from a port group.
- If a range of ports is specified using the syntax *slot/port-port* (i.e., 2/1-8), a single port within that range cannot be removed on its own. The entire range must be deleted as it was entered.
- On the OmniSwitch 7700/7800/8800, when a port group is used as part of a policy rule and a policy action specifies a maximum bandwidth, each interface in the port group will be allowed the maximum bandwidth. On the OmniSwitch 6624/6648, when a port group is used as part of a policy rule and a policy action specifies a maximum bandwidth, the maximum bandwidth is divided equally among the number of active ports in the port group (100 percent for one active port; 50 percent each for two active ports; 25 percent each for four active ports, etc.)
- To prevent IP source address spoofing on an OmniSwitch 7700/7800/8800, add ports to to the port group called UserPorts. This port group does not need to be used in a condition or rule to be effected on flows and only applies to routed traffic. Ports added to the UserPorts group will block spoofed traffc while still allowing normal traffic on the port. Refer to the switch *Network Configuration Guide* for more information about ACL security enhancements.

- If the **snapshot** command is entered after the **policy port group** command is configured, the resulting ASCII file will include the following additional syntax for the **policy port group** command:

  from {cli | ldap | blt}

  This syntax indicates how the port group was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.

Examples

```
-> policy port group port_group4 3/1-2 4/3 5/4
-> policy port group port_group4 no 3/1-2
```

Release History

Release 5.1; command was introduced.

Related Commands

policy condition	Configures a policy condition. A port group may be configured as part of a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.
policy action maximum bandwidth	Configures a maximum bandwidth value for a policy action.
show policy port group	Displays information about policy port groups.

MIB Objects

```
alaQoSPortGroupsTable
   alaQoSPortGroupsName
   alaQoSPortGroupsSource
alaQoSAppliedPortGroupsTable
   alaQoSAppliedPortGroupsName
   alaQoSAppliedPortGroupsSource
alaPortGroupTable
   alaQoSPortGroupSlot
   alaQoSPortGroupPort
   alaQoSPortGroupPortEnd
alaAppliedPortGroupTable
   alaQoSAppliedPortGroupSlot
   alaQoSAppliedPortGroupPort
   alaQoSAppliedPortGroupPortEnd
```

policy service

Configures a service that may be used as part of a policy service group or included as part of a policy condition. A service is a source and/or destination TCP or UDP port or port range.

This overview section describes the base command. *At least one option must be configured with the base command.* Some options may be used in combination; some options are shortcuts for keyword combinations (see the Usage Guidelines). Options are described as separate commands. See the command descriptions and usage guidelines for valid combinations.

Use the **no** form for keywords to remove a parameter from a service.

policy service *service_name*
[protocol *protocol***]**
[source ip port *port***[-***port***]]**
[destination ip port *port***[-***port***]]**
[source tcp port *port***[-***port***]]**
[destination tcp port *port***[-***port***]]**
[source udp port *port***[-***port***]]**
[destination udp port *port***[-***port***]]**

no policy service *service_name*

Syntax Definitions

service_name	The name of the service (up to 31 alphanumeric characters).
protocol	The protocol associated with the service. The range of values is 0–255. Currently a value of 6 (for TCP) or 17 (for UDP) is supported. This value must be specified for **source ip port** or **destination ip port**; it cannot be specified for **source tcp port**, **destination tcp port**, **source udp port**, or **destination udp port**.
port	The well-known port number (or port range) for the desired service. For example, the port number for Telnet is 23. A port range should be separated by a hyphen (for example, **22-23**).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a service from the configuration, or to remove parameters from a particular service. Note that at least one parameter must be associated with a service.

- The command options offer alternate ways of configuring TCP or UDP ports for a service. Note that port types (TCP or UDP) cannot be mixed in the same service. The following table shows how the keywords are used:

To configure:	Use keywords:	Notes
TCP or UDP ports for a service	**protocol** **source ip port** **destination ip port**	*The protocol must be specified with at least one source or destination port.*
TCP ports for a service	**source tcp port** **destination tcp port**	*Keywords may be used in combination.*
UDP ports for a service	**source udp port** **destination udp port**	*Keywords may be used in combination.*

- If the **snapshot** command is entered after the **policy service** command is configured, the resulting ASCII file will include the following additional syntax for the **policy service** command:

  from {cli | ldap | blt}

  This syntax indicates how the service was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.

Examples

The following two commands show two different ways of configuring the same service:

```
-> policy service telnet2 protocol 6 destination ip port 23
-> policy service telnet3 destination tcp port 23
```

Release History

Release 5.1; command was introduced.

Related Commands

policy service group	Configures a policy service group, which is made up of policy services.
policy condition	Creates a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy service	Displays information about policy services configured on the switch.

MIB Objects

alaQoSServiceTable

- alaQoSServiceName
- alaQoSServiceSource
- alaQoSServiceIpProtocol
- alaQoSServiceSourceIpPort
- alaQoSServiceSourceIpPortEnd
- alaQoSServiceDestinationIpPort
- alaQoSServiceDestinationIpPortEnd
- alaQoSServiceSourceTcpPort
- alaQoSServiceSourceTcpPortEnd
- alaQoSServiceDestinationTcpPort
- alaQoSServiceDestinationTcpPortEnd
- alaQoSServiceSourceUdpPort
- alaQoSServiceSourceUdpPortEnd
- alaQoSServiceDestinationUdpPort
- alaQoSServiceDestinationUdpPortEnd

alaQoSAppliedServiceTable

- alaQoSAppliedServiceName
- alaQoSAppliedServiceSource
- alaQoSAppliedServiceIpProtocol
- alaQoSAppliedSourceIpPort
- alaQoSAppliedSourceIpPortEnd
- alaQoSAppliedServiceDestinationIpPort
- alaQoSAppliedServiceDestinationIpPortEnd
- alaQoSAppliedSourceTcpPort
- alaQoSAppliedSourceTcpPortEnd
- alaQoSAppliedServiceDestinationTcpPort
- alaQoSAppliedServiceDestinationTcpPortEnd
- alaQoSAppliedSourceUdpPort
- alaQoSAppliedSourceUdpPortEnd
- alaQoSAppliedServiceDestinationUdpPort
- alaQoSAppliedServiceDestinationUdpPortEnd

policy service protocol

Configures a service with a protocol and IP port or port range that may be used as part of a policy service group or included as part of a policy condition.

policy service *service_name* **protocol** *protocol* **{[source ip port** *port***[-***port***]] [destination ip port** *port***[-***port***]]}**

no policy service *service_name*

policy service *service_name* **[no source ip port] [no destination ip port]**

Syntax Definitions

service_name	The name of the service (up to 31 alphanumeric characters).
protocol	The protocol associated with the service. The range of values is 0–255. Currently a value of 6 (for TCP) or 17 (for UDP) is supported.
port	The well-known port number (or port range) for the desired service. For example, the port number for Telnet is 23. A port range should be separated by a hyphen (for example, **22-23**).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a service from the configuration, or to remove parameters from a particular service. (A protocol value cannot be removed from a service.)
- Shortcut commands for the **policy service protocol** command include the following: **policy service source tcp port**, **policy service destination tcp port**, **policy service source udp port**, and **policy service destination udp port**.
- If the **snapshot** command is entered after the **policy service** command is configured, the resulting ASCII file will include the following additional syntax for the **policy service** command:

  from {cli | ldap | blt}

  This syntax indicates how the service was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.

Examples

```
-> policy service telnet2 protocol 6 destination ip port 23 source ip port 22
-> policy service telnet2 no source ip port
```

Release History

Release 5.1; command was introduced.

Related Commands

policy service group	Configures a policy service group, which is made up of policy services.
policy condition	Creates a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy service	Displays information about policy services configured on the switch.

MIB Objects

```
alaQoSServiceTable
   alaQoSServiceName
   alaQoSServiceSource
   alaQoSServiceIpProtocol
   alaQoSServiceSourceIpPort
   alaQoSServiceSourceIpPortEnd
   alaQoSServiceDestinationIpPort
   alaQoSServiceDestinationIpPortEnd
alaQoSAppliedServiceTable
   alaQoSAppliedServiceName
   alaQoSAppliedServiceSource
   alaQoSAppliedServiceIpProtocol
   alaQoSAppliedSourceIpPort
   alaQoSAppliedSourceIpPortEnd
   alaQoSAppliedServiceDestinationIpPort
   alaQoSAppliedServiceDestinationIpPortEnd
```

policy service source tcp port

Configures a service with a source TCP port or port range that may be used as part of a policy service group or included as part of a policy condition.

policy service *service_name* **source tcp port** *port***[-***port***]**

no policy service *service_name*

policy service *service_name* **no source tcp port**

Syntax Definitions

service_name	The name of the service (up to 31 alphanumeric characters).
port	The well-known port number (or port range) for the desired TCP service. For example, the port number for Telnet is 23. A port range should be separated by a hyphen (for example, **22-23**).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command is a shortcut for the **policy service protocol** command.
- Use the **no** form of the command to remove a service from the configuration, or to remove parameters from a particular service. Note that at least one parameter must be associated with a service.
- Ports associated with a particular service must all be of the same type. (The **destination tcp port** keyword may be used with this command; other keywords for the command are not allowed.)
- If the **snapshot** command is entered after the **policy service** command is configured, the resulting ASCII file will include the following additional syntax for the **policy service** command:

  from {cli | ldap | blt}

  This syntax indicates how the service was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.

Examples

```
-> policy service serv_5 source tcp port 21-22
```

Release History

Release 5.1; command was introduced.

Related Commands

policy service group	Configures a policy service group, which is made up of policy services.
policy condition	Creates a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy service	Displays information about policy services configured on the switch.

MIB Objects

```
alaQoSServiceTable
   alaQoSServiceName
   alaQoSServiceSource
   alaQoSServiceSourceTcpPort
   alaQoSServiceSourceTcpPortEnd
alaQoSAppliedServiceTable
   alaQoSAppliedServiceName
   alaQoSAppliedServiceSource
   alaQoSAppliedSourceTcpPort
   alaQoSAppliedSourceTcpPortEnd
```

policy service destination tcp port

Configures a service with a destination TCP port or port range that may be used as part of a policy service group or included as part of a policy condition.

policy service *service_name* **destination tcp port** *port***[**-*port***]**

no policy service *service_name*

policy service *service_name* **no destination tcp port**

Syntax Definitions

service_name	The name of the service (up to 31 alphanumeric characters).
port	The well-known port number (or port range) for the desired TCP service. For example, the port number for Telnet is 23. A port range should be separated by a hyphen (for example, **22-23**).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command is a shortcut for the **policy service protocol** command.
- A policy service may be grouped in a policy group using the **policy service group** command. A policy condition may then be associated with the service group.
- Use the **no** form of the command to remove a service from the configuration, or to remove parameters from a particular service.
- If the **snapshot** command is entered after the **policy service** command is configured, the resulting ASCII file will include the following additional syntax for the **policy service** command:

  from {cli | ldap | blt}

  This syntax indicates how the service was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.

Examples

```
-> policy service service4 destination tcp port 23
```

Release History

Release 5.1; command was introduced.

Related Commands

policy service group	Configures a policy service group, which is made up of policy services.
policy condition	Creates a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy service	Displays information about policy services configured on the switch.

MIB Objects

```
alaQoSServiceTable
   alaQoSServiceName
   alaQoSServiceSource
   alaQoSServiceDestinationTcpPort
   alaQoSServiceDestinationTcpPortEnd
alaQoSAppliedServiceTable
   alaQoSAppliedServiceName
   alaQoSAppliedServiceSource
   alaQoSAppliedServiceDestinationTcpPort
   alaQoSAppliedServiceDestinationTcpPortEnd
```

policy service source udp port

Configures a service with a source UDP port or port range that may be used as part of a policy service group or included as part of a policy condition.

policy service *service_name* **source udp port** *port***[-***port***]**

no policy service *service_name*

policy service *service_name* **no source udp port**

Syntax Definitions

service_name	The name of the service (up to 31 alphanumeric characters).
port	The well-known port number (or port range) for the desired UDP service. A port range should be separated by a hyphen (for example, **22-23**).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command is a shortcut for the **policy service protocol** command.
- Use the **no** form of the command to remove a service from the configuration, or to remove parameters from a particular service. Note that at least one parameter must be associated with a service.
- Ports associated with a particular service must all be of the same type. (The **destination tcp port** keyword may be used with this command; other keywords for the command are not allowed.)
- If the **snapshot** command is entered after the **policy service** command is configured, the resulting ASCII file will include the following additional syntax for the **policy service** command:

  from {cli | ldap | blt}

  This syntax indicates how the service was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.

Examples

```
-> policy service serv_a source udp port 1000
-> no policy service serv_a
```

Release History

Release 5.1; command was introduced.

Related Commands

policy service group	Configures a policy service group, which is made up of policy services.
policy condition	Creates a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy service	Displays information about policy services configured on the switch.

MIB Objects

```
alaQoSServiceTable
   alaQoSServiceName
   alaQoSServiceSource
   alaQoSServiceSourceUdpPort
   alaQoSServiceSourceUdpPortEnd
alaQoSAppliedServiceTable
   alaQoSAppliedServiceName
   alaQoSAppliedServiceSource
   alaQoSAppliedSourceUdpPort
   alaQoSAppliedSourceUdpPortEnd
```

policy service destination udp port

Configures a service with a destination UDP port or port range that may be used as part of a policy service group or included as part of a policy condition.

policy service *service_name* **destination udp port** *port***[-***port***]**

no policy service *service_name*

policy service *service_name* **no destination udp port**

Syntax Definitions

service_name	The name of the service (up to 31 alphanumeric characters).
port	The well-known port number (or port range) for the desired UDP service. For example, a port number for NETBIOS is 137. A port range should be separated by a hyphen (for example, **137-138**).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command is a shortcut for the **policy service protocol** command.
- A policy service may be grouped in a policy group using the **policy service group** command. A policy condition may then be associated with the service group.
- Use the **no** form of the command to remove a service from the configuration, or to remove parameters from a particular service.
- If the **snapshot** command is entered after the **policy service** command is configured, the resulting ASCII file will include the following additional syntax for the **policy service** command:

  from {cli | ldap | blt}

  This syntax indicates how the service was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.

Examples

```
-> policy service service4 destination udp port 137
```

Release History

Release 5.1; command was introduced.

Related Commands

policy service group	Configures a policy service group, which is made up of policy services.
policy condition	Creates a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy service	Displays information about policy services configured on the switch.

MIB Objects

```
alaQoSServiceTable
   alaQoSServiceName
   alaQoSServiceSource
   alaQoSServiceDestinationUdpPort
   alaQoSServiceDestinationUdpPortEnd
alaQoSAppliedServiceTable
   alaQoSAppliedServiceName
   alaQoSAppliedServiceSource
   alaQoSAppliedServiceDestinationUdpPort
   alaQoSAppliedServiceDestinationUdpPortEnd
```

policy map group

Configures a map group and its associated mappings for 802.1p, Type of Service (ToS), or Differentiated Services Code Point (DSCP) values. A map group may be referenced in a policy action with the **map** keyword.

policy map group *map_group* **{***value1***:***value2***...}**

no policy map group *map_group*

policy map group no {*value1***:***value2***...}**

Syntax Definitions

map_group	The name of the map group (up to 31 alphanumeric characters).
value1	The 802.1p, ToS, or DSCP value to be mapped to another value. May be a value or a range of values (for example, **1-2**).
value2...	The 802.1p, ToS, or DSCP value to be used in place of *value1*. Additional mapping pairs may be included.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The map group may contain more than one mapping pair.
- Use the **no** form of the command to remove a mapping pair or to remove the map group entirely.
- If the **snapshot** command is entered after the **policy map group** command is configured, the resulting ASCII file will include the following additional syntax for the **policy map group** command:

  from {cli | ldap | blt}

  This syntax indicates how the map group was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.

Examples

```
-> policy map group tosGroup 1-4:3 5-6:5 7:6
-> policy map group tosGroup no 7:6
-> no policy map group tosGroup
```

Release History

Release 5.1; command was introduced.

Related Commands

policy action map	Configures a mapping group for a policy action.

MIB Objects

```
alaQoSMapGroupsTable
   alaQoSMapGroupsName
   alaQoSMapGroupsSource
alaQoSAppliedMapGroupsTable
   alaQoSAppliedMapGroupsName
   alaQoSAppliedMapGroupsSource
alaQoSMapGroupTable
   alaQoSMapGroupKey
   alaQoSMapGroupKeyEnd
   alaQoSMapGroupValue
alaQoSAppliedMapGroupTable
   alaQoSAppliedMapGroupKey
   alaQoSAppliedMapGroupKeyEnd
   alaQoSAppliedMapGroupValue
```

policy condition

Creates a QoS policy condition. The condition determines what parameters the switch uses to classify incoming flows. Condition parameters may be configured when the condition is created; or parameters may be configured for an existing condition. At least one parameter must be configured for a condition.

This section describes the base command. Optional keywords are listed below and described as separate commands later in this chapter. (Options may be used in combination but are described separately for ease in explanation.) Use the **no** form for keywords to remove a parameter from the condition.

Some condition parameters may not be supported depending on the platform you are using. Also some condition parameters may not be supported with some action parameters. See the condition/action tables in your switch *Network Configuration Guide*.

policy condition *condition_name*
[source ip *ip_address* **[mask** *netmask***]]**
[destination ip *ip_address* **[mask** *netmask***]]**
[multicast ip *ip_address* **[mask** *netmask***]]**
[source network group *network_group***]**
[destination network group *network_group***]**
[multicast network group *multicast_group***]**
[source ip port *port***[-***port***]]**
[destination ip port *port***[-***port***]]**
[source tcp port *port***[-***port***]]**
[destination tcp port *port***[-***port***]]**
[source udp port *port***[-***port***]]**
[destination udp port *port***[-***port***]]**
[ethertype *etype***]**
[established]
[tcpflags {any | all} *flag* **[mask** *flag***]**
[service *service***]**
[service group *service_group***]**
[icmptype *type***]**
[icmpcode *code***]**
[ip protocol *protocol***]**
[tos *tos_value tos_mask***]**
[dscp *dscp_value dscp_mask***]**
[source mac *mac_address* **[mask** *mac_mask***]]**
[destination mac *mac_address* **[mask** *mac_mask***]]**
[source mac group *group_name***]**
[destination mac group *mac_group***]**
[source vlan *vlan_id***]**
[destination vlan *vlan_id***]**
[802.1p *802.1p_value***]**
[source port *slot/port***[-***port***]]**
[source port group *group_name***}**
[destination port *slot/port***[-***port***]]**
[destination port group *group_name***]**

[source interface type *type***]**
[destination interface type *type***]**

no policy condition *condition_name*

Syntax Definitions

condition_name	The name of the condition. Any alphanumeric string.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- A policy condition and a policy action are combined to make a policy rule. See the **policy rule** command on page 38-40.
- Use the **qos apply** command to activate configuration changes. See page 38-34 for more information about this command.
- If multiple keywords are defined for a single condition, the traffic flow must match all of the parameters in the condition before the rule is enforced.
- Use the **no** form of the command to remove a condition from a policy rule.
- At least one parameter must be associated with a condition.
- If the **snapshot** command is entered after the **policy condition** command is configured, the resulting ASCII file will include the following additional syntax for the **policy condition** command:

  from {cli | ldap | blt}

  This syntax indicates how the condition was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in condition, this option is not configurable.

Examples

```
-> policy condition cond4 source port 3/1
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy action	Configures a policy action.
policy rule	Configures a policy rule on the switch. A rule is made up of a condition (for classifying incoming traffic) and an action (to be applied to outgoing traffic).
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionSource
   alaQoSConditionSourceSlot
   alaQoSConditionSourcePort
   alaQoSConditionSourcePortEnd
   alaQoSConditionSourcePortGroup
   alaQoSConditionDestinationSlot
   alaQoSConditionDestinationPort
   alaQoSConditionDestinationPortEnd
   alaQoSConditionDestinationPortGroup
   alaQoSConditionSourceInterfaceType
   alaQoSConditionDestinationInterfaceType
   alaQoSConditionSourceMacAddr
   alaQoSConditionSourceMacMask
   alaQoSConditionSourceMacGroup
   alaQoSConditionDestinationMacAddr
   alaQoSConditionDestinationMacMask
   alaQoSConditionDestinationMacGroup
   alaQoSConditionSourceVlan
   alaQoSConditionDestinationVlan
   alaQoSCondition8021p
   alaQoSConditionSourceIpAddr
   alaQoSConditionSourceIpMask
   alaQoSConditionSourceNetworkGroup
   alaQoSConditionDestinationIpAddr
   alaQoSConditionDestinationIpMask
   alaQoSConditionDestinationNetworkGroup
   alaQoSConditionMulticastIpAddr
   alaQoSConditionMulticastIpMask
   alaQoSConditionMulticastNetworkGroup
   alaQoSConditionTos
   alaQoSConditionDscp
   alaQoSConditionTcpFlags
   alaQoSConditionIpProtocol
   alaQoSConditionSourceIpPort
   alaQoSConditionSourceIpPortEnd
   alaQoSConditionDestinationIpPort
   alaQoSConditionDestinationIpPortEnd
   alaQoSConditionSourceTcpPort
   alaQoSConditionSourceTcpPortEnd
   alaQoSConditionDestinationTcpPort
   alaQoSConditionDestinationTcpPortEnd
   alaQoSConditionSourceUdpPort
   alaQoSConditionSourceUdpPortEnd
```

```
   alaQoSConditionDestinationUdpPort
   alaQoSConditionDestinationUdpPortEnd
   alaQoSConditionService
   alaQoSConditionServiceStatus
   alaQoSConditionServiceGroup
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionSource
   alaQoSAppliedConditionSourceSlot
   alaQoSAppliedConditionSourcePort
   alaQoSAppliedConditionSourcePortEnd
   alaQoSAppliedConditionSourcePortGroup
   alaQoSAppliedConditionDestinationSlot
   alaQoSAppliedConditionDestinationPort
   alaQoSAppliedConditionDestinationPortEnd
   alaQoSAppliedConditionDestinationPortGroup
   alaQoSAppliedConditionSourceInterfaceType
   alaQoSAppliedConditionDestinationInterfaceType
   alaQoSAppliedConditionSourceMacAddr
   alaQoSAppliedConditionSourceMacMask
   alaQoSAppliedConditionSourceMacGroup
   alaQoSAppliedConditionDestinationMacAddr
   alaQoSAppliedConditionDestinationMacMask
   alaQoSAppliedConditionDestinationMacGroup
   alaQoSAppliedConditionSourceVlan
   alaQoSAppliedConditionDestinationVlan
   alaQoSAppliedCondition8021p
   alaQoSAppliedConditionSourceIpAddr
   alaQoSAppliedConditionSourceIpMask
   alaQoSAppliedConditionSourceNetworkGroup
   alaQoSAppliedConditionDestinationIpAddr
   alaQoSAppliedConditionDestinationIpMask
   alaQoSAppliedConditionDestinationNetworkGroup
   alaQoSAppliedConditionMulticastIpAddr
   alaQoSAppliedConditionMulticastIpMask
   alaQoSAppliedConditionMulticastNetworkGroup
   alaQoSAppliedConditionTos
   alaQoSAppliedConditionDscp
   alaQoSAppliedConditionTcpFlags
   alaQoSAppliedConditionIpProtocol
   alaQoSAppliedConditionSourceIpPort
   alaQoSAppliedConditionSourceIpPortEnd
   alaQoSAppliedConditionDestinationIpPort
   alaQoSAppliedConditionDestinationIpPortEnd
   alaQoSAppliedConditionSourceTcpPort
   alaQoSAppliedConditionSourceTcpPortEnd
   alaQoSAppliedConditionDestinationTcpPort
   alaQoSAppliedConditionDestinationTcpPortEnd
   alaQoSAppliedConditionSourceUdpPort
   alaQoSAppliedConditionSourceUdpPortEnd
   alaQoSAppliedConditionDestinationUdpPort
   alaQoSAppliedConditionDestinationUdpPortEnd
   alaQoSAppliedConditionService
   alaQoSAppliedConditionServiceStatus
   alaQoSAppliedConditionServiceGroup
```

policy condition source ip

Configures a source IP address for a policy condition.

policy condition *condition_name* **source ip** *ip_address* **[mask** *netmask***]**

policy condition *condition_name* **no source ip**

Syntax Definitions

condition_name	The name of the condition.
ip_address	The source IP address of the Layer 3 flow.
netmask	The mask for the source IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If a mask is not specified, the IP address is assumed to be a host address.
- A source IP address and a source IP network group cannot be specified in the same condition.
- Use the **no** form of the command to remove a source IP address from a condition; however, at least one classification parameter must be associated with a condition.

Examples

```
-> policy condition cond3 source ip 173.201.18.3
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
show policy condition	Shows information about a particular policy condition configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionSourceIpAddr
   alaQoSConditionSourceIpMask
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionSourceIpAddr
   alaQoSAppliedConditionSourceIpMask
```

policy condition destination ip

Configures a destination IP address for a policy condition.

policy condition *condition_name* **destination ip** *ip_address* **[mask** *netmask***]**

policy condition *condition_name* **no destination ip**

Syntax Definitions

condition_name	The name of the condition.
ip_address	The destination IP address of the Layer 3 flow.
netmask	The mask for the destination IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If a mask is not specified, the IP address is assumed to be a host address.
- A destination IP address and a destination IP network group cannot be specified in the same condition.
- Use the **no** form of the command to remove a destination IP address from a condition; however, at least one classification parameter must be associated with a condition.

Examples

```
-> policy condition cond4 destination ip 208.192.21.0 mask 255.255.255.0
```

Release History

Release 5.1; command was introduced.

Related Commands

policy condition	Creates a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy condition	Shows information about a particular policy condition configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionDestinationIpAddr
   alaQoSConditionDestinationIpMask
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionDestinationIpAddr
   alaQoSAppliedConditionDestinationIpMask
```

policy condition multicast ip

Configures a multicast IP address for a policy condition.

policy condition *condition_name* **multicast ip** *ip_address* **[mask** *netmask***]**

policy condition *condition_name* **no multicast ip**

Syntax Definitions

condition_name	The name of the condition.
ip_address	The multicast IP address.
netmask	Optional. The mask for the multicast IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If a mask is not specified, the IP address is assumed to be a host address.
- A multicast IP address and a multicast network group cannot be specified in the same condition.
- Use the **no** form of the command to remove a multicast IP address from a condition; however, at least one classification parameter must be associated with a condition.

Examples

```
-> policy condition cond4 multicast ip 224.1.1.1
```

Release History

Release 5.1; command was introduced.

Related Commands

policy condition	Creates a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSMulticastIpAddr
   alaQoSMulticastIpMask
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedMulticastIpAddr
   alaQoSAppliedMulticastIpMask
```

policy condition source network group

Associates a source network group with a policy condition.

policy condition *condition_name* **source network group** *network_group*

policy condition *condition_name* **no source network group**

Syntax Definitions

condition_name	The name of the condition.
network_group	The name of the source network group. Network groups are configured through the **policy network group** command. See page 38-43 for more information about this command.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a source network group from a condition; however, at least one classification parameter must be associated with a condition.
- A source IP address and a source IP network group cannot be specified in the same condition.

Examples

```
-> policy condition cond5 source network group webgroup1
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
policy network group	Configures a network group name and its associated IP addresses.
show policy condition	Shows information about policy conditions configured on the switch.
show policy network group	Displays information about policy network groups.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionSourceNetworkGroup
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionSourceNetworkGroup
```

policy condition destination network group

Associates a destination network group with a policy condition.

policy condition *condition_name* **destination network group** *network_group*

policy condition *condition_name* **no destination network group**

Syntax Definitions

condition_name	The name of the condition.
network_group	The name of the destination network group. Network groups are configured through the **policy network group** command. See page 38-43 for more information about this command.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a destination network group from a condition; however, at least one classification parameter must be associated with a condition.
- A destination IP address and a destination IP network group cannot be specified in the same condition.

Examples

```
-> policy condition cond6 destination network group webgroup1
```

Release History

Release 5.1; command was introduced.

Related Commands

policy condition	Creates a policy condition.
policy network group	Configures a network group name and its associated IP addresses.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy condition	Shows information about policy conditions configured on the switch.
show policy network group	Displays information about policy network groups.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionDestinationNetworkGroup
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionDestinationNetworkGroup
```

policy condition multicast network group

Associates a multicast group with a policy condition.

policy condition *condition_name* **multicast network group** *multicast_group*

policy condition *condition_name* **no multicast network group**

Syntax Definitions

condition_name	The name of the condition.
multicast_group	The multicast group name. Multicast groups are configured through the **policy network group** command.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a multicast group from a condition; however, at least one classification parameter must be associated with a condition.
- A multicast address and a multicast network group cannot be specified in the same condition.

Examples

```
-> policy condition cond3 multicast group video2
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
policy network group	Configures a network group name and its associated IP addresses.
show policy condition	Shows information about policy conditions configured on the switch.
show policy network group	Displays information about policy network groups.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionMulticastNetworkGroup
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionMulticastNetworkGroup
```

policy condition source ip port

Configures a source IP port number for a policy condition.

policy condition *condition_name* **source ip port** *port***[-***port***]**

policy condition *condition_name* **no source ip port**

Syntax Definitions

condition_name	The name of the condition.
port	The TCP or UDP port number of the source address of the Layer 3 flow, in the range from 0–65535. A range of ports (separated by a hyphen) may be specified instead of a single port. (On the OmniSwitch 6624/ 6648, the supported range is 1–25).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a source IP port from a condition; however, at least one classification parameter must be associated with a condition.
- The protocol (TCP or UDP) must be specified in the condition, either on the same command line or in a previous command. Use the **ip protocol** keywords. See the **policy condition ip protocol** command on page 38-99.
- The same condition cannot specify a source IP port with a source TCP port, source UDP port, service, or service group.

Examples

```
-> policy condition cond1 ip protocol 6 source ip port 137
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition ip protocol	Configures an IP protocol for a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionSourceIpPort
   alaQoSConditionSourceIpPortEnd
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionSourceIpPort
   alaQoSAppliedConditionSourceIpPortEnd
```

policy condition destination ip port

Configures a destination IP port number for a policy condition.

policy condition *condition_name* **destination ip port** *port***[-***port***]**

policy condition *condition_name* **no destination ip port**

Syntax Definitions

condition_name	The name of the condition.
port	The TCP or UDP port number (or port range) of the destination address of the Layer 3 flow, in the range from 0–65535. A range of ports (separated by a hyphen) may be specified instead of a single port.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a destination IP port from a condition; however, at least one classification parameter must be associated with a condition.
- The protocol (TCP or UDP) must be specified in the same condition, either on the same command line or in a previous command. Use the **ip protocol** keywords. See the **policy condition ip protocol** command on page 38-99.
- The same condition cannot specify a destination IP port with a service or service group.

Examples

```
-> policy condition cond2 ip protocol 6 destination ip port 137-138
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition ip protocol	Configures an IP protocol for a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionDestinationIpPort
   alaQoSConditionDestinationIpPortEnd
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionDestinationIpPort
   alaQoSAppliedConditionDestinationIpPortEnd
```

policy condition source tcp port

Configures a source TCP port number for a policy condition.

policy condition *condition_name* **source tcp port** *port***[-***port***]**

policy condition *condition_name* **no source tcp port**

Syntax Definitions

condition_name	The name of the condition.
port	The TCP port number of the source address of the Layer 3 flow, in the range from 0–65535. A range of ports (separated by a hyphen) may be specified instead of a single port.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a source TCP port from a condition; however, at least one classification parameter must be associated with a condition.
- This command is a shortcut for the **policy condition source ip port** command, which requires that the protocol also be specified. Rather than specifying **source ip port** and **ip protocol**, use **source tcp port**.
- The same condition cannot specify a source TCP port with a service or service group.
- IP port protocol types cannot be mixed in the same condition; ports must be either TCP or UDP.

Examples

```
-> policy condition cond3 source tcp port 137
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionSourceTcpPort
   alaQoSConditionSourceTcpPortEnd
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionSourceTcpPort
   alaQoSAppliedConditionSourceTcpPortEnd
```

policy condition destination tcp port

Configures a destination TCP port number for a policy condition.

policy condition *condition_name* **destination tcp port** *port***[-***port***]**

policy condition *condition_name* **no destination tcp port**

Syntax Definitions

condition_name	The name of the condition.
port	The TCP port number (or port range) of the destination address of the Layer 3 flow, in the range from 0–65535. A range of ports (separated by a hyphen) may be specified instead of a single port.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a destination IP port from a condition; however, at least one classification parameter must be associated with a condition.
- This command is a shortcut for the **policy condition destination ip port** command, which requires that the protocol also be specified. Rather than specifying **destination ip port** and **ip protocol**, use **destination tcp port**.
- The same condition cannot specify a destination TCP port with a service or service group.
- IP port protocol types cannot be mixed in the same condition; ports must be either TCP or UDP.

Examples

```
-> policy condition cond4 destination tcp port 137-138
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionDestinationTcpPort
   alaQoSConditionDestinationTcpPortEnd
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionDestinationTcpPort
   alaQoSAppliedConditionDestinationTcpPortEnd
```

policy condition source udp port

Configures a source UDP port number for a policy condition.

policy condition *condition_name* **source udp port** *port***[-***port***]**

policy condition *condition_name* **no source udp port**

Syntax Definitions

condition_name	The name of the condition.
port	The UDP port number of the source address of the Layer 3 flow, in the range from 0–65535. A range of ports (separated by a hyphen) may be specified instead of a single port.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a source UDP port from a condition; however, at least one classification parameter must be associated with a condition.
- This command is a shortcut for the **policy condition source ip port** command, which requires that the protocol also be specified. Rather than specifying **source ip port** and **ip protocol**, use **source udp port**.
- The same condition cannot specify a source UDP port with a service or service group.
- IP port protocol types cannot be mixed in the same condition; ports must be either TCP or UDP.

Examples

```
-> policy condition cond5 source udp port 1200-1400
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionSourceUdpPort
   alaQoSConditionSourceUdpPortEnd
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionSourceUdpPort
   alaQoSAppliedConditionSourceUdpPortEnd
```

policy condition destination udp port

Configures a destination UDP port number for a policy condition.

policy condition *condition_name* **destination udp port** *port***[**-*port***]**

policy condition *condition_name* **no destination udp port**

Syntax Definitions

condition_name	The name of the condition.
port	The UDP port number (or port range) of the destination address of the Layer 3 flow, in the range from 0–65535. A range of ports (separated by a hyphen) may be specified instead of a single port.

Defaults

N/A

Platforms Supported

OmniSwitch 6624, 6648, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a destination IP port from a condition; however, at least one classification parameter must be associated with a condition.
- This command is a shortcut for the **policy condition destination ip port** command, which requires that the protocol also be specified. Rather than specifying **destination ip port** and **ip protocol**, use **destination tcp port**.
- The same condition cannot specify a destination UDP port with a service or service group.
- IP port protocol types cannot be mixed in the same condition; ports must be either TCP or UDP.

Examples

```
-> policy condition cond4 destination tcp port 137-138
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionDestinationTcpPort
   alaQoSConditionDestinationTcpPortEnd
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionDestinationTcpPort
   alaQoSAppliedConditionDestinationTcpPortEnd
```

policy condition ethertype

Configures an ethertype value to use for traffic classification.

policy condition *condition_name* **ethertype** *etype*

policy condition *condition_name* **no ethertype**

Syntax Definitions

condition_name	The name of the condition.
etype	The ethertype value, in the range 1536–65535 or 0x600–0xffff hex..

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove an ethertype value from a condition; however, at least one classification parameter must be associated with a condition.
- Enter a numeric or equivalent hex value for the *etype*.

Examples

```
-> policy condition cond12 ethertype 8137
```

Release History

Release 5.3.1; command was introduced.

Related Commands

policy condition	Creates a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionEthertype
   alaQoSConditionEthertypeStatus
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionEthertype
   alaQoSAppliedConditionEthertypeStatus
```

policy condition service

Configures a service for a policy condition.

policy condition *condition_name* **service** *service_name*

policy condition *condition_name* **no service**

Syntax Definitions

condition_name	The name of the condition.
service_name	The service name, configured through the **policy service** command.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a service group from a condition; however, at least one classification parameter must be associated with a condition.
- A policy condition that specifies a service cannot also specify a service group, IP protocol, source IP port, or destination IP port.

Examples

```
-> policy condition cond12 service serv2
```

Release History

Release 5.1; command was introduced.

Related Commands

policy service	Configures a service that may be used as part of a policy service group.
qos apply	Applies configured global QoS and policy settings to the current configuration (changes will be active and stored in flash).
show policy service	Displays information about all particular policy services or a particular policy service configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionService
alaQoSAppliedConditionTable
   alaQoSAppliedConditionService
```

policy condition service group

Associates a policy service group with a policy condition.

policy condition *condition_name* **service group** *service_group*

policy condition *condition_name* **no service group**

Syntax Definitions

condition_name	The name of the condition.
service_group	The service group name. Service groups are configured through the **policy service group** command. See page 38-45 for more information about this command.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a service group from a condition; however, at least one classification parameter must be associated with a condition.
- A policy condition that specifies a service group cannot also specify a service, IP protocol, source IP port, or destination IP port.

Examples

```
-> policy condition cond12 service group servgroup2
```

Release History

Release 5.1; command was introduced.

Related Commands

policy service group	Configures a service group and its associated services.
policy condition	Creates a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionServiceGroup
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionServiceGroup
```

policy condition ip protocol

Configures an IP protocol for a policy condition.

policy condition *condition_name* **ip protocol** *protocol*

policy condition *condition_name* **no ip protocol**

Syntax Definitions

condition_name	The name of the condition.
protocol	The protocol associated with the flow. Valid values are **6** for TCP, **17** for UDP, or **1** for ICMP.

Defaults

parameter	default
protocol	6

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a protocol from a condition; however, at least one classification parameter must be associated with a condition.
- If a source or destination port is specified (through the **policy condition source ip port** or **policy condition destination ip port** commands), the protocol must be specified.
- The same condition cannot specify an IP protocol with a service or service group.

Examples

```
-> policy condition cond4 ip protocol 6
```

Release History

Release 5.1; command was introduced.

Related Commands

policy condition source ip port	Configures a source IP port number for a policy condition.
policy condition destination ip port	Configures a destination IP port number for a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionIpProtocol
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionIpProtocol
```

policy condition source mac

Configures a source MAC address for a policy condition.

policy condition *condition_name* **source mac** *mac_address* **[mask** *mac_mask***]**

policy condition *condition_name* **no source mac**

Syntax Definitions

condition_name	The name of the condition. May be an existing condition name or a new condition.
mac_address	The source MAC address in the Layer 2 header of the frame (for example, 00:20:da:05:f6:23)
mac_mask	Optional. The mask for the source MAC address (for example, ff:ff:ff:ff:ff:ff).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a source MAC address from a condition; however, at least one classification parameter must be associated with a condition.
- A source MAC address and a source MAC group cannot be specified in the same condition.
- On an OmniSwitch 7700/7800/8800, a source MAC address or source MAC group can only be used with a policy action that specifies disposition. Any other action is not supported. This restriction does *not* apply to an OmniSwitch 6600.

Examples

```
-> policy condition cond2 source mac 00:20:da:05:f6:23
```

Release History

Release 5.1; command was introduced.

Related Commands

policy condition	Creates a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionSourceMacAddr
   alaQoSConditionSourceMacMask
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionSourceMacAddr
   alaQoSAppliedConditionSourceMacMask
```

policy condition destination mac

Configures a destination MAC address for a policy condition.

policy condition *condition_name* **destination mac** *mac_address* **[mask** *mac_mask***]**

policy condition *condition_name* **no destination mac**

Syntax Definitions

condition_name	The name of the condition. May be an existing condition name or a new condition.
mac_address	The destination MAC address in the Layer 2 header of the frame (for example, 00:20:da:05:f6:23).
mac_mask	Optional. The mask for the destination MAC address (for example, ff:ff:ff:ff:ff:ff).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a destination MAC address from a condition; however, at least one classification parameter must be associated with a condition.
- A destination MAC address and a destination MAC group cannot be specified in the same condition.

Examples

```
-> policy condition cond3 destination mac 00:20:da:05:f6:23
```

Release History

Release 5.1; command was introduced.

Related Commands

policy condition	Creates a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionSource
   alaQoSConditionDestinationMacAddr
   alaQoSConditionDestinationMacMask
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionSource
   alaQoSAppliedConditionDestinationMacAddr
   alaQoSAppliedConditionDestinationMacMask
```

policy condition source mac group

Associates a source MAC group with a policy condition.

policy condition *condition_name* **source mac group** *group_name*

policy condition *condition_name* **no source mac group**

Syntax Definitions

condition_name	The name of the condition. May be an existing condition name or a new condition.
group_name	The name of the source MAC group, configured through the **policy mac group** command. See page 38-47 for more information about this command.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a source MAC group from a condition; however, at least one classification parameter must be associated with a condition.
- A source MAC address and a source MAC group cannot be specified in the same condition.

Examples

```
-> policy condition cond4 source mac group mac_group1
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy mac group	Configures a MAC group and its associated MAC addresses.
policy condition	Creates a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionSourceMacGroup
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionSourceMacGroup
```

policy condition destination mac group

Associates a destination MAC group with a policy condition.

policy condition *condition_name* **destination mac group** *mac_group*

policy condition *condition_name* **no destination**

Syntax Definitions

condition_name	The name of the condition. May be an existing condition name or a new condition.
mac_group	The name of the destination MAC group, configured through the **policy mac group** command. See page 38-47 for more information about this command.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a destination MAC group from a policy condition; however, at least one classification parameter must be associated with a condition.
- A destination MAC address and a destination MAC group cannot be specified in the same condition.

Examples

```
-> policy condition cond5 destination mac group mac_group1
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy mac group	Configures a MAC group and its associated MAC addresses.
policy condition	Creates a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionDestinationMacGroup
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionDestinationMacGroup
```

policy condition source vlan

Configures a source VLAN for a policy condition.

policy condition *condition_name* **source vlan** *vlan_id*

policy condition *condition_name* **no source vlan**

Syntax Definitions

condition_name	The name of the condition. May be an existing condition name or a new condition.
vlan_id	The source VLAN ID for the flow.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **no** form of the command to remove a source VLAN from a policy condition; however, at least one classification parameter must be associated with a condition.

Examples

```
-> policy condition cond5 source vlan 3
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionSourceVlan
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionSourceVlan
```

policy condition destination vlan

Configures a destination VLAN for a policy condition. Use the **no** form of the command to remove a destination VLAN from a condition.

policy condition *condition_name* **destination vlan** *vlan_id*

policy condition *condition_name* **no destination vlan**

Syntax Definitions

condition_name	The name of the condition. May be an existing condition name or a new condition.
vlan_id	The destination VLAN ID for the flow.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **no** form of the command to remove a destination VLAN from a condition; however, at least one classification parameter must be associated with a condition.

Examples

```
-> policy condition cond4 destination vlan 3
```

Release History

Release 5.1; command was introduced.

Related Commands

policy condition	Creates a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionDestinationVlan
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionDestinationVlan
```

policy condition source port

Configures a source port number for a policy condition. Use the **no** form of the command to remove a source port number from a condition.

policy condition *condition_name* **source port** *slot/port***[-***port***]**

policy condition *condition_name* **no source port**

Syntax Definitions

condition_name	The name of the condition. May be an existing condition name or a new condition.
slot/port	The slot and port number (or range of ports) on which the frame is received.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **no** form of the command to remove a source port from a condition; however, at least one classification parameter must be associated with a condition.

Examples

```
-> policy condition cond2 source port 3/1
-> policy condition cond3 source port 3/2-4
```

Release History

Release 5.1; command was introduced.

Related Commands

policy condition	Creates a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionSourceSlot
   alaQoSConditionSourcePort
   alaQoSConditionSourcePortEnd
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionSourceSlot
   alaQoSAppliedConditionSourcePort
   alaQoSAppliedConditionSourcePortEnd
```

policy condition destination port

Configures a destination port number for a policy condition. Use the **no** form of the command to remove a destination port from a condition.

policy condition *condition_name* **destination port** *slot/port***[-***port***]**

policy condition *condition_name* **no destination port**

Syntax Definitions

condition_name	The name of the condition. May be an existing condition name or a new condition.
slot/port	The slot and port number (or range of ports) on which the frame is received.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **no** form of the command to remove a destination port from a condition; however, at least one classification parameter must be associated with a condition.

Examples

```
-> policy condition cond3 destination port 4/2
-> policy condition cond4 destination port 4/3-4
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionDestinationSlot
   alaQoSConditionDestinationPort
   alaQoSConditionDestinationPortEnd
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionDestinationSlot
   alaQoSAppliedConditionDestinationPort
   alaQoSAppliedConditionDestinationPortEnd
```

policy condition source port group

Associates a source port group with a policy condition. Use the **no** form of the command to remove a source port group from a condition.

policy condition *condition_name* **source port group** *group_name*

policy condition *condition_name* **no source port group**

Syntax Definitions

condition_name	The name of the condition. May be an existing condition name or a new condition.
group_name	The name of the source port group. Port groups are configured through the **policy port group** command. See page 38-49 for more information about this command.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **no** form of the command to remove a source port group from a condition; however, at least one classification parameter must be associated with a condition.

Examples

```
-> policy condition cond6 source port group portgr4
```

Release History

Release 5.1; command was introduced.

Related Commands

policy port group	Configures a port group and its associated slot and port numbers.
policy condition	Creates a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionSourcePortGroup
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionSourcePortGroup
```

policy condition destination port group

Associates a destination port group with a policy condition. Use the **no** form of the command to remove a destination port group from a condition.

policy condition *condition_name* **destination port group** *group_name*

policy condition *condition_name* **no destination port**

Syntax Definitions

condition_name	The name of the condition. May be an existing condition name or a new condition.
group_name	The name of the destination port group. Port groups are configured through the **policy port group** command. See page 38-49 for more information about this command.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **no** form of the command to remove a destination port group from a condition; however, at least one classification parameter must be associated with a condition.

Examples

```
-> policy condition cond6 destination port group portgr4
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy port group	Configures a port group and its associated slot and port numbers.
policy condition	Creates a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionDestinationPortGroup
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionDestinationPortGroup
```

policy condition source interface type

Configures a source interface type for a policy condition.

policy condition *condition_name* **source interface type {ethernet | wan | ethernet-10 | ethernet-100 | ethernet-1G | ethernet-10G}**

policy condition *condition_name* **no source interface type**

Syntax Definitions

condition_name	The name of the condition. May be an existing condition name or a new condition.
ethernet	Indicates that policies for all Ethernet interfaces should be displayed.
wan	Indicates that policies for WAN interfaces should be displayed. *Not supported in the current release.*
ethernet-10	Indicates that only policies for 10 Mb Ethernet should be displayed.
ethernet-100	Indicates that only policies for 100 Mb Ethernet should be displayed.
ethernet-1G	Indicates that only policies for 1 Gigabit Ethernet should be displayed.
ethernet-10G	Indicates that only policies for 10 Gigabit Ethernet should be displayed.

Defaults

parameter	default
type	ethernet

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a source interface type from a condition; however, at least one classification parameter must be associated with a condition.
- In the current release, only Ethernet interface types are supported.

Examples

```
-> policy condition cond2 source interface type ethernet
-> policy condition cond2 no source interface type
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionSourceInterfaceType
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionSourceInterfaceType
```

policy condition destination interface type

Configures a destination interface type for a particular condition. Use the **no** form of the command to remove a destination interface type from a condition.

policy condition *condition_name* **destination interface type {ethernet | wan | ethernet-10 | ethernet-100 | ethernet-1G | ethernet-10G}**

policy condition *condition_name* **no destination interface type**

Syntax Definitions

condition_name	The name of the condition.
ethernet	Indicates that policies for all Ethernet interfaces should be displayed.
wan	Indicates that policies for WAN interfaces should be displayed. *Not supported in the current release.*
ethernet-10	Indicates that only policies for 10 Mb Ethernet should be displayed.
ethernet-100	Indicates that only policies for 100 Mb Ethernet should be displayed.
ethernet-1G	Indicates that only policies for 1 Gigabit Ethernet should be displayed.
ethernet-10G	Indicates that only policies for 10 Gigabit Ethernet should be displayed.

Defaults

parameter	default
ethernet | wan | ethernet-10...	ethernet

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- In the current release, only Ethernet interface types are supported.
- Use the **no** form of the command to remove an interface type from a condition; however, at least one classification parameter must be associated with a condition.

Examples

```
-> policy condition cond2 destination interface type ethernet
```

Release History

Release 5.1; command was introduced.

Related Commands

policy condition	Creates a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionDestinationInterfaceType
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionDestinationInterfaceType
```

policy action

Configures or deletes a QoS action. A QoS action describes how traffic that matches a particular QoS condition should be treated. It may specify a particular set of bandwidth and queue parameters, or it may simply specify whether the flow is allowed or denied on the switch.

This section describes the base command. Optional keywords are listed below and described as separate commands later in this chapter. (Options may be used in combination but are described separately for ease in explanation.) Use the **no** form for keywords to remove the parameter from the action.

Note that some action parameters may not be supported depending on the platform you are using. Also some action parameters may not be supported with some conditions. See the condition table in your switch's *Network Configuration Guide*.

policy action *action_name*
[disposition {accept | drop | deny}]
[shared]
[priority *priority_value***]**
[minimum bandwidth *bps***]**
[maximum bandwidth *bps***]**
[maximum buffers *max_buffers***]**
[minimum depth *bytes***]**
[maximum depth *bytes***]**
[tos *tos_value***]**
[802.1p *802.1p_value***]**
[dcsp *dcsp_value***]**
[map {802.1p | tos | dscp} to {802.1p | tos| dscp} using *map_group***]**
[source rewrite ip *ip_address* **[mask** *netmask***]]**
[source rewrite network group *net_group***]**
[destination rewrite ip *ip_address* **[mask** *netmask***]]**
[destination rewrite network group *net_group***]**
[gateway ip *ip_address***]**
[default gateway ip *ip_address***]**

policy no action *action_name*

Syntax Definitions

action_name	A name for the action, any alphanumeric string.

Defaults

By default, no drop algorithm is configured for the action, and any queues created by the action are not shared.

parameter	default
accept | drop | deny	accept

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Any condition parameters that the hardware supports will be used to classify the traffic; any condition parameters that are not supported by the hardware will not be used to classify traffic, and the event will be logged in the QoS log.
- Bandwidth and queue parameters may be specified when the action is created or may be specified as separate commands.
- Use the **qos apply** command to activate configuration changes. See page 38-34 for more information about this command.
- Use the **no** form of the command to remove a QoS action from the configuration.
- To prevent IP source address spoofing on an OmniSwitch 6600, create a new policy action called *string*DisablePorts that will administratively disable a port when spoofed traffic is detected on that port. Note that *string* represents text that the user enters as a required part of the policy action name and must be followed by DisablePorts. In addition, this action does not need a disposition to be specified and only applies to routed traffic. Refer to the switch *Network Configuration Guide* for more information about ACL security enhancements.
- If the **snapshot** command is entered after the **policy action** command is configured, the resulting ASCII file will include the following additional syntax for the **policy action** command:

  from {cli | ldap | blt}

  This syntax indicates how the action was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in action, this setting is not configurable.

Examples

```
-> policy action action1 accept
```

Release History

Release 5.1; command was introduced.

Related Commands

policy condition	Configures a condition associated with the action.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy action	Displays information about policy actions.

MIB Objects

alaQoSActionTable

- alaQoSActionName
- alaQoSActionSource
- alaQoSActionDisposition
- alaQoSActionMinimumBandwidth
- alaQoSActionMaximumBandwidth
- alaQoSActionPeakBandwidth
- alaQoSActionPriority
- alaQoSActionShared
- alaQoSActionMaximumBuffers
- alaQoSActionMaximumDepth
- alaQoSAction8021p
- alaQoSActionTos
- alaQoSActionTosRewriteMask
- alaQoSActionDscp
- alaQoSActionMapFrom
- alaQoSActionMapTo
- alaQoSActionMapGroup
- alaQoSActionSourceRewriteIpAddr
- alaQoSActionSourceRewriteIpMask
- alaQoSActionSourceRewriteIpGroup
- alaQoSActionDestinationRewriteIpAddr
- alaQoSActionDestinationRewriteIpMask
- alaQoSActionDestinationRewriteIpGroup

alaQoSAppliedActionTable

- alaQoSAppliedActionName
- alaQoSAppliedActionSource
- alaQoSAppliedActionDisposition
- alaQoSAppliedActionMinimumBandwidth
- alaQoSAppliedActionMaximumBandwidth
- alaQoSAppliedActionPeakBandwidth
- alaQoSAppliedActionPriority
- alaQoSAppliedActionShared
- alaQoSAppliedActionMaximumDepth
- alaQoSAppliedActionMaximumBuffers
- alaQoSAppliedAction8021p
- alaQoSAppliedActionTos
- alaQoSAppliedActionTosRewriteMask
- alaQoSAppliedActionDscp
- alaQoSAppliedActionMapFrom
- alaQoSAppliedActionMapTo
- alaQoSAppliedActionMapGroup
- alaQoSAppliedActionSourceRewriteIpAddr
- alaQoSAppliedActionSourceRewriteIpMask
- alaQoSAppliedActionSourceRewriteIpGroup
- alaQoSAppliedActionDestinationRewriteIpAddr
- alaQoSAppliedActionDestinationRewriteIpMask
- alaQoSAppliedActionDestinationRewriteIpGroup

policy action disposition

Configures a disposition for a policy action.

policy action *action_name* **disposition {accept | drop | deny}**

policy action *action_name* **no disposition**

Syntax Definitions

action_name	The name of the action.
accept	Specifies that the switch should accept the flow.
drop	Specifies that the switch should silently drop the flow.
deny	Specifies that the switch should drop the flow and issue an ICMP message indicating the flow was dropped for administrative reasons. Currently this option will provide the same result as **drop**; that is, the flow is silently dropped.

Defaults

parameter	default
accept | drop | deny	accept

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a disposition from an action.
- This command does not support Layer 2 conditions such as destination VLAN or destination MAC address.

Examples

```
-> policy action action3 disposition deny
-> policy action action 3 no disposition
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy action	Creates a policy action.
show policy action	Displays information about policy actions.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionDisposition
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionDisposition
```

policy action shared

Enables queues created by a particular action to be shared.

policy action *action_name* **shared**

policy action *action_name* **no shared**

Syntax Definitions

action_name	The name of the action.

Defaults

By default, queues created by an action are *not* shared.

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- If multiple rules have the same action, more than one flow may be scheduled on the same queue if the queue is defined as shared; otherwise, a separate queue is created for each flow.
- Note that flows must be sent over the same virtual port for the flows to share a queue. For example, flows with the same 802.1Q tag may share the same queue.
- Use the **no** form of the command to disable sharing.

Example

```
-> policy action action5 shared
-> policy action action5 no shared
```

Release History

Release 5.1; command was introduced.

Related Commands

policy action	Creates a policy action.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy action	Displays information about actions configured on the switch.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionShared
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionShared
```

policy action priority

Configures the priority for queuing a flow to which the QoS action applies.

policy action *action_name* **priority** *priority_value*

policy action *action_name* **no priority**

Syntax Definitions

action_name	The name of the action.
priority_value	The priority given to scheduling traffic on the output port. Values range from 0 (lowest) to 7 (highest).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This priority value is independent of 802.1Q, Type of Service (ToS), or Differentiated Services Code Point (DSCP) values.
- Note that the value displayed on the **show qos queue** screen may be different from the value entered here. See the output descriptions on page 38-266 for more information.
- Use the **no** form of the command to remove a priority value from an action.

Examples

```
-> policy action action1 priority 1
-> policy action action1 no priority
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy action	Creates a policy action.
show policy action	Displays information about actions configured on the switch.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionPriority
   alaQoSActionPriorityStatus
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionPriority
   alaQoSAppliedActionPriorityStatus
```

policy action maximum bandwidth

Configures a maximum bandwidth value for a policy action.

policy action *action_name* **maximum bandwidth** *bps*

policy action *action_name* **no maximum bandwidth**

Syntax Definitions

action_name	The name of the action.
bps	The desired value for maximum bandwidth, in bits per second. The value may be entered as an integer (for example, **10000**) or with abbreviated units (for example, **10k**). If the value is entered in bits per second, the switch rounds the value up to the nearest thousand.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a maximum bandwidth value from an action.
- Note that the bandwidth may be entered in bits per second. Alternatively, the bandwidth may be entered in abbreviated units (**1k**, **2k**, etc). If the bandwidth value is entered in bytes, the switch rounds the value to the nearest thousand bytes. For example, if you enter 1 to 1024, the result is 1K. If you enter 1025 to 2048, the result is 2K.
- On the OmniSwitch 7700/7800/8800, when a port group is used as part of a policy rule and a policy action specifies a maximum bandwidth, each interface in the port group will be allowed the maximum bandwidth.
- On the OmniSwitch 6624/6648, when a source port group is used as part of a policy rule and a policy action specifies a maximum bandwidth, the maximum bandwidth is divided equally among the number of active ports in the port group (100 percent for one active port; 50 percent each for two active ports; 25 percent each for four active ports, etc.).
- On the OmniSwitch 6624/6648, when a destination port group is used as part of a policy rule and a policy action specifies a maximum bandwidth, the maximum bandwidth is divided equally among the number of active ports in the port group if the ports are part of the same 24-port physical location (hardware ASIC). If the destination ports belong to discreet 24-port locations (different ASICs), the maximum bandwidth is applied to each ASIC.
- The maximum bandwidth action may be used for ingress policing on Network Processor interfaces; the policy must contain a source slot/port or port group, or source VLAN that corresponds to the Network Processor interface.

Examples

```
-> policy action action4 maximum bandwidth 10000
-> policy action action4 maximum bandwidth 10k
-> policy action action4 no maximum bandwidth
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy action	Creates a policy action.
show policy action	Displays information about actions configured on the switch.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionMaximumBandwidth
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionMaximumBandwidth
```

policy action maximum buffers

Configures the maximum number of buffers that may be assigned to queues created according to a particular policy action.

policy action *action_name* **maximum buffers** *max_buffers*

policy action *action_name* **no maximum buffers**

Syntax Definitions

action_name	The name of the action.
max_buffers	The maximum number of buffers that may be assigned to queues created by the action specified by *action_name*. The number of buffers cannot exceed that allowed by the interface type. For Ethernet the range is 0–2048.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a maximum buffers value from an action.
- The maximum number of buffers allowed for an Ethernet interface type is 2048.

Examples

```
-> policy action action3 maximum buffers 128
-> policy action action3 no maximum buffers
```

Release History

Release 5.1; command was introduced.

Related Commands

policy action	Creates a policy action.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy action	Displays information about actions configured on the switch.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionMaximumBuffers
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionMaximumBuffers
```

policy action minimum depth

Configures the minimum queue depth assigned to this action, in bytes. The queue depth determines the amount of buffer allocated to each queue.

policy action *action_name* **minimum depth** *bytes*

policy action *action_name* **no minimum depth**

Syntax Definitions

action_name	The name of the action.
bytes	The minimum queue depth, in bytes. The value may be entered as an integer (for example, **10000**) or with abbreviated units (for example, **10k**). If the value is entered in bytes, the switch rounds the value up to the nearest thousand.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a minimum depth value from a policy action.
- Note that the bandwidth may be entered in bytes. Alternatively, the bandwidth may be entered in abbreviated units (**1k**, **2k**, etc). If the bandwidth value is entered in bytes, the switch rounds the value to the nearest thousand bytes. For example, if you enter 1 to 1024, the result is 1K. If you enter 1025 to 2048, the result is 2K.
- The minimum depth action may be used for ingress policing on Network Processor interfaces; the policy must contain a source slot/port or port group, or source VLAN that corresponds to the Network Processor interface.

Examples

```
-> policy action action2 minimum depth 100
-> policy action action2 no minimum depth
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy action	Creates a policy action.
show policy action	Displays information about actions configured on the switch.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionMinimumDepth
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionMinimumDepth
```

policy action maximum depth

Configures the maximum queue depth assigned to this action, in bytes. The queue depth determines the amount of buffer allocated to each queue. When the queue depth is reached, the switch starts dropping packets.

policy action *action_name* **maximum depth** *bytes*

policy action *action_name* **no maximum depth**

Syntax Definitions

action_name	The name of the action.
bytes	The maximum queue depth, in bytes. The value may be entered as an integer (for example, **10000**) or with abbreviated units (for example, **10k**). If the value is entered in bytes, the switch rounds the value up to the nearest thousand.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a maximum depth value from a policy action.
- Note that the bandwidth may be entered in bytes. Alternatively, the bandwidth may be entered in abbreviated units (**1k**, **2k**, etc). If the bandwidth value is entered in bytes, the switch rounds the value to the nearest thousand bytes. For example, if you enter 1 to 1024, the result is 1K. If you enter 1025 to 2048, the result is 2K.
- The maximum depth action may be used for ingress policing on Network Processor interfaces; the policy must contain a source slot/port or port group, or source VLAN that corresponds to the Network Processor interface.

Examples

```
-> policy action action2 maximum depth 100
-> policy action action2 no maximum depth
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy action	Creates a policy action.
show policy action	Displays information about actions configured on the switch.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionMaximumDepth
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionMaximumDepth
```

policy action tos

Configures a Type of Service (ToS) bits value to be applied to packets in outgoing flows to which the specified policy applies.

policy action *action_name* **tos** *tos_value*

policy action *action_name* **no tos**

Syntax Definitions

action_name	The name of the action.
tos_value	The three-bit priority value in the IP header that should be set on outgoing frames in flows that match the specified policy. Values range from 0 (lowest priority) to 7 (highest priority).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a ToS value from a policy action.
- If a ToS value is specified for the action, a DSCP value or 802.1p value may not be specified
- Note that specifying both ToS and DSCP in the same action is *not* allowed..

Examples

```
-> policy action action3 tos 4
-> policy action action3 no tos
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy action	Creates a policy action.
show policy action	Displays information about actions configured on the switch.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionTos
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionTos
```

policy action 802.1p

Configures a value to be set in the 802.1p bits of the 802.1Q byte of an outgoing frame for traffic that matches a policy with this action.

policy action *action_name* **802.1p** *802.1p_value*

policy action *action_name* **no 802.1p**

Syntax Definitions

action_name	The name of the action.
802.1p_value	The priority value to be set in 802.1Q frames. Values range from 0 (lowest priority) to 7 (highest priority).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove an 802.1p value from a policy action.
- If an 802.1p value is configured for a policy action, a ToS value or DSCP value may not be specified.
- Note that specifying both ToS and DSCP in the same action is not allowed.

Examples

```
-> policy action action4 802.1p 7
-> policy action action4 no 802.1p
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy action	Creates a policy action.
show policy action	Displays information about actions configured on the switch.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSAction8021p
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedAction8021p
```

policy action dscp

Configures a Differentiated Services Code Point (DSCP) value to be set in an outgoing flow for traffic that matches rules with this action.

policy action *action_name* **dscp** *dscp_value*

policy action *action_name* **no dscp**

Syntax Definitions

action_name	The name of the action.
dscp_value	The DSCP value to be set, in the range 0–63.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a DSCP value from a policy action.
- If a DSCP value is specified for an action, a ToS value or 802.1p value may be not specified.
- Note that specifying both ToS and DSCP in the same action is *not* allowed.

Examples

```
-> policy action action2 dscp 61
-> policy action action2 no dscp
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy action	Creates a policy action.
show policy action	Displays information about actions configured on the switch.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionDscp
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionDscp
```

policy action map

Configures a mapping group for a policy action.

policy action map {802.1p | tos | dscp} to {802.1p | tos| dscp} using *map_group*

policy action no map

Syntax Definitions

802.1p	Indicates that an 802.1p value should be mapped.
tos	Indicates that a ToS value should be mapped.
dscp	Indicates that a DSCP value should be mapped.
map_group	The name of the map group, configured through the **policy map group** command.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- When remapping is configured with this command and a flow matches a policy with this remapping action, and the 802.1p, ToS, or DSCP setting in the incoming flow is specified by the map group, the value will be remapped in the outgoing flow according to the map group.
- If the 802.1p, ToS, or DSCP setting in the incoming flow is not a value specified in the map group, the switch will do one of two things:

  If the *remap from* and *remap to* types are the same (802.1p to 802.1p, ToS to ToS, or DSCP to DSCP), the values in the outgoing flow will be unchanged. If the *remap from* and *remap to* types are not the same (for example: 802.1p to ToS), the switch will set the *remap to* value to zero (in this case, the ToS bit would be set to zero). The *remap to* value remains the same (in this case, the 802.1p bit would remain unchanged).
- A map action should not be combined with any other action. If another action parameter is specified, the flow will not be prioritized correctly.
- On the OmniSwitch 6624/6648, remapping is only supported from 802.1p to 802.1p and ToS/DSCP to 802.1p.
- Use the **no** form of the command to delete the map group from the configuration.

Examples

```
-> policy action a1 map 802.1p to 802.1p using mapGroup2
-> policy action a2 map 802.1p to tos using mapGroup3
```

Release History

Release 5.1; command was introduced.

Related Commands

policy map group	Configures a map group and its associated mappings for 802.1p, Type of Service (ToS), or Differentiated Services Code Point (DSCP) values.
qos apply	Applies configured QoS and policy settings to the current configuration.
policy action	Creates a policy action.
show policy action	Displays information about actions configured on the switch.
show policy map group	Displays information about all pending and applied policy map groups or a particular map group.

MIB Objects

```
alaQoSActionTable
   alaQoSActionMapFrom
   alaQoSActionMapTo
   alaQoSActionMapGroup
alaQoSAppliedActionTable
   alaQoSAppliedActionMapFrom
   alaQoSAppliedActionMapTo
   alaQoSAppliedActionMapGroup
```

policy action source rewrite ip

Used for IP translation. Configures a source IP address that should be used for outgoing flows associated with the specified action. This source address replaces the source IP address for packets in the flow that match the condition.

policy action *action_name* **source rewrite ip** *ip_address* **[mask** *netmask***]**

policy action *action_name* **no source rewrite ip**

Syntax Definitions

action_name	The name of the action.
ip_address	The IP address that should replace the source IP address in outgoing packets of the flow.
netmask	The network mask for the IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a source rewrite IP address from a policy action.
- A single source IP address may be translated to a single address; multiple source IP addresses may be translated to multiple addresses.
- Multiple source IP addresses may also be translated to a single IP address. This is referred to as network address translation (NAT).
- IP translation actions may be combined (for example, source rewrite IP address and destination rewrite IP address); however, a source rewrite IP address and a source rewrite network group and cannot be specified in the same action.
- IP translation actions cannot be combined with any other type of action (priority, bandwidth shaping, etc.).

Examples

```
-> policy action action2 source rewrite ip 10.10.2.3
-> policy action action2 no source rewrite ip
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition source ip	Configures a source IP address for a policy condition.
policy rule	Configures a policy rule on the switch. A rule is made up of a condition (for classifying incoming traffic) and an action (to be applied to outgoing traffic).
show policy action	Displays information about actions configured on the switch.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionSourceRewriteIpAddr
   alaQoSActionSourceRewriteIpMask
   alaQoSActionSourceRewriteIpGroup
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionSourceRewriteIpAddr
   alaQoSAppliedActionSourceRewriteIpMask
   alaQoSAppliedActionSourceRewriteIpGroup
```

policy action source rewrite network group

Used for IP translation. Specifies a source network group that should be used for outgoing flows associated with the specified action. When the action is included in a policy rule, addresses in the source rewrite network group replace the source IP address(es) specified in the condition.

policy action *action_name* **source rewrite network group** *network_group*

policy action *action_name* **no source rewrite network group**

Syntax Definitions

action_name	The name of the action.
network_group	The name of the network group, configured through the **policy network group** command.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a source rewrite IP address from a policy action.
- A single source IP address may be translated to a single address; multiple source IP addresses may be translated to multiple addresses.
- Multiple source IP addresses may also be translated to a single IP address.
- IP translation actions may be combined (for example, source rewrite network group and destination rewrite network group); however, a source rewrite network group and a source rewrite IP address cannot be specified in the same action.
- IP translation actions cannot be combined with any other type of action (priority, bandwidth shaping, etc.).

Examples

```
-> policy action action2 source rewrite network group netgroup4
-> policy action action2 no source rewrite network group
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy network group	Configures a network group name and its associated IP addresses.
policy condition	Creates a QoS policy condition. The condition determines what parameters the switch uses to classify incoming flows.

MIB Objects

```
alaQoSActionTable
   alaQoSActionSourceRewriteIpGroup
alaQoSAppliedActionTable
   alaQoSAppliedActionSourceRewriteIpGroup
```

policy action destination rewrite ip

Used for IP translation. Configures a destination IP address that should be used for outgoing flows associated with the specified action. This destination address replaces the destination IP address in the condition.

policy action *action_name* **destination rewrite ip** *ip_address* **[mask** *netmask***]**

policy action *action_name* **no destination rewrite ip**

Syntax Definitions

action_name	The name of the action.
ip_address	The IP address that should replace the destination IP address in outgoing packets of the flow.
netmask	The network mask for the IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a destination rewrite IP address from a policy action.
- There is a one-to-one correspondence between the destination rewrite address and the destination IP address given in the condition. A single destination IP address may be translated to a single address; multiple destination IP addresses may be translated to multiple addresses.
- IP translation actions may be combined (for example, destination rewrite IP address and source rewrite IP address); however, a destination rewrite IP address and a destination rewrite network group and cannot be specified in the same action.
- IP translation actions cannot be combined with any other type of action (priority, bandwidth shaping, etc.).

Examples

```
-> policy action action2 destination rewrite ip 10.10.2.1
-> policy action action3 destination rewrite ip 198.60.82.0/24
-> policy action action2 no destination rewrite ip
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition destination ip	Configures a destination IP address for a policy condition.
show policy action	Displays information about actions configured on the switch.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionDestinationRewriteIpAddr
   alaQoSActionDestinationRewriteIpMask
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionDestinationRewriteIpAddr
   alaQoSAppliedActionDestinationRewriteIpMask
```

policy action destination rewrite network group

Used for IP translation. Configures a destination network group that should be used for outgoing flows associated with the specified action. When the action is included in a policy rule, addresses in the destination rewrite network group replace destination IP addresses specified in the destination network group in the condition.

policy action *action_name* **destination rewrite network group** *network_group*

policy action *action_name* **no destination rewrite network group**

Syntax Definitions

action_name	The name of the action.
network_group	The name of the network group, configured through the **policy network group** command.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a destination rewrite IP address from a policy action.
- There is a one-to-one correspondence between the destination rewrite address and the destination IP address given in the condition. A single destination IP address may be translated to a single address; multiple destination IP addresses may be translated to multiple addresses.
- IP translation actions may be combined (for example, destination rewrite network group and source rewrite network group); however, a destination rewrite network group and a destination rewrite IP address cannot be specified in the same action.
- IP translation actions cannot be combined with any other type of action (priority, bandwidth shaping, etc.).

Examples

```
-> policy action action2 destination rewrite network group netgroup7
-> policy action action2 no destination rewrite ip
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy network group	Configures a network group name and its associated IP addresses.
policy condition	Creates a QoS policy condition. The condition determines what parameters the switch uses to classify incoming flows.
show policy action	Displays information about all pending and applied policy actions or a particular policy action configured on the switch.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionDestinationRewriteIpGroup
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionDestinationRewriteIpGroup
```

policy action load balance group

Associates a server load balance group with a policy action. Server load balancing is configured through the Server Load Balancing commands.

policy action *action_name* **load balance group** *slb_cluster*

policy action *action_name* **no load balance group**

Syntax Definitions

action_name	The name of the action.
slb_cluster	The name of the server load balance cluster, which is configured through the **ip slb cluster** command.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a load balance cluster from a policy action.
- Load balance groups are only supported for routed traffic; they do not work with bridged traffic.
- You cannot combine a load balance group action with any other action.

Examples

```
-> policy action action4 load balance group hr_servers
-> policy action action4 no load balance group
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
ip slb cluster	Configures a server load balancing (SLB) cluster on a switch.
show policy action	Displays information about all pending and applied policy actions or a particular policy action configured on the switch.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionLoadBalanceGroup
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionLoadBalanceGroup
```

policy action alternate gateway ip

Used for Policy Based Routing. Routed flows to which this action is applied will be directed to the IP address specified in the action if a route for the flow does not already exist in the switch routing table.

policy action *action_name* **alternate gateway ip** *ip_address*

policy action *action_name* **no alternate gateway ip**

Syntax Definitions

action_name	The name of the action.
ip_address	The destination IP address to which packets may be routed.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a gateway IP address from a policy action.
- Use this command to route Layer 3 traffic that matches the policy and does not already have a route in the switch routing table. Use the **policy action permanent gateway ip** command to route Layer 3 traffic that matches the policy regardless of whether or not a route exists for the traffic in the routing table.
- If the gateway goes down, traffic to be routed to the gateway will be sent over the relevant route in the switch's routing table. If there is no route in the routing table, the traffic will be dropped.

Examples

```
-> policy action pbr alternate gateway ip 10.10.2.1
-> policy action pbr no alternate gateway ip
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
show policy action	Displays information about actions configured on the switch.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionAlternateGatewayIpAddr
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionAlternateGatewayIpAddr
```

policy action permanent gateway ip

Used for Policy Based Routing (PBR). Routed flows to which this action is applied will be directed to the IP address specified in the action regardless of whether or not a route already exists in the switch routing table.

policy action *action_name* **permanent gateway ip** *ip_address*

policy action *action_name* **no permanent gateway ip**

Syntax Definitions

action_name	The name of the action.
ip_address	The destination IP address to which packets will be routed.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove a gateway IP address from a policy action.
- Use this command to route Layer 3 traffic that matches the policy, regardless of whether or not a route already exists in the routing table. Use the **policy action alternate gateway ip** command to route Layer 3 traffic that matches the policy only if no route exists in the routing table.
- If the gateway goes down, the traffic to be routed over the gateway will be dropped.

Examples

```
-> policy action pbr2 permanent gateway ip 10.10.2.1
-> policy action pbr2 no permanent gateway ip
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
show policy action	Displays information about actions configured on the switch.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionPermanentGatewayIpAddr
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionPermanentGatewayIpAddr
```

qos port reset

Resets all QoS port configuration to the default values.

qos port *slot/port* **reset**

Syntax Definitions

slot/port	The physical slot and port number. For example: 3/1.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

The QoS port configuration parameters that are reset include:

parameter	default
default queues	4
trusted	not trusted
maximum reserve bandwidth	The maximum bandwidth allowed for the interface type. *Currently not supported.*
maximum signal bandwidth	The maximum bandwidth allowed for the interface type. *Currently not supported.*
maximum default buffers	The maximum buffers allowed for the interface type.

Examples

```
-> qos port 3/1 reset
```

Release History

Release 5.1; command was introduced.

MIB Objects

```
alaQoSPortTable
   alaQoSPortSlot
   alaQoSPortPort
   alaQoSPortReset
```

qos port

Configures a physical port for QoS.

qos port *slot/port*
[default queues {2 | 4}]
[servicing mode]
[trusted]
[maximum reserve bandwidth *bps***]**
[maximum signal bandwidth *bps***]**
[maximum default depth *bytes***]**
[maximum default buffers *max_default_buffers***]**
[default 802.1p *value***]**
[default dscp *value***]**
[default classification {802.1p | tos | dscp}]
[enqueuing thresholds]
[protocol priority]

Syntax Definitions

slot/port	The physical slot and port number. For example: 4/1.

Defaults

- Mobile ports and ports enabled for 802.1Q are always trusted; by default, any other ports are not trusted.
- By default, QoS ports do not preempt queues of lower priority.

parameter	default
2 | 4	4

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **trusted** option to change the trust mode for the port.

Examples

```
-> qos port 3/1 trusted
-> qos port 4/2 no trusted
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
qos port	Configures whether the default mode for QoS ports is trusted or untrusted.
show qos port	Displays information about QoS ports.

MIB Objects

```
alaQoSPortTable
   alaQoSPortSlot
   alaQoSPortPort
   alaQoSPortTrusted
   alaQoSPortDefault8021p
   alaQoSPortDefaultDSCP
   alaQoSPortMaximumReservedBandwidth
   alaQoSPortAppliedMaximumReservedBandwidth
   alaQoSPortMaximumSignalledBandwidth
   alaQoSPortAppliedMaximumSignalledBandwidth
   alaQoSPortDefaultQueues
   alaQoSPortAppliedDefaultQueues
   alaQoSPortMaximumDefaultBandwidth
   alaQoSPortAppliedMaximumDefaultBandwidth
   alaQoSPortMaximumDefaultDepth
   alaQoSPortAppliedMaximumDefaultDepth
   alaQoSPortMaximumDefaultBuffers
   alaQoSPortAppliedMaximumDefaultBuffers
   alaQoSPortDefaultClassification
   alaQoSPortAppliedDefaultClassification
   alaQoSPortLowPriorityWeight
   alaQoSPortAppliedLowPriorityWeight
   alaQoSPortMediumPriorityWeight
   alaQoSPortAppliedMediumPriorityWeight
   alaQoSPortHighPriorityWeight
   alaQoSPortAppliedHighPriorityWeight
   alaQoSPortUrgentPriorityWeight
   alaQoSPortAppliedUrgentPriorityWeight
```

qos port default queues

Configures the number of default queues for the QoS port. Default queues are the queues created for the port when the switch is booted up. *Not supported in the current release.*

qos port *slot/port* **default queues [2 | 4]**

Syntax Definitions

slot/port	The slot and port number on which default queues are created.
2 | 4	The number of default queues that are created for the specified port at switch startup.

Defaults

parameter	default
2 | 4	4

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- If you do not enter a value, the default value is used.
- Default queues are created at startup. QoS queues are created when a flow matches a policy with at least one configured action parameter (other than disposition). A flow that matches a policy which has a disposition of **accept** but no other action parameters configured will be placed in a default queue. All other flows are placed in default queues.
- For 802.1p or ToS traffic coming into the switch that does not match a policy, the switch places the traffic into a default queue based on the 802.1p bit value.

2 default queues/port	• low priority default queue services 802.1p values of 0–3 • high priority default queue services 802.1p values of 4–7
4 default queues/port	• lowest priority default queue services 802.1p values of 0–1 • low priority default queue services 802.1p values of 2–3 • higher priority default queue services 802.1p values of 4–5 • highest priority queue services 802.1p values of 6–7

- By default switch ports are not “trusted;” that is, they do not recognize 802.1p or ToS bits. The ports, however, may be configured to recognize 802.1p or ToS bits through the **qos port trusted** command. See page 38-167 for more information about this command.

Examples

```
-> qos port 3/2 default queues 4
-> qos port 3/1 default queues
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
qos port	Configures a physical port for QoS.
show qos port	Displays information about QoS ports.
qos port trusted	Configures whether an individual port is trusted or untrusted.

MIB Objects

```
alaQoSPortTable
   alaQoSPortDefaultQueues
   alaQoSPortAppliedDefaultQueues
```

qos port trusted

Configures whether an individual port is trusted or untrusted. When a port is trusted, the switch will recognize 802.1p or ToS bits in incoming packets and will give priority to packets based on the values.

qos port *slot/port* **trusted**

qos port *slot/port* **no trusted**

Syntax Definitions

slot/port	The slot number and port number of the physical port.

Defaults

By default, QoS ports are not trusted.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **qos trust ports** command to set the default trust mode for all QoS ports. The **qos port trusted** command may be used to override the default.
- The setting applies only to ports with incoming traffic.
- If the port is not trusted, the switch sets any 802.1p or ToS bits to zero in the incoming packet.
- Mobile ports and ports configured for 802.1Q are always trusted.

Examples

```
-> qos port 3/1 trusted
-> qos port 4/2 no trusted
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
qos port	Configures a physical port for QoS.
qos trust ports	Configures the global trust mode for QoS ports.
show qos port	Displays information about QoS ports.

MIB Objects

```
alaQoSPortTable
   alaQoSPortTrusted
```

qos port maximum reserve bandwidth

Configures the maximum amount of physical port bandwidth that may be reserved on a port. *Not supported in the current release*.

qos port *slot/port* **maximum reserve bandwidth** *bps*

qos port *slot/port* **no maximum reserve bandwidth**

Syntax Definitions

slot/port	The slot number and port number of the physical port.
bps	The maximum amount of bandwidth that may be reserved on the port (in bits per second). The value may be entered as an integer (for example, **10000**) or with abbreviated units (for example, **10k**). If the value is entered in bits per second, the switch rounds the value up to the nearest thousand.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

The maximum amount of bandwidth is the amount allowed by all policies (configured through the CLI and PolicyView) for the port.

Examples

```
-> qos port 3/1 maximum reserve bandwidth 1000
-> qos port 3/1 no maximum reserve bandwidth
-> qos port 3/1 maximum reserve bandwidth 10k
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
qos port	Configures a physical port for QoS.
show qos port	Displays information about QoS ports.

MIB Objects

```
alaQoSPortTable
   alaQoSPortSlot
   alaQoSPortPort
   alaQoSPortMaximumReservedBandwidth
   alaQoSAppliedPortMaximumReservedBandwidth
```

qos port maximum signal bandwidth

Configures the maximum amount of physical port bandwidth that may be requested by RSVP flows on the port. *Not supported in the current release*.

qos port *slot/port* **maximum signal bandwidth** *bps*

qos port *slot/port* **no maximum signal bandwidth**

Syntax Definitions

slot/port	The slot number and port number of the physical port.
bps	The maximum amount of bandwidth that may be requested by RSVP flows on the port (in bits per second).The value may be entered as an integer (for example, **10000**) or with abbreviated units (for example, **10k**). If the value is entered in bits per second, the switch rounds the value up to the nearest thousand.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The maximum amount of bandwidth is the amount allowed by all policies (configured through the CLI and PolicyView) for the port.

Examples

```
-> qos port 4/1 maximum signal bandwidth 10000
-> qos port 4/1 maximum signal bandwidth 10k
-> qos port 4/1 no maximum signal bandwidth
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
qos port	Configures a physical port for QoS.
show qos port	Displays information about QoS ports.

MIB Objects

```
alaQoSPortTable
   alaQoSPortSlot
   alaQoSPortPort
   alaQoSPortMaximumSignalledBandwidth
   alaQoSAppliedPortMaximumSignalledBandwidth
```

qos port maximum default depth

Configures the maximum queue depth allowed for a default queue. *Not supported in the current release.*

qos port *slot/port* **maximum default depth** *bytes*

qos port *slot/port* **no maximum default depth**

Syntax Definitions

slot/port	The slot number and port number of the physical port.
bytes	The maximum queue depth for a default queue associated with the specified slot and port.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Queue depth determines the amount of buffer allocated to a queue. When the queue depth is reached, the switch starts to drop packets.
- Use the **no** form of the command to remove maximum default depth from a port.
- Modifying the maximum depth of a default queue is most useful for low-bandwidth links.

Examples

```
-> qos port 3/1 maximum default depth 100
-> qos port 3/1 no maximum default depth
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
qos port	Configures a physical port for QoS.
show qos port	Displays information about QoS ports.

MIB Objects

```
alaQoSPortTable
   alaQoSPortSlot
   alaQoSPortPort
   alaQoSPortMaximumDefaultDepth
   alaQoSAppliedPortMaximumDefaultDepth
```

qos port maximum default buffers

Configures the maximum number of buffers that may be allocated to a default queue. *Not supported in the current release.*

qos port *slot/port* **maximum default buffers** *max_default_buffers*

qos port *slot/port* **no maximum default buffers**

Syntax Definitions

slot/port	The slot number and port number of the physical port.
max_default_buffers	The maximum number of buffers that may be allocated to a default queue. The range of values is 0–2048. The maximum number depends on the interface type.

Defaults

parameter	default
max_default_buffers	64 (ENI) 192 (GNI)

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Modifying the maximum buffers for best effort queues is most useful for low-bandwidth links.
- Use the **no** form of the command to return the maximum best effort buffers value to its default (64).

Examples

```
-> qos port 3/1 maximum default buffers 2048
-> qos port 3/1 no maximum default buffers
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
qos port	Configures a physical port for QoS.
show qos port	Displays information about QoS ports.

MIB Objects

```
alaQoSPortTable
   alaQoSPortSlot
   alaQoSPortPort
   alaQoSPortMaximumDefaultBuffers
```

```
   alaQoSAppliedPortMaximumDefaultBuffers
```

qos port default 802.1p

Configures the 802.1p value to be inserted in flows ingressing on an untrusted port.

qos port *slot/port* **default 802.1p** *value*

Syntax Definitions

slot/port	The slot number and port number of the physical port.
value	The priority value to be set. Values range from 0 (lowest priority) to 7 (highest priority).

Defaults

parameter	default
value	0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

By default untrusted ports will set the 802.1p bit to zero on incoming flows. Use this command to specify that a different 802.1p value should be applied to the flow.

Examples

```
-> qos port 3/1 default 802.1p 5
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
qos port	Configures a physical port for QoS.
show qos port	Displays information about QoS ports.

MIB Objects

```
alaQoSPortTable
   alaQoSPortDefault8021p
   alaQoSAppliedPortDefault8021p
```

qos port default dscp

Configures the ToS/DSCP value to be inserted in flows ingressing on an untrusted port.

qos port *slot/port* **default dscp** *value*

Syntax Definitions

slot/port	The slot number and port number of the physical port.
value	The ToS/DSCP value. The range is 0–63.

Defaults

parameter	default
value	0

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

The value configured by this command sets the upper byte (precedence) and therefore configures the ToS/DSCP value for the port.

Examples

```
-> qos port 3/1 default dscp 63
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
qos port	Configures a physical port for QoS.
show qos port	Displays information about QoS ports.

MIB Objects

```
alaQoSPortTable
   alaQoSPortDefaultDSCP
   alaQoSAppliedPortDefaultDSCP
```

qos port default classification

Specifies how traffic is classified on a high-density gigabit port.

qos port *slot/port* **default classification {802.1p | tos | dscp}**

Syntax Definitions

slot/port	The slot number and port number of the physical port.
802.1p	Specifies that 802.1p will be used to prioritize flows coming in on the port.
tos	Specifies that ToS will be used to prioritize flows coming in on the port.
dscp	Specifies that DSCP will be used to prioritize flows coming in on the port.

Defaults

parameter	default
802.1p | tos | dscp	802.1p

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Use this command to change how ingress IP packets are classified on high-density gigabit ports. (In some network situations, some IP traffic may be dropped before any QoS rules can take effect for the traffic.)
- This command does not affect Layer 2 traffic, which is always classified with 802.1p.
- On trusted ports, priority is determined by the 802.1p/ToS/DSCP value in the flow; on untrusted ports, the priority is determined by the setting of the **qos port default 802.1p** and **qos port default dscp** commands. The port default classification is then used for classifying the traffic on the port.
- The command is not supported for ports on other modules.

Examples

```
-> qos port 3/1 default classification tos
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
qos port	Configures a physical port for QoS.
show qos port	Displays information about QoS ports.

MIB Objects

```
alaQoSPortTable
   alaQoSPortDefaultClassification
   alaQoSPorAppliedtDefaultClassification
```

qos port enqueuing thresholds

Specifies the First In First Out (FIFO) thresholds on a high-density gigabit Ethernet port for enqueuing packets. Packets are discarded when the upper threshold is reached for each internal priority.

qos port *slot/port* **enqueuing thresholds** *up0-low0 up1-low1 up2-low2 up3-low3*

qos port *slot/port* **no enqueuing thresholds**

Syntax Definitions

slot/port	The high-density slot/port on which the enqueuing thresholds are configured.
up0	The value of the desired upper enqueuing threshold on the specified port for frames with internal priority 0. The range is 0 to 4095. The value must be greater than *low0*.
low0	The value of the desired lower enqueuing threshold on the specified port for frames with internal priority 0. The range is 0 to 4095. The value must be less than *up0*.
up1	The value of the desired upper enqueuing threshold on the specified port for frames with internal priority 1. The range is 0 to 4095. The value must be greater than *low1*.
low1	The value of the desired lower enqueuing threshold on the specified port for frames with internal priority 1. The range is 0 to 4095. The value must be less than *up1*.
up2	The value of the desired upper enqueuing threshold on the specified port for frames with internal priority 2. The range is 0 to 4095. The value must be greater than *low2*.
low2	The value of the desired lower enqueuing threshold on the specified port for frames with internal priority 2. The range is 0 to 4095. The value must be less than *up2*.
up3	The value of the desired upper enqueuing threshold on the specified port for frames with internal priority 3. The range is 0 to 4095. The value must be greater than *low3*.
low3	The value of the desired lower enqueuing threshold on the specified port for frames with internal priority 3. The range is 0 to 4095. The value must be less than *up3*.

Defaults

parameter	default
up0	30
low0	10
up1	35
low1	10
up2	40
low2	10
up3	575
low3	260

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to return the thresholds to the defaults.
- The enqueuing thresholds control the memory availability on the port First In First Out (FIFO) mechanism. The thresholds specify a count of the number of "chunks" of buffer for packets with the corresponding internal priority. When the upper threshold is reached, packets with that internal priority will be discarded. When the lower threshold is reached, packets with that internal internal priority will be enqueued rather than discarded.
- If all upper thresholds are set to 0, all packets will be discarded. If all upper thresholds are set to 4095 (top of the data buffer), FIFO discarding is disabled.
- A "chunk" is 64 bytes of the 256-Kbyte buffer on the high-density interface (4096 possible chunks). Every received packet on the high-density interface may be stored in a 64-byte chunk of the buffer.

Examples

```
-> qos port 1/3 enqueuing thresholds 30-10 35-10 55-10 500-200
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
qos port protocol priority	Specifies the internal priority for incoming priority frames on a QoS port. The internal priority is used for queuing.
show qos port high-density-module	Displays information about the enqueuing thresholds on high-density QoS ports.

MIB Objects

```
alaQoSPortTable
   alaQoSPortSlot
   alaQoSPortPort
   alaQoSPortEnqueuingThresholdP0Upper
   alaQoSPortEnqueuingThresholdP0Lower
   alaQoSPortEnqueuingThresholdP1Upper
   alaQoSPortEnqueuingThresholdP1Lower
   alaQoSPortEnqueuingThresholdP2Upper
   alaQoSPortEnqueuingThresholdP2Lower
   alaQoSPortEnqueuingThresholdP3Upper
   alaQoSPortEnqueuingThresholdP3Lower
```

qos port protocol priority

Specifies the internal priority for incoming priority frames of a particular protocol type on a high-density gigabit Ethernet QoS port. The internal priority is used for queuing.

qos port *slot/port* **protocol** *id* **[priority {***p0 p1 p2 p3 p4 p5 p6 p7***}] [classification {tos | 802.1p | dscp}]**

qos port *slot/port* **no protocol** *id*

Syntax Definitions

slot/port	The high-density slot/port number for this protocol priority.
id	The protocol ID associated with the port. Possible values include: user1, user2, user3, user4, arp, rarp, ipv6, ipx, apple, sna, decnet.
p0 p1 p2 p3 p4 p5 p6 p7	Maps ingress priority values from ToS or 802.1p frames on this slot/port to internal priority values. There are four internal priorities (0 to 3, lowest to highest).
tos	Specifies that the ToS priority in incoming packets with this protocol will be mapped to the specified **priority** value to determine the internal priority.
802.1p	Specifies that the 802.1p priority in incoming packets with this protocol will be mapped to the specified **priority** value to determine the internal priority.
dscp	Specifies that the DiffServ priority value of incoming packets with this protocol will be used to determine the internal priority. If **dscp** is specified, **priority** cannot be specified. The switch uses a separate method to calculate the internal priority for DiffServ traffic.

Defaults

parameter	default
p0	0
p1	0
p2	1
p3	1
p4	2
p5	2
p6	3
p7	3

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- The port must be trusted in order for this command to take effect. Port may be configured as trusted through the **qos trust ports** command or **qos port trusted** command.
- The internal priorities are indexed in the switch based on an internal protocol number (extracted from the protocol CAM of the high-density module). Protocol CAM entries are built-in and may be manually configured through the **qos slice** command.
- Priority values cannot be changed for IPV4, LACP, or BPDU protocols. To change priority values on these protocols, specify a user protocol (**user1**, **user2**, **user3**, or **user4**) and set the desired priorities. The ethernet type for the user protocol may be specified by the **qos slice** command.
- If classification is set to **tos** or **dscp**, the protocol may only be set to **user1**, **user2**, **user3**, **user4**, or **ipv4**. All other protocols will use the default ToS or DSCP value, which may be configured through the **qos port default dscp** command.
- If packets arrive on the port with an unknown protocol, the default priority is used. The default priority is based on the 802.1p, ToS, or DSCP value configured on the port through the **qos port default 802.1p** or **qos port default dscp** command.

Examples

```
-> qos port 1/3 protocol arp priority 0 0 1 1 2 2 2 3 classification 802.1p
-> qos port 1/3 no protocol arp
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
qos slice	Creates an entry in the protocol CAM of a high-density gigabit Ethernet slot/slice.
qos slice dscp	Modifies the internal table for mapping DSCP values to internal priorities.
show qos port	Displays information about all QoS ports or a particular port.

MIB Objects

```
alaQoSPortProtocolTable
   alaQoSPortSlot
   alaQoSPortPort
   alaQoSProtocolId
   alaQoSPortProtocolPriorityP0
   alaQoSPortProtocolPriorityP1
   alaQoSPortProtocolPriorityP2
   alaQoSPortProtocolPriorityP3
   alaQoSPortProtocolPriorityP4
   alaQoSPortProtocolPriorityP5
   alaQoSPortProtocolPriorityP6
   alaQoSPortProtocolPriorityP7
   alaQoSPortProtocolClassification
```

qos slice

Creates an entry in the protocol CAM of a high-density gigabit Ethernet slot/slice. Protocol CAM entries are used by the switch for calculating internal protocol numbers.

qos slice *slot/slice* **protocol** *id* **ethertype** *etype* **[dsapssap** *dsap/ssap***] [802.3 {enable | disable}] [priority | fallback]**

qos slice *slot/slice* **no protocol** *id*

Syntax Definitions

slot/slice	The slot/slice number associated with the protocol CAM entry. A *slice* is a logical section of hardware that corresponds to particular ports on a network interface module. On the OmniSwitch 7700/7800, each interface has one slice (slice 0). On the OmniSwitch 8800, each interface may have up to 4 slices (slices 0 to 3).
id	The protocol ID for this user-configured CAM entry. Possible values are **user1**, **user2**, **user3**, and **user4**.
etype	The Ethernet type code for this CAM entry (for example, **0800** indicates an IP packet; **0806** indicates an ARP packet).
dsap	The destination Service Access Point (SAP) code for this CAM entry.
ssap	The source Service Access Point (SAP) code for this CAM entry.
priority	Indicates that this CAM entry should have precedence over built-in CAM entries.
fallback	Indicates that built-in CAM entries should have precedence over this entry.
enable	Enables 802.3 for this protocol CAM entry.
disable	Disables 802.3 for this protocol CAM entry.

Defaults

parameter	default
type	0
dssap/ssap	0/0
priority | fallback	priority
enable | disable	disable

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- A maximum of two priority and two fallback entries may be configured per slot/slice.
- Every frame received on the high-density gigabit slot/slice is assigned an internal priority number based on the ingress priority value, the MAC port, and the protocol of the frame. There are four internal priorities (0 to 3, lowest to highest). The assignment of internal priority may be manually configured per port through the **qos port protocol priority** command.
- When a frame arrives on the high-density port, the switch examines the packet based on the protocol CAM entries and creates a 4-bit internal protocol number. The protocol number is used to index internal priorities. For ToS and 802.1p frames, the port number is also used to index internal priorities.

Examples

```
-> qos slice 3/0 protocol user2 ethertype 800 dsap aa ssap aa priority
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
qos port protocol priority	Specifies the internal priority for incoming priority frames on a QoS port.
show qos slice high-density-module	Displays information about servicing thresholds and WRED thresholds for slots/slices on high-density gigabit modules.

MIB Objects

```
alaQoSSlotProtocol
   alaQoSSlotProtocolSlot
   alaQoSSlotProtocolSlice
   alaQoSSlotProtocolId
   alaQoSSlotProtocolEthertype
   alaQoSSlotProtocolType
   alaQoSSlotProtocolDsap
   alaQoSSlotProtocolSsap
   alaQoSSlotProtocol8023Enabled
```

qos slice dscp

Modifies the internal table for mapping DSCP values to internal priorities on high-density gigabit modules.

qos slice *slot/slice* **dscp** *index value*

Syntax Definitions

slot/slice	The slot number and slice for which you want to view information. A *slice* is a logical section of hardware that corresponds to particular ports on a network interface module. On the OmniSwitch 7700/7800, each interface has one slice (slice 0). On the OmniSwitch 8800, each interface may have up to 4 slices (slices 0 to 3).
index	The index value for mapping internal priority for DSCP. (See table in "Defaults" below.)
value	The internal priority value to which DSCP traffic with this index should be mapped.

Defaults

The default internal priority mapping for DSCP is listed here:

index	value (internal priority)
0–15	0
16–31	1
32–47	2
48–63	3

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

Use this command to change the way DSCP traffic coming in on a high-density port is indexed to internal priority.

Examples

```
-> qos slice 2/0 dscp 30 2
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
qos slice	Creates an entry in the protocol CAM of a high-density gigabit Ethernet slot/slice.

MIB Objects

```
alaQoSSlotDscpTable
   alaQoSSlotDscpSlot
   alaQoSSlotDscpSlice
   alaQoSSlotDscpIndex
   alaQoSSlotDscpPriority
```

qos slice servicing mode

Specifies the dequeuing algorithm for a slot/slice on a high-density gigabit module.

qos slice *slot/slice* **servicing mode {strict-priority | wrr | priority-wrr [***p1 p2 p3***]}**

Syntax Definitions

slot/slice	The slot and slice number to which this servicing mode applies. A *slice* is a logical section of hardware that corresponds to particular ports on a network interface module. On the OmniSwitch 7700/7800, each interface has one slice (slice 0). On the OmniSwitch 8800, each interface may have up to 4 slices (slices 0 to 3).
strict-priority	Indicates that the highest priority packets should always be sent first.
wrr	Indicates that the Weighted Round Robin algorithm should be used for dequeueing on this slot/slice. Packets of each priority are sent out on each "round," with higher priority queues sending more packets than lower priority queues.
priority-wrr	Indicates the Priority Weighted Round Robin algorithm should be used for dequeueing on this slot/slice. The default thresholds may be used; or the thresholds may be user-configured. The Priority Weighted Round Robin algorithm sends out packets in the same round robin sequence as the Weighted Round Robin algorithm—until a threshold is reached. When a threshold is reached, only packets with that priority are sent out.
p1 p2 p3	The value of the desired servicing thresholds for Priority Weighted Round Robin for incoming packets with priority 1 to 3. The range is 0 to 4095. Each threshold specifies a maximum number of "chunks" of buffer for packets of a particular priority. When a threshold is reached, only packets with that priority are sent out.

Defaults

The default servicing mode is Priority Weighted Round Robin (**priority-wrr**).The default servicing mode is Priority Weighted Round Robin, which sets the default thresholds to the following:

parameter	default
p1	90
p2	180
p3	360

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- A "chunk" is 64 bytes of the 256-Kbyte buffer on the high-density interface (4096 possible chunks). Every received packet on the high-density interface may be stored in a 64-byte chunk of the buffer.

- Changing the servicing mode changes the servicing thresholds. If you change the mode to **strict-priority**, the thresholds are set to zero. If you change the mode to **wrr**, the thresholds are each set to 4095.
- The threshold for priority 0 packets cannot be modified. If the servicing mode is set to Priority Weighted Round Robin (the default), the priority 0 threshold is set to 45.
- If the threshold for a priority is exceeded, packets with that priority are sent first. For example, if *p2* is set to 150, and 150 is exceeded, any incoming packets with a priority of 2 will be sent first.

Examples

```
-> qos slice 2/0 servicing mode strict-priority
-> qos slice 3/0 servicing mode wrr
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
qos slice wred thresholds	Specifies the buffer accumulation thresholds and weight for the Weighted Random Early Detection (WRED) discarding algorithm on a high-density gigabit slot/slice.
show qos slice high-density-module	Displays information for QoS slices of QoS slots on high-density gigabit modules only

MIB Objects

```
alaQoSSlotTable
   alaQoSSlotSlot
   alaQoSSlotSlice
   alaQoSSlotCbqThresholdP1
   alaQoSSlotCbqThresholdP2
   alaQoSSlotCbqThresholdP3
   alaQoSSlotCbqThresholdMode
```

qos slice wred thresholds

Specifies the buffer accumulation thresholds and weight for the Weighted Random Early Detection (WRED) discarding algorithm on a high-density gigabit slot/slice.

qos slice *slot/slice* **wred thresholds** *up0-low0 up1-low1 up2-low2 up3-low3* **[weight** *weight_value***]**

qos slice *slot/slice* **no wred thresholds**

Syntax Definitions

slot/slice	The slot number and slice number on which you want to configure WRED thresholds. A *slice* is a logical section of hardware that corresponds to particular ports on a network interface module. On the OmniSwitch 7700/7800, each interface has one slice (slice 0). On the OmniSwitch 8800, each interface may have up to 4 slices (slices 0 to 3).
up0-low0	The upper and lower thresholds of the average buffer "chunk" count for frames with priority 0. (See Usage Guidelines for the definition of "chunk.") When the lower threshold is reached, some frames with priority 0 are discarded; when the upper threshold is reached, all frames with priority 0 are discarded. Valid ranges are 0 to 4095. The upper threshold must be higher than the lower threshold.
up1-low1	The upper and lower thresholds of the average buffer "chunk" count for frames with priority 1. (See Usage Guidelines for the definition of "chunk.") When the lower threshold is reached, some frames with priority 1 are discarded; when the upper threshold is reached, all frames with priority 1 are discarded. Valid ranges are 0 to 4095. The upper threshold must be higher than the lower threshold.
up2-low2	The upper and lower thresholds of the average buffer "chunk" count for frames with priority 2. (See Usage Guidelines for the definition of "chunk.") When the lower threshold is reached, some frames with priority 2 are discarded; when the upper threshold is reached, all frames with priority 2 are discarded. Valid ranges are 0 to 4095. The upper threshold must be higher than the lower threshold.
up3-low3	The upper and lower thresholds of the average buffer "chunk" count for frames with priority 3. (See Usage Guidelines for the definition of "chunk.") When the lower threshold is reached, some frames with priority 3 are discarded; when the upper threshold is reached, all frames with priority 3 are discarded. Valid ranges are 0 to 4095. The upper threshold must be higher than the lower threshold.
weight_value	A value used to compute the average chunk count, in the range 1 through 7. The value is a negative power of 2. (See Usage Guidelines for the definition of "chunk.")

Defaults

By default, WRED is disabled; that is, all thresholds are set to the maximum amount of chunks of buffer that may be used:

parameter	default
up0-low0	4095-4095
up1-low1	4095-4095
up2-low2	4095-4095
up3-low3	4095-4095
weight_value	4

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to return the thresholds to the defaults.
- The command enables WRED on the slot/slice when any of the thresholds are configured to be anything other than the default range of 0 to 4095.
- A “chunk” is 64 bytes of the 256-Kbyte buffer on the high-density interface (4096 possible chunks). Every received packet on the high-density interface may be stored in a 64-byte chunk of the buffer.
- The average chunk count is computed with the current chunk count and the *weight_value*.
- As the average chunk count gets closer to the upper threshold, more frames are discarded. The decision to discard is made randomly by the switch.
- To view which ports correspond to a particular slice on a slot, use the **show policy port group** command, which displays the built-in port groups by slot and slice.

Examples

```
-> qos slice 3/0 wred thresholds 30-10 35-10 40-10 575-260 weight 4
```

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
qos slice servicing mode	Specifies the queuing algorithm for a slot/slice on a high-density gigabit module.
show qos slice high-density-module	Displays information for QoS slices of QoS slots on high-density gigabit modules only

MIB Objects

```
alaQoSSlotTable
   alaQoSSlotSlot
   alaQoSSlotSlice
   alaQoSSlotWredThresholdP0Upper
   alaQoSSlotWredThresholdP0Lower
   alaQoSSlotWredThresholdP1Upper
   alaQoSSlotWredThresholdP1Lower
   alaQoSSlotWredThresholdP2Upper
   alaQoSSlotWredThresholdP2Lower
   alaQoSSlotWredThresholdP3Upper
   alaQoSSlotWredThresholdP3Lower
   alaQoSSlotWredAverageCounterWeight
```

show policy classify

Sends hypothetical information to the Layer 2, Layer 3, or multicast classifier to see how the switch will handle the packet. Used to verify that a policy rule works a particular way.

This section describes the base command. Optional keywords are listed below and described as separate commands later in this chapter. (Note that options may be used in combination but are described separately for ease in explanation.)

show policy classify {l2 | l3 | multicast} [applied]
[source port *slot/port***]**
[destination port *slot/port***]**
[source mac *mac_address***]**
[destination mac *mac_address***]**
[source vlan *vlan_id***]**
[destination vlan *vlan_id***]**
[source interface type {ethernet | **wan | ethernet-10 | ethernet-100 | ethernet-1G | ethernet-10G}]**
[destination interface type {ethernet | **wan | ethernet-10 | ethernet-100 | ethernet-1G | ethernet-10G}]**
[802.1p *value***]**
[source ip *ip_address***]**
[destination ip *ip_address***]**
[multicast ip *ip_address***]**
[tos *tos_value***]**
[dscp *dscp_value***]**
[ip protocol *protocol***]**
[source ip port *port***]**
[destination ip port *port***]**

Syntax Definitions

l2	Uses the Layer 2 classifier for the hypothetical packet. Typically specified for port, MAC address, VLAN, interface type, or 802.1p.
l3	Uses the Layer 3 classifier for the hypothetical packet. Typically specified for interface type, IP address, ToS or DSCP, IP protocol, or TCP/UDP port.
multicast	Uses the multicast IGMP classifier for the hypothetical packet. Typically specfied for multicast IP address (which is the multicast stream) and destination parameters (for the client issuing an IGMP request).
applied	Indicates that only applied policies should be examined.

Defaults

By default, only pending policies are examined.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use this command to determine if the switch will classify the traffic condition specified and match it to a policy. By default the classifier only tests pending policies (policies that have not yet been applied). Use the **applied** keyword to test only those policies that have been applied.
- If you specify multicast traffic, any destination parameters specified indicate the client(s) attempting to join a multicast group.
- Use the **qos apply** command to activate saved policies.
- See command descriptions in the next sections for more information about the individual options.

Examples

```
-> show policy classify l3 source ip 1.2.3.4 destination ip 198.60.22.2
destination ip port 80 ip protocol 6
Packet headers:
L3:
 *Port         :                                0/0  -> 0/0
 *MAC          :                  000000:000000  -> 000000:000000
 *VLAN         :                              0  -> 0
 *802.1p       : 0
L3/L4:
 *IP           :                        1.2.3.4  -> 198.60.22.2
 TCP           :                              0  -> 80
 *TOS/DSCP     : 0/0
Using pending l3 policies
Classify L3:
*Matches rule 'filter1': action pri3 (accept)
```

- Source and destination are indicated to the left and right of the arrow (->) respectively. A zero displays for values not requested in the hypothetical packet.
- Note that some fields only display for particular traffic types.

output definitions

L2/L3/L4	Indicates the type of traffic (Layer 2 or Layer 3/4).
Port	The physical slot/port of the theoretical traffic.
IfType	Displays for hypothetical Layer 2 packets only. The interface type of the packet.
MAC	The MAC address of the hypothetical packet.
VLAN	The VLAN ID of the hypothetical packet.
802.1p	The 802.1p value of the hypothetical packet.
Mcast	Displays for hypothetical multicast packets only. The multicast address of the hypothetical packet.
IP	The IP address of the hypothetical packet.
TCP	The TCP/UDP port of the hypothetical packet.
TOS/DSCP	The ToS or DSCP value of the hypothetical packet.

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.

MIB Objects

```
alaQoSClassifyTable
   alaQoSClassifySourceSlot
   alaQoSClassifySourcePort
   alaQoSClassifyDestinationSlot
   alaQoSClassifyDestinationPort
   alaQoSClassifySourceMac
   alaQoSClassifyDestinationMac
   alaQoSClassifySourceVlan
   alaQoSClassifyDestinationVlan
   alaQoSClassifySourceInterfaceType
   alaQoSClassifyDestinationInterfaceType
   alaQoSClassify8021p
   alaQoSClassifySourceIp
   alaQoSClassifyDestinationIp
   alaQoSClassifyMulticastIp
   alaQoSClassifyTos
   alaQoSClassifyDscp
   alaQoSClassifyIpProtocol
   alaQoSClassifySourceIpPort
   alaQoSClassifyDestinationIpPort
   alaQoSClassifyExecute
   alaQoSClassifyL2SourceResultRule
   alaQoSClassifyL2SourceResultDisposition
   alaQoSClassifyL2DestinationResultRule
   alaQoSClassifyL2DestinationResultDisposition
   alaQoSClassifyL3ResultRule
   alaQoSClassifyL3ResultDisposition
   alaQoSClassifyIGMPResultRule
   alaQoSClassifyIGMPResultDisposition
   alaQoSClassifyMulticastResultRule
   alaQoSClassifyMulticastResultDisposition
```

show policy classify source port

Specifies a source port for a hypothetical packet to show how the QoS software in the switch will handle the packet.

show policy classify {l2 | l3 | multicast} [applied] source port *slot/port*

Syntax Definitions

l2	Uses the Layer 2 classifier for the hypothetical packet.
l3	Uses the Layer 3 classifier for the hypothetical packet.
multicast	Uses the multicast IGMP classifier for the hypothetical packet.
applied	Indicates that only applied policies should be examined.
slot/port	The slot and port number of the source address of the flow.

Defaults

By default, only pending policies are examined.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use this command to determine if the switch will classify the traffic condition specified and match it to a policy. By default the classifier only tests pending policies (policies that have not yet been applied). Use the **applied** keyword to test only those policies that have been applied.
- Use the **qos apply** command to activate saved policies.

Examples

```
-> show policy classify l2 source port 3/1
```

See the output example given on page 38-195 for more information about the potential screen display.

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
show policy classify	Describes the base command.

MIB Objects

```
alaQoSClassifyTable
   alaQoSClassifySourceSlot
   alaQoSClassifySourcePort
```

show policy classify destination port

Specifies a destination port for a hypothetical packet to show how the QoS software in the switch will handle the packet.

show policy classify {l2 | l3 | multicast} [applied] destination port *slot/port*

Syntax Definitions

l2	Uses the Layer 2 classifier for the hypothetical packet.
l3	Uses the Layer 3 classifier for the hypothetical packet.
multicast	Uses the multicast IGMP classifier for the hypothetical packet.
applied	Indicates that only applied policies should be examined.
slot/port	The slot and port number of the destination address of the flow.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use this command to determine if the switch will classify the traffic condition specified and match it to a policy. By default the classifier only tests pending policies (policies that have not yet been applied). Use the **applied** keyword to test only those policies that have been applied.
- Use the **qos apply** command to activate saved policies.

Examples

```
-> show policy classify l2 destination port 2/1
```

See the output example given on page 38-195 for more information about the potential screen display.

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
show policy classify	Describes the base command.

MIB Objects

```
alaQoSClassifyTable
   alaQoSClassifyDestinationSlot
   alaQoSClassifyDestinationPort
```

show policy classify source mac

Specifies a source MAC address for a hypothetical packet to show how the QoS software in the switch will handle the packet.

show policy classify {l2 | l3 | multicast} [applied] source mac *mac_address*

Syntax Definitions

l2	Uses the Layer 2 classifier for the hypothetical packet.
l3	Uses the Layer 3 classifier for the hypothetical packet.
multicast	Uses the multicast IGMP classifier for the hypothetical packet.
applied	Indicates that only applied policies should be examined.
mac_address	The source MAC address of the Layer 2 flow (for example, 00:20:da:05:f6:23) .

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use this command to determine if the switch will classify the traffic condition specified and match it to a policy. By default the classifier only tests pending policies (policies that have not yet been applied). Use the **applied** keyword to test only those policies that have been applied.
- Use the **qos apply** command to activate saved policies.

Examples

```
-> show policy classify l2 source mac 00:20:da:05:f6:23
```

See the output example given on page 38-195 for more information about the potential screen display.

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
show policy classify	Describes the base command.

MIB Objects

```
alaQoSClassifyTable
   alaQoSClassifySourceMac
```

show policy classify destination mac

Specifies a destination MAC address for a hypothetical packet to show how the QoS software in the switch will handle the packet.

show policy classify {l2 | l3 multicast} [applied] destination mac *mac_address*

Syntax Definitions

l2	Uses the Layer 2 classifier for the hypothetical packet.
l3	Uses the Layer 3 classifier for the hypothetical packet.
multicast	Uses the multicast IGMP classifier for the hypothetical packet.
applied	Indicates that only applied policies should be examined.
mac_address	The destination MAC address of the Layer 2 flow (for example, 00:20:da:05:f6:23).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use this command to determine if the switch will classify the traffic condition specified and match it to a policy. By default the classifier only tests pending policies (policies that have not yet been applied). Use the **applied** keyword to test only those policies that have been applied.
- Use the **qos apply** command to activate saved policies.

Examples

```
-> show policy classify l2 destination mac 00:20:da:05:f6:23
```

See the output example given on page 38-195 for more information about the potential screen display.

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
show policy classify	Describes the base command.

MIB Objects

```
alaQoSClassifyTable
   alaQoSClassifyDestinationMac
```

show policy classify source vlan

Specifies a source VLAN for a hypothetical packet to show how the QoS software in the switch will handle the packet.

show policy classify {l2 | l3 | multicast} [applied] source vlan *vlan_id*

Syntax Definitions

l2	Uses the Layer 2 classifier for the hypothetical packet.
l3	Uses the Layer 3 classifier for the hypothetical packet.
multicast	Uses the multicast IGMP classifier for the hypothetical packet.
applied	Indicates that only applied policies should be examined.
vlan_id	The destination VLAN ID for the flow.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use this command to determine if the switch will classify the traffic condition specified and match it to a policy. By default the classifier only tests pending policies (policies that have not yet been applied). Use the **applied** keyword to test only those policies that have been applied.
- Use the **qos apply** command to activate saved policies.

Examples

```
-> show policy classify l2 source vlan 2
```

See the output example given on page 38-195 for more information about the potential screen display.

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
show policy classify	Describes the base command.

MIB Objects

```
alaQoSClassifyTable
   alaQoSClassifySourceVlan
```

show policy classify destination vlan

Specifies a destination VLAN for a hypothetical packet to show how the QoS software in the switch will handle the packet.

show policy classify {l2 | l3 | multicast} [applied] destination vlan *vlan_id*

Syntax Definitions

l2	Uses the Layer 2 classifier for the hypothetical packet.
l3	Uses the Layer 3 classifier for the hypothetical packet.
multicast	Uses the multicast IGMP classifier for the hypothetical packet.
applied	Indicates that only applied policies should be examined.
vlan_id	The destination VLAN ID for the flow.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use this command to determine if the switch will classify the traffic condition specified and match it to a policy. By default the classifier only tests pending policies (policies that have not yet been applied). Use the **applied** keyword to test only those policies that have been applied.
- Use the **qos apply** command to activate saved policies.

Examples

```
-> show policy classify l2 destination vlan 3
```

See the output example given on page 38-195 for more information about the potential screen display.

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
show policy classify	Describes the base command.

MIB Objects

```
alaQoSClassifyTable
   alaQoSClassifySourceVlan
```

show policy classify source interface type

Specifies a source interface type for a hypothetical packet to show how the QoS software in the switch will handle the packet.

show policy classify {l2 | l3 | multicast} [applied] source interface type {ethernet | wan | ethernet-10 | ethernet-100 | ethernet-1G | ethernet-10G}

Syntax Definitions

l2	Uses the Layer 2 classifier for the hypothetical packet.
l3	Uses the Layer 3 classifier for the hypothetical packet.
multicast	Uses the multicast IGMP classifier for the hypothetical packet.
applied	Indicates that only applied policies should be examined.
ethernet	Indicates that the flow's source port is an Ethernet interface.
wan	Indicates that the flow's source port is a WAN interface. *Not supported in the current release.*
ethernet-10	Indicates that the flow's source port is 10 Mb Ethernet.
ethernet-100	Indicates that the flow's source port is 100 Mb Ethernet.
ethernet-1G	Indicates that the flow's source port is 1 gigabit Ethernet.
ethernet-10G	Indicates that the flow's source port is 10 gigabit Ethernet.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use this command to determine if the switch will classify the traffic condition specified and match it to a policy. By default the classifier only tests pending policies (policies that have not yet been applied). Use the **applied** keyword to test only those policies that have been applied.
- Use the **qos apply** command to activate saved policies.

Examples

```
-> policy classify l2 source interface type ethernet
```

See the output example given on page 38-195 for more information about the potential screen display.

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
show policy classify	Describes the base command.

MIB Objects

```
alaQoSClassifyTable
   alaQoSClassifySourceInterfaceType
```

show policy classify destination interface type

Specifies a destination interface type for a hypothetical packet to show how the QoS software in the switch will handle the packet.

show policy classify {l2 | l3 | multicast} [applied] destination interface type {ethernet | wan | ethernet-10 | ethernet-100 | ethernet-1G | ethernet-10G}

Syntax Definitions

l2	Uses the Layer 2 classifier for the hypothetical packet.
l3	Uses the Layer 3 classifier for the hypothetical packet.
multicast	Uses the multicast IGMP classifier for the hypothetical packet.
applied	Indicates that only applied policies should be examined.
ethernet	Indicates that the flow's destination port is an Ethernet interface.
wan	Indicates that the flow's destination port is a WAN interface. *Not supported in the current release.*
ethernet-10	Indicates that the flow's destination port is 10 Mb Ethernet.
ethernet-100	Indicates that the flow's destination port is 100 Mb Ethernet.
ethernet-1G	Indicates that the flow's destination port is 1 gigabit Ethernet.
ethernet-10G	Indicates that the flow's destination port is 10 gigabit Ethernet.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use this command to determine if the switch will classify the traffic condition specified and match it to a policy. By default the classifier only tests pending policies (policies that have not yet been applied). Use the **applied** keyword to test only those policies that have been applied.
- Use the **qos apply** command to activate saved policies.

Examples

```
-> show policy classify l2 destination interface type ethernet-10
```

See the output example given on page 38-195 for more information about the potential screen display.

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
show policy classify	Describes the base command.

MIB Objects

```
alaQoSClassifyTable
   alaQoSClassifyDestinationInterfaceType
```

show policy classify 802.1p

Specifies a destination interface type for a hypothetical packet to show how the QoS software in the switch will handle the packet.

show policy classify {l2 | l3 | multicast} [applied] 802.1p *value*

Syntax Definitions

l2	Uses the Layer 2 classifier for the hypothetical packet.
l3	Uses the Layer 3 classifier for the hypothetical packet.
multicast	Uses the multicast IGMP classifier for the hypothetical packet.
applied	Indicates that only applied policies should be examined.
value	The 802.1p value for the flow.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use this command to determine if the switch will classify the traffic condition specified and match it to a policy. By default the classifier only tests pending policies (policies that have not yet been applied). Use the **applied** keyword to test only those policies that have been applied.
- Use the **qos apply** command to activate saved policies.

Examples

```
-> show policy classify l2 802.1p 4
```

See the output example given on page 38-195 for more information about the potential screen display.

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
show policy classify	Describes the base command.

MIB Objects

```
alaQoSClassifyTable
   alaQoSClassify8021p
```

show policy classify source ip

Specifies a source IP address for a hypothetical packet to show how the QoS software in the switch will handle the packet.

show policy classify {l2 | l3 | multicast} [applied] source ip *ip_address*

Syntax Definitions

l2	Uses the Layer 2 classifier for the hypothetical packet.
l3	Uses the Layer 3 classifier for the hypothetical packet.
multicast	Uses the multicast IGMP classifier for the hypothetical packet.
applied	Indicates that only applied policies should be examined.
ip_address	The source IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use this command to determine if the switch will classify the traffic condition specified and match it to a policy. By default the classifier only tests pending policies (policies that have not yet been applied). Use the **applied** keyword to test only those policies that have been applied.
- Use the **qos apply** command to activate policies.

Examples

```
-> show policy classify l3 source ip 1.2.3.4
```

See the output example given on page 38-195 for more information about the potential screen display.

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
show policy classify	Describes the base command.

MIB Objects

```
alaQoSClassifyTable
   alaQoSClassifySourceIp
```

show policy classify destination ip

Specifies a destination IP address for a hypothetical packet to show how the QoS software in the switch will handle the packet.

show policy classify {l2 | l3 | multicast} [applied] destination ip *ip_address*

Syntax Definitions

l2	Uses the Layer 2 classifier for the hypothetical packet.
l3	Uses the Layer 3 classifier for the hypothetical packet.
multicast	Uses the multicast IGMP classifier for the hypothetical packet.
applied	Indicates that only applied policies should be examined.
ip_address	The destination IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use this command to determine if the switch will classify the traffic condition specified and match it to a policy. By default the classifier only tests pending policies (policies that have not yet been applied). Use the **applied** keyword to test only those policies that have been applied.
- Use the **qos apply** command to activate policies.

Examples

```
-> show policy classify l3 destination ip 198.60.22.2
```

See the output example given on page 38-195 for more information about the potential screen display.

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
show policy classify	Describes the base command.

MIB Objects

```
alaQoSClassifyTable
   alaQoSClassifyDestinationIpPort
```

show policy classify multicast ip

Specifies a multicast address for a hypothetical packet to show how the QoS software in the switch will handle the packet.

show policy classify {l2 | l3 | multicast} [applied] multicast ip *ip_address*

Syntax Definitions

l2	Uses the Layer 2 classifier for the hypothetical packet.
l3	Uses the Layer 3 classifier for the hypothetical packet.
multicast	Uses the multicast IGMP classifier for the hypothetical packet.
applied	Indicates that only applied policies should be examined.
ip_address	The multicast IP address (the address of the multicast stream).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use this command to determine if the switch will classify the traffic condition specified and match it to a policy. By default the classifier only tests pending policies (policies that have not yet been applied). Use the **applied** keyword to test only those policies that have been applied.
- Use the **qos apply** command to activate policies.

Examples

```
-> show policy classify multicast multicast ip 224.22.22.1
Packet headers:
L2:
 *Port         :                        0/0 (any)  -> 0/0 (any)
 *MAC          :                   000000:000000  -> 080020:D1E51
 *VLAN         :                               0  -> 0
 *802.1p       : 0
L3/L4:
 *Mcast        :                     224.22.22.1
 *IP           :                         0.0.0.0  -> 0.0.0.0
 *TOS/DSCP     : 0/0
Using pending multicast policies
Classify Multicast:
 *No rule matched: (accept)
```

See the output example given on page 38-195 for information about the displayed fields.

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
show policy classify	Describes the base command.

MIB Objects

```
alaQoSClassifyTable
   alaQoSClassifyMulticastIp
```

show policy classify tos

Specifies a ToS value for a hypothetical packet to show how the QoS software in the switch will handle the packet.

show policy classify {l2 | l3 | multicast} [applied] tos *tos_value*

Syntax Definitions

l2	Uses the Layer 2 classifier for the hypothetical packet.
l3	Uses the Layer 3 classifier for the hypothetical packet.
multicast	Uses the multicast IGMP classifier for the hypothetical packet.
applied	Indicates that only applied policies should be examined.
tos_value	The Type of Service bits value included in the IP header. The three most significant bits of the byte determine the precedence (i.e, priority) of the frame (0 is the lowest, 7 is the highest).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use this command to determine if the switch will classify the traffic condition specified and match it to a policy. By default the classifier only tests pending policies (policies that have not yet been applied). Use the **applied** keyword to test only those policies that have been applied.
- Use the **qos apply** command to activate policies.
- If a ToS value is specified, a DSCP value may not be specified.

Examples

```
-> show policy classify l3 tos 7
```

See the output example given on page 38-195 for more information about the potential screen display.

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
show policy classify	Describes the base command.

MIB Objects

```
alaQoSClassifyTable
   alaQoSClassifyTos
```

show policy classify dscp

Specifies a DiffServ Code Point (DSCP) value for a hypothetical packet to show how the QoS software in the switch will handle the packet.

show policy classify {l2 | l3 | multicast} [applied] dscp *dscp_value*

Syntax Definitions

l2	Uses the Layer 2 classifier for the hypothetical packet.
l3	Uses the Layer 3 classifier for the hypothetical packet.
multicast	Uses the multicast IGMP classifier for the hypothetical packet.
applied	Indicates that only applied policies should be examined.
dscp_value	The DiffServ Code Point value, in the range 0–63.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use this command to determine if the switch will classify the traffic condition specified and match it to a policy. By default the classifier only tests pending policies (policies that have not yet been applied). Use the **applied** keyword to test only those policies that have been applied.
- Use the **qos apply** command to activate policies.
- If a DSCP value is specified, a ToS value may not be specified.

Examples

```
-> show policy classify l3 dscp 63
```

See the output example given on page 38-195 for more information about the potential screen display.

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
show policy classify	Describes the base command.

MIB Objects

```
alaQoSClassifyTable
   alaQoSClassifyDscp
```

show policy classify ip protocol

Specifies an IP protocol for a hypothetical packet to show how the QoS software in the switch will handle the packet.

show policy classify {l2 | l3 | multicast} [applied] ip protocol *protocol*

Syntax Definitions

l2	Uses the Layer 2 classifier for the hypothetical packet.
l3	Uses the Layer 3 classifier for the hypothetical packet.
multicast	Uses the multicast IGMP classifier for the hypothetical packet.
applied	Indicates that only applied policies should be examined.
protocol	The IP protocol number, for example, 6.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use this command to determine if the switch will classify the traffic condition specified and match it to a policy. By default the classifier only tests pending policies (policies that have not yet been applied). Use the **applied** keyword to test only those policies that have been applied.
- Use the **qos apply** command to activate policies.

Examples

```
-> show policy classify l3 ip protocol 6
```

See the output example given on page 38-195 for more information about the potential screen display.

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
show policy classify	Describes the base command.

MIB Objects

```
alaQoSClassifyTable
   alaQoSClassifyIpProtocol
```

show policy classify source ip port

Specifies a source IP port for a hypothetical packet to show how the QoS software in the switch will handle the packet.

show policy classify {l2 | l3 | multicast} [applied] source ip port *port*

Syntax Definitions

l2	Uses the Layer 2 classifier for the hypothetical packet.
l3	Uses the Layer 3 classifier for the hypothetical packet.
multicast	Uses the multicast IGMP classifier for the hypothetical packet.
applied	Indicates that only applied policies should be examined.
port	The well-known port number for the desired service. For example, the port number for Telnet is 23.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use this command to determine if the switch will classify the traffic condition specified and match it to a policy. By default the classifier only tests pending policies (policies that have not yet been applied). Use the **applied** keyword to test only those policies that have been applied.
- Use the **qos apply** command to activate policies.

Examples

```
-> show policy classify l3 source ip port 80
```

See the output example given on page 38-195 for more information about the potential screen display.

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
show policy classify	Describes the base command.

MIB Objects

```
alaQoSClassifyTable
   alaQoSClassifySourceIpPort
```

show policy classify destination ip port

Specifies a destination IP port for a hypothetical packet to show how the QoS software in the switch will handle the packet.

show policy classify {l2 | l3 | multicast} [applied] destination ip port *port*

Syntax Definitions

l2	Uses the Layer 2 classifier for the hypothetical packet.
l3	Uses the Layer 3 classifier for the hypothetical packet.
multicast	Uses the multicast IGMP classifier for the hypothetical packet.
applied	Indicates that only applied policies should be examined.
port	The well-known port number for the desired service. For example, the port number for Telnet is 23.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use this command to determine if the switch will classify the traffic condition specified and match it to a policy. By default the classifier only tests pending policies (policies that have not yet been applied). Use the **applied** keyword to test only those policies that have been applied.
- Use the **qos apply** command to activate policies.

Examples

```
-> show policy classify l3 destination ip port 80
```

See the output example given on page 38-195 for more information about the potential screen display.

Release History

Release 5.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
show policy classify	Describes the base command.

MIB Objects

```
alaQoSClassifyTable
   alaQoSClassifyDestinationIpPort
```

show policy network group

Displays information about pending and applied policy network groups.

show [applied] policy network group [*network_group***]**

Syntax Definitions

applied	Indicates that only network groups that have been applied should be displayed.
network_group	The name of the policy network group for which you want to display information; or a wildcard sequence of characters for displaying information about network groups with similar names. Use an asterisk (*) to indicate a wildcard character.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Information for all policy network groups displays unless *network_group* is specified.
- The display may include any of the following characters:

character	definition
+	Indicates a new policy network group.
-	Indicates the policy network group is pending deletion.
#	Indicates that the policy network group differs between the pending/applied network groups.

Examples

```
-> show policy network group
Group Name:                    From   Entries
Switch                          blt   4.0.1.166
                                      10.0.1.166
                                      143.209.92.166
                                      192.85.3.1

+netgroup1                      cli   143.209.92.0/255.255.255.0
                                      172.28.5.0/255/255/255.0
```

output definitions

Group Name	The name of the port group, configured through the **policy network group** command.
From	The way the group was configured: **blt** indicates a built-in entry; **cli** indicates that the entry was configured on the switch; **ldap** indicates the entry was configured through PolicyView
Entries	The IP addresses associated with the network group.

Release History

Release 5.1; command was introduced.

Related Commands

policy network group	Configures policy network groups.

MIB Objects

```
alaQoSNetworkGroupsTable
   alaNetworkGroupsName
   alaNetworkGroupsSource
alaNetworkGroupTable
   alaNetworkGroupIpAddr
   alaQoSNetworkGroupIpMask
```

show policy service

Displays information about pending and applied policy services.

show [applied] policy service [*service_name***]**

Syntax Definitions

applied	Indicates that only services that have been applied should be displayed.
service_name	The name of the service for which you want to display information; or a wildcard sequence of characters for displaying information about services with similar names. Use an asterisk (*) to indicate a wildcard character.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Information about all policy services is displayed unless *service_name* is specified.
- The display may include any of the following characters:

character	definition
+	Indicates a new policy service.
-	Indicates the policy service is pending deletion.
#	Indicates that the policy service differs between the pending/applied services.

Examples

```
-> show policy service
   Service Name                From          IPProto   ScrPort    DstPort
telnet_service                 cli           6 (TCP)                  23
+ftp_service                   cli           6 (TCP)                  21
test_service                   cli           6 (TCP)                  21

-> show policy service telnet_service
   Service Name                From          IPProto   ScrPort    DstPort
telnet_service                 cli           6 (TCP)                  23

-> show applied policy service
   Service Name                From          IPProto   ScrPort    DstPort
telnet_service                 cli           6 (TCP)                  23
test_service                   cli           6 (TCP)                  21
```

output definitions

Service Name	The name of the port group, configured through the **policy service** command.
From	The way the service was configured: **blt** indicates a built-in entry; **cli** indicates that the entry was configured on the switch; **ldap** indicates the entry was configured through PolicyView.
IPProto	The IP protocol associated with the service.
ScrPort	A source port associated with the service.
DstPort	A destination port associated with the service.

Release History

Release 5.1; command was introduced.

Related Commands

policy service	Configures a service that may be used as part of a policy service group.

MIB Objects

```
alaQoSServiceTable
   alaQoSServiceName
   alaQoSServiceSource
   alaQoSServiceIpProtocol
   alaQoSServiceSourceIpPort
   alaQoSServiceDestinationIpPort
alaQoSAppliedServiceTable
   alaQoSAppliedServiceName
   alaQoSAppliedServiceSource
   alaQoSAppliedServiceIpProtocol
   alaQoSAppliedSourceIpPort
   alaQoSAppliedServiceDestinationIpPort
```

show policy service group

Displays information about pending and applied policy service groups.

show [applied] policy service group [*service_group***]**

Syntax Definitions

applied	Indicates that only service groups that have been applied should be displayed.
service_group	The name of the service group for which you want to display information; or a wildcard sequence of characters for displaying information about service groups with similar names. Use an asterisk (*) to indicate a wildcard character.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Information for all policy service groups displays unless *service_group* is specified.
- The display may include any of the following characters:

character	definition
+	Indicates a new policy service group.
-	Indicates the policy service group is pending deletion.
#	Indicates that the policy service group differs between the pending/applied service groups.

Examples

```
-> show policy service group
Group Name:                   From   Entries
serv_group1                    cli   telnet
                                     ftp

serv_group2                    cli   telnet
```

output definitions

Group Name	The name of the port group, configured through the **policy service group** command.
From	The origin of the service group: **cli** indicates that the entry was configured on the switch; **ldap** indicates the entry was configured through PolicyView.
Entries	The services associated with the group. Services are configured through the **policy service** command.

Release History

Release 5.1; command was introduced.

Related Commands

policy service group	Configures a service group and its associated services. A service group may be attached to a policy condition.

MIB Objects

```
alaQoSServiceGroupsTable
   alaQoSServiceGroupsName
   alaQoSServiceGroupsSource
alaQoSAppliedServiceGroupsTable
   alaQoSAppliedServiceGroupsName
   alaQoSAppliedServiceGroupsSource
alaQoSServiceGroupTable
   alaQoSServiceGroupServiceName
alaQoSAppliedServiceGroupTable
   alaQoSAppliedServiceGroupServiceName
```

show policy mac group

Displays information about pending and applied MAC groups.

show [applied] policy mac group [*mac_group***]**

Syntax Definitions

applied	Indicates that only MAC groups that have been applied should be displayed.
mac_group	The name of the MAC group for which you want to display information; or a wildcard sequence of characters for displaying information about MAC groups with similar names. Use an asterisk (*) to indicate a wildcard character.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Information for all policy MAC groups displays unless *mac_group* is specified.
- The display may include any of the following characters:

character	definition
+	Indicates a new policy MAC group.
-	Indicates the policy MAC group is pending deletion.
#	Indicates that the policy MAC group differs between the pending/applied MAC groups.

Examples

```
-> show policy mac group
Group Name:                   From   Entries
pubs1                          cli   0020da:05f623
                                     0020da:05f624
                                     143.209.92.166
                                     192.85.3.1

+yuba                          cli   080020:D16E51
                                     172.28.5.0/255/255/255.0
```

output definitions

Group Name	The name of the port group, configured through the **policy mac group** command.
From	The origin of the MAC group: **cli** indicates that the entry was configured on the switch; **ldap** indicates the entry was configured through PolicyView.
Entries	The MAC addresses associated with the group.

Release History

Release 5.1; command was introduced.

Related Commands

policy mac group	Configures policy MAC groups.

MIB Objects

```
alaQoSMACGroupsTable
   alaQoSMACGroupsName
   alaQoSMACGroupsSource
alaQoSAppliedMACGroupsTable
   alaQoSAppliedMACGroupsName
   alaQoSAppliedMACGroupsSource
alaQoSMACGroupTable
   alaQoSMACGroupMacAddr
   alaQoSMACGroupMacMask
alaQoSAppliedMACGroupTable
   alaQoSAppliedMACGroupMacAddr
   alaQoSAppliedMACGroupMacMask
```

show policy port group

Displays information about pending and applied policy port groups.

show [applied] policy port group [*group_name***]**

Syntax Definitions

applied	Indicates that only policy port groups that have been applied should be displayed.
group_name	The name of the policy port group for which you want to display information; or a wildcard sequence of characters for displaying information about port groups with similar names. Use an asterisk (*) to indicate a wildcard character.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Information for all policy port groups displays unless *group_name* is specified.
- The display may include any of the following characters:

character	definition
+	Indicates a new policy port group.
-	Indicates the policy port group is pending deletion.
#	Indicates that the policy port group differs between the pending/applied port groups.

Examples

```
-> show policy port group
Group Name:                   From   Entries
Slot01                         blt

Slot02                         blt


Slot03                         blt

Slot04                         blt

Slot05                         blt

Slot06                         blt
```

```
Slot07                          blt

Slot08                          blt

pgroup1                         cli   2/1
                                      3/1
                                      3/2

pgroup2                         cli   2/2
                                      2/3
```

output definitions

Group Name	The name of the port group, configured through the **policy port group** command or built-in port groups automatically set up by the switch (**Slot01**, **Slot02**, **Slot03**, etc.).
From	The origin of the port group: **cli** indicates that the entry was configured on the switch; **ldap** indicates the entry was configured through Policy-View; **blt** indicates the entry was set up automatically by the switch based on the current hardware.
Entries	The slot/port combinations associated with the port group.

Release History

Release 5.1; command was introduced.

Related Commands

policy port group	Configures a port group and its associated slot and port numbers.

MIB Objects

```
alaQoSPortGroupsTable
   alaQoSPortGroupsName
   alaQoSPortGroupsSource
alaQoSAppliedPortGroupsTable
   alaQoSAppliedPortGroupsName
   alaQoSAppliedPortGroupsSource
alaPortGroupTable
   alaQoSPortGroupSlot
   alaQoSPortGroupPort
alaAppliedPortGroupTable
   alaQoSAppliedPortGroupSlot
   alaQoSAppliedPortGroupPort
```

show policy map group

Displays information about pending and applied policy map groups.

show [applied] policy map group [*group_name***]**

Syntax Definitions

applied	Indicates that only map groups that have been applied should be displayed.
group_name	The name of the policy map group for which you want to display information; or a wildcard sequence of characters for displaying information about map groups with similar names. Use an asterisk (*) to indicate a wildcard character.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Information for all policy map groups displays unless *group_name* is specified.
- The display may include any of the following characters:

character	definition
+	Indicates a new policy port group.
-	Indicates the policy port group is pending deletion.
#	Indicates that the policy port group differs between the pending/applied port groups.

Examples

```
-> show policy map group
Group Name                    From  Entries
+tosGroup                      cli  1-2:4
                                    4:5
```

output definitions

Group Name	The name of the map group, configured through the **policy map group** command.

output definitions

From	The origin of the port group: **cli** indicates that the entry was configured on the switch; **ldap** indicates the entry was configured through Policy-View.
Entries	The slot/port combinations associated with the port group.

Release History

Release 5.1; command was introduced.

Related Commands

policy map group	Configures a map group and its associated mappings for 802.1p, Type of Service (ToS), or Differentiated Services Code Point (DSCP) values.

MIB Objects

```
alaQoSMapGroupsTable
   alaQoSMapGroupsName
   alaQoSMapGroupsSource
alaQoSAppliedMapGroupsTable
   alaQoSAppliedMapGroupsName
   alaQoSAppliedMapGroupsSource
alaQoSMapGroupTable
   alaQoSMapGroupKey
   alaQoSMapGroupKeyEnd
   alaQoSMapGroupValue
alaQoSAppliedMapGroupTable
   alaQoSAppliedMapGroupKey
   alaQoSAppliedMapGroupKeyEnd
   alaQoSAppliedMapGroupValue
```

show policy action

Displays information about pending and applied policy actions configured on the switch.

show [applied] policy action [*action_name***]**

Syntax Definitions

applied	Indicates that only actions that have been applied should be displayed.
action_name	The name of the action for which you want to display information; or a wildcard sequence of characters for displaying information about actions with similar names. Use an asterisk (*) to indicate a wildcard character.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Information for all policy actions displays unless *action_name* is specified.
- The display may include any of the following characters:

character	definition
+	Indicates a new policy action.
-	Indicates the policy action is pending deletion.
#	Indicates that the policy action differs between the pending/applied actions.

Examples

```
-> show policy action
                                                  Bandwidth
       Action  Name     From   Disp   Pri  Share  Min  Max
action1                   cli  accept       No
+action2                  cli  accept       No
test_action               cli  accept       Yes

-> show policy action action2
                                                  Bandwidth
       Action  Name     From   Disp   Pri  Share  Min  Max
action2                   cli  accept       No
```

```
-> show applied policy action
                                                    Bandwidth
       Action  Name     From   Disp   Pri   Share  Min  Max
action1                   cli  accept       No
action2                   cli  accept       No

-> show policy action action*
                                                    Bandwidth
       Action  Name     From   Disp   Pri   Share  Min  Max
action1                   cli  accept       No
action2                   cli  accept       No
```

output definitions

Action Name	The name of the action , configured through the **policy action** command.
From	Where the policy rule originated: **cli** indicates that the entry was configured on the switch; **ldap** indicates the entry was configured through PolicyView.
Disp	The disposition of the rule, either **accept** or **deny**.
Pri	The priority configured for the rule.
Share	Whether or not the rule specifies that the queue should be shared.
Min Bandwidth	The minimum bandwidth required by the rule.
Max Bandwidth	The maximum bandwidth required by the rule.

Release History

Release 5.1; command was introduced.

Related Commands

policy action	Creates a policy action. A QoS action is a particular set of bandwidth and queue parameters that may be applied to a flow matching particular QoS conditions.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionSource
   alaQoSActionDisposition
   alaQoSActionShared
   alaQoSActionMinimumBandwidth
   alaQoSActionMaximumBandwidth
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionSource
   alaQoSAppliedActionDisposition
   alaQoSAppliedActionShared
   alaQoSAppliedActionMinimumBandwidth
   alaQoSAppliedActionMaximumBandwidth
```

show policy condition

Displays information about pending and applied policy conditions.

show [applied] policy condition [*condition_name***]**

Syntax Definitions

applied	Indicates that only conditions that have been applied should be displayed.
condition_name	The name of the condition for which you want to display information; or a wildcard sequence of characters for displaying information about conditions with similar names. Use an asterisk (*) to indicate a wildcard character.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Information for all policy conditions displays unless *condition_name* is specified.
- The display may include any of the following characters:

character	definition
+	Indicates a new policy condition.
-	Indicates the policy condition is pending deletion.
#	Indicates that the policy condition differs between the pending/applied conditions.

Examples

```
-> show policy condition
Condition Name:               From   Src    ->    Dest
pcond1                         cli
*IP      :                           Any    ->    198.60.82.0/255.255.255.0

+c4                            cli
*IP      : 10.11.2.0/255/255/255.0         ->    Any
*TCP     :                           Any    ->    600


-> show policy condition c*
Condition Name:               From   Src    ->    Dest
+c4                            cli
*IP      : 10.11.2.0/255/255/255.0         ->    Any
*TCP     :                           Any    ->    600
```

output definitions

Condition Name	The name of the condition, configured through the **policy condition** command.
From	The origin of the condition: **cli** indicates that the entry was configured on the switch; **ldap** indicates the entry was configured through Policy-View.
Scr	The source address associated with the condition.
Dest	The destination address associated with the condition.

Release History

Release 5.1; command was introduced.

Related Commands

policy condition	Creates a policy condition. The condition determines what parameters the switch uses to classify incoming flows.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionSource
   alaQoSConditionSourceSlot
   alaQoSConditionSourcePort
   alaQoSConditionSourcePortGroup
   alaQoSConditionDestinationSlot
   alaQoSConditionDestinationPort
   alaQoSConditionDestinationPortGroup
   alaQoSConditionSourceInterfaceType
   alaQoSConditionDestinationInterfaceType
   alaQoSConditionSourceMacAddr
   alaQoSConditionSourceMacMask
   alaQoSConditionSourceMacGroup
   alaQoSConditionDestinationMacAddr
   alaQoSConditionDestinationMacMask
   alaQoSConditionDestinationMacGroup
   alaQoSConditionSourceVlan
   alaQoSConditionDestinationVlan
   alaQoSCondition8021p
   alaQoSConditionSourceIpAddr
   alaQoSConditionSourceIpMask
   alaQoSConditionSourceNetworkGroup
   alaQoSConditionDestinationIpAddr
   alaQoSConditionDestinationIpMask
   alaQoSConditionDestinationNetworkGroup
   alaQoSConditionMulticastIpAddr
   alaQoSConditionMulticastIpMask
   alaQoSConditionMulticastNetworkGroup
   alaQoSConditionTos
   alaQoSConditionDscp
   alaQoSConditionTcpFlags
```

```
alaQoSConditionIpProtocol
alaQoSConditionSourceIpPort
alaQoSConditionDestinationIpPort
alaQoSConditionService
alaQoSConditionServiceGroup
```

show active policy rule

Displays information about pending and applied policy rules that are active (enabled) on the switch.

show active [bridged | routed | multicast] policy rule [*rule_name***]**

Syntax Definitions

bridged	Displays active rules that apply to bridged traffic.
routed	Displays active rules that apply to routed traffic.
multicast	Displays active rules that apply to multicast traffic.
rule_name	The name of the rule for which you want to display information; or a wildcard sequence of characters for displaying information about rules with similar names. Use an asterisk (*) to indicate a wildcard character.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **show policy rule** command to display inactive as well as active policy rules.
- Information for all rules is displayed unless *rule_name* is specified.
- Information for all rule types is displayed unless a keyword (**bridged**, **routed**, **multicast**) is specified.
- Applied rules may or may not be active on the switch. Applied rules are inactive if they have been administratively disabled with the **disable** option in the **policy rule** command.
- The display may include any of the following characters:

character	definition
+	Indicates that the policy rule has been modified or has been created since the last **qos apply**.
-	Indicates the policy object is pending deletion.
#	Indicates that the policy object differs between the pending/applied objects.

Examples

```
-> show active policy rule
                  Policy          From  Prec  Enab Inact  Refl  Log  Save  Matches
mac1                              cli    0   Yes  No     No    No   Yes        0
Cnd/Act:                       dmac1 -> pri2
```

output definitions

Policy	The name of the policy rule, configured through the **policy rule** command. A plus sign (+) preceding a policy rule name indicates that the policy rule has been modified or has been created since the last **qos apply**.
From	Where the rule originated.
Prec	The precedence of the rule. Precedence determines the order in which the switch will apply rules.
Enab	Whether or not the rule is administratively enabled. (By default, rules are enabled.)
Inact	Whether or not the rule is currently being enforced on the switch. A rule might be inactive if it includes condition or condition/action combinations that cannot be enforced.
Refl	Whether the rule is reflexive or not.
Log	Whether or not information about the rule will be logged.
Save	Whether the rule will be captured in an ASCII text file (using the **configuration snapshot** command), saved to the working directory after the **write memory** command or **copy running-config working** command is entered, or saved after a reboot.
Matches	The number of flows matching this rule.
Cnd/Act	The condition and the action associated with the rule; configured through the **policy condition** and **policy action** commands respectively.

Release History

Release 5.1; command was introduced.

Related Commands

policy rule	Configures a policy rule on the switch. A rule is made up of a condition (for classifying incoming traffic) and an action (to be applied to outgoing traffic).

MIB Objects

```
alaQoSRuleTable
   alaQoSRuleName
   alaQoSRuleEnabled
   alaQoSRuleSource
   alaQoSRulePrecedence
   alaQoSRuleCondition
   alaQoSRuleAction
   alaQoSRuleReflexive
   alaQoSRuleActive
```

show policy rule

Displays information about pending and applied policy rules.

show [applied] [bridged | routed | multicast] policy rule [*rule_name***]**

Syntax Definitions

applied	Indicates that only policy rules that have been applied should be displayed.
bridged	Displays rules that apply to bridged traffic.
routed	Displays rules that apply to routed traffic.
multicast	Displays rules that apply to multicast traffic.
rule_name	The name of the rule for which you want to display information; or a wildcard sequence of characters for displaying information about rules with similar names. Use an asterisk (*) to indicate a wildcard character.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Information for all rules is displayed unless *rule_name* is specified.
- Information for all rule types is displayed unless a keyword (**bridged**, **routed**, **multicast**) is specified.
- Use the **show active policy rule** command to display only active rules that are currently being enforced on the switch.
- The display may include any of the following characters:

character	definition
+	Indicates that the policy rule has been modified or has been created since the last **qos apply**.
-	Indicates the policy object is pending deletion.
#	Indicates that the policy object differs between the pending/applied objects.

Examples

```
-> show policy rule
                  Policy          From  Prec  Enab Inact  Refl  Log  Save
my_rule                           cli    0   Yes  Yes    No    No   Yes
  Cnd/Act:                        cond5 -> action2

+my_rule5                         cli    0   Yes  No     No    No   Yes
Cnd/Act:                          cond2 -> pri2

mac1                              cli    0   Yes  No     No    No   Yes
Cnd/Act:                          dmac1 -> pri2


-> show applied policy rule
                  Policy          From  Prec  Enab Inact  Refl  Log  Save
my_rule                           cli    0   Yes  Yes    No    No   Yes
  Cnd/Act:                        cond5 -> action2

mac1                              cli    0   Yes  No     No    No   Yes
Cnd/Act:                          dmac1 -> pri2
```

output definitions

Policy	The name of the policy rule, configured through the **policy rule** command. A plus sign (+) preceding a policy rule name indicates that the policy rule has been modified or has been created since the last **qos apply**.
From	Where the rule originated.
Prec	The precedence of the rule. Precedence determines the order in which the switch will apply rules.
Enable	Whether or not the rule is enabled.
Inactive	Whether or not the rule is currently being enforced on the switch.
Reflexive	Whether the rule is reflexive or not.
Cnd/Act	The condition and the action associated with the rule; configured through the **policy condition** and **policy action** commands respectively.

Release History

Release 5.1; command was introduced.

Related Commands

policy rule	Configures a policy rule on the switch. A rule is made up of a condition (for classifying incoming traffic) and an action (to be applied to outgoing traffic).

MIB Objects

```
alaQoSRuleTable
   alaQoSRuleName
   alaQoSRuleEnabled
   alaQoSRuleSource
   alaQoSRulePrecedence
   alaQoSRuleCondition
   alaQoSRuleAction
   alaQoSRuleReflexive
```

show qos port

Displays information about all QoS ports or a particular port.

show qos port [*slot/port***] [statistics]**

Syntax Definitions

slot/port	The physical slot and port number. For example: 3/1.
statistics	Displays statistics for high-density gigabit modules.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Information for all ports is displayed unless a particular port is specified.
- Use the **qos port** command to configure port parameters.
- For ports that are trusted (**Yes** displays in the Trust field), the Trust field includes one of the following characters:

character	definition
+	Indicates that the port is manually configured as trusted through the **qos port trusted** command; the port setting takes precedence over the global trust setting configured through the **qos trust ports** command.
*	Indicates that the port is automatically trusted regardless of the global setting set through the **qos trust ports** command. (Applies to mobile ports and ports configured for 802.1Q.)

Examples

The following are examples of the **show qos port** output display on an OmniSwitch 6600, 7700/7800, and 8800:

```
-> show qos port
Slot/  QoS             Deflt       Queues     Bandwidth
Port  Act Enabled  Trust P/DSCP Deflt Tot  Physical Reserved   Clsfy  Type
 1/1  No  Yes        No 0/ 0     4       0     0K    0K/<phy>    t   ethernet
 1/2  Yes Yes        No 0/ 0     4       0 1.00M    0K/<phy>    t   ethernet-1G
 3/1  Yes Yes        No 0/       4       0  100K    0K/<phy>    t   ethernet-100
 3/2  Yes Yes      +Yes 0/       4       0  100K    0K/<phy>    t   ethernet-100
 3/3  No  Yes        No 0/       4       0     0K    0K/<phy>    t   ethernet
 3/4  No  Yes        No 0/       4       0     0K    0K/<phy>    t   ethernet
 3/5  No  Yes        No 0/       4       0     0K    0K/<phy>    t   ethernet
-> show qos port 3/2
```

```
Slot/  QoS             Deflt       Queues     Bandwidth
Port  Act Enabled  Trust P/DSCP  Deflt ToS  Physical Reserved   Clsfy  Type
 3/2  Yes Yes        No 0/       4       0  100K    0K/<phy>    t   ethernet-100
```

The following are examples of the **show qos port statistics** output display on an OmniSwitch 6600, 7700/7800, and 8800:

```
->show qos port statistics
Slot/  QoS             Deflt       Queues     Bandwidth
Port  Act Enabled  Trust P/DSCP  Deflt Tot  Physical Reserved   Clsfy  Type
 1/1  No  Yes        No 0/ 0     4       0    0K    0K/<phy>    t   - ethernet
 1/2  Yes Yes        No 0/ 0     4       0 1.00M    0K/<phy>    t   - ethernet-1G
 3/1  Yes Yes        No 0/       4       0  100K    0K/<phy>    t   - ethernet-100
 3/2  Yes Yes        No 0/       4       0  100K    0K/<phy>    t   - ethernet-100
 3/3  No  Yes        No 0/       4       0    0K    0K/<phy>    t   - ethernet
 3/4  No  Yes        No 0/       4       0    0K    0K/<phy>    t   - ethernet
 3/5  No  Yes        No 0/       4       0    0K    0K/<phy>    t   - ethernet
Prio Enq-Bytes Deq-Bytes  Enq-Pkts  Deq-Pkts Qid-Disc Wred-Disc   Overf-Disc
 0   7.66e+07  7.66e+07   7.24e+05 7.24e+05       0         0         0
 1      0         0          0         0          0         0         0
 2      0         0          0         0          0         0         0
 3      0         0          0         0          0         0         0

-> show qos port 5/1 statistics
Slot/    QoS             Deflt    Queues      Bandwidth
Port  Act Enabled  Trust P/DSCP Deflt  Tot Physical Reserved    Clsfy Type
 5/1   No  Yes        No 0/  0    4      0    0K    0K/<phy>      t ethernet
 Prio Enq-Bytes Deq-Bytes  Enq-Pkts  Deq-Pkts  Qid-Disc Wred-Disc Overf-Disc
   0          0         0         0         0         0         0         0
   1          0         0         0         0         0         0         0
   2          0         0         0         0         0         0         0
   3          0         0         0         0         0         0         0
```

output definitions

Slot/Port	The slot and physical port number.
QoS	Whether or not the interface supports QoS.
Act	Whether or not the port is sending/receiving QoS traffic.
Enabled	Whether or not the port is enabled for QoS.
Trust	Whether the port is trusted or not trusted.
Default P	The default 802.1p setting for the port.
Default DSCP	The default ToS/DSCP setting for the port.
Default Queues	The number of default queues.
Tot Queues	The total number of queues.
Physical Bandwidth	The amount of physical bandwidth available on the port.
Reserved Bandwidth	Displays the amount of bandwidth reserved and whether it is physical (<**phy**>) or maximum virtual port bandwidth (<**max**>).
Clsfy	The default classification setting on a high-density gigabit port (**p** for 802.1p; **t** for ToS; **d** for DSCP). The field displays a hyphen (-) if the port is not located on a high-density gigabit interface.
Type	The interface type, **ethernet** or **wan**.

output definitions (continued)

Prio	Displays for high-density gigabit ports only. The priority queues associated with the port (0 through 3, lowest to highest).
Enq-Bytes	Displays for high-density gigabit ports only. The number of bytes enqueued on each priority queue for the port.
Deq-Bytes	Displays for high-density gigabit ports only. The number of bytes dequeued on each priority queue for the port.
Enq-Pkts	Displays for high-density gigabit ports only. The number of packets enqueued on each priority queue for the port.
Deq-Pkts	Displays for high-density gigabit ports only. The number of packets dequeued on each priority queue for the port.
Qid-Disc	Displays for high-density gigabit ports only. The number of packets discarded from the queue because the queue was full.
Wred-Disc	Displays for high-density gigabit ports only. The number of packets discarded from the queue based on the Weighted Random Early Detection (WRED) algorithm.
Overf-Disc	Displays for high-density gigabit ports only. The number of packets discarded from the queue because the queue buffer was full.

Release History

Release 5.1; command was introduced.

Related Commands

qos port	Configures a physical port for QoS.

MIB Objects

```
alaQoSPortTable
   alaQoSPortSlot
   alaQoSPortPort
   alaQoSPortEnabled
   alaQoSPortDefault8021p
   alaQoSPortDefaultDSCP
   alaQoSPortDefaultQueues
   alaQoSPortMaximumReservedBandwidth
   alaQoSPortMaximumDefaultBandwidth
   alaQoSPortDefaultClassification
   alaQoSPortFirPrio0EnqBytes
   alaQoSPortFirPrio0DeqBytes
   alaQoSPortFirPrio0EnqPkts
   alaQoSPortFirPrio0DeqPkts
   alaQoSPortFirPrio0QidDiscardPkts
   alaQoSPortFirPrio0WredDiscardPkts
   alaQoSPortFirPrio0OverflowDiscardPkts
   alaQoSPortFirPrio1EnqBytes
   alaQoSPortFirPrio1DeqBytes
   alaQoSPortFirPrio1EnqPkts
   alaQoSPortFirPrio1DeqPkts
   alaQoSPortFirPrio1QidDiscardPkts
   alaQoSPortFirPrio1WredDiscardPkts
```

```
alaQoSPortFirPrio1OverflowDiscardPkts
alaQoSPortFirPrio2EnqBytes
alaQoSPortFirPrio2DeqBytes
alaQoSPortFirPrio2EnqPkts
alaQoSPortFirPrio2DeqPkts
alaQoSPortFirPrio2QidDiscardPkts
alaQoSPortFirPrio2WredDiscardPkts
alaQoSPortFirPrio2OverflowDiscardPkts
alaQoSPortFirPrio3EnqBytes
alaQoSPortFirPrio3DeqBytes
alaQoSPortFirPrio3EnqPkts
alaQoSPortFirPrio3DeqPkts
alaQoSPortFirPrio3QidDiscardPkts
alaQoSPortFirPrio3WredDiscardPkts
alaQoSPortFirPrio3OverflowDiscardPkts
alaQosPortFreeFFPRules
alaQosPortUsedFFPRules
alaQosPortFreeFFPMasks
alaQosPortUsedFFPMasks
```

show qos port statistics

Displays information about all QoS ports or a particular port.

show qos port [*slot/port***] [statistics]**

Syntax Definitions

slot/port	The physical slot and port number. For example: 3/1.
statistics	Displays statistics for high-density gigabit modules.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Information for all ports is displayed unless a particular port is specified.
- Use the **qos port** command to configure port parameters.
- For ports that are trusted (**Yes** displays in the Trust field), the Trust field includes one of the following characters:

character	definition
+	Indicates that the port is manually configured as trusted through the **qos port trusted** command; the port setting takes precedence over the global trust setting configured through the **qos trust ports** command.
*	Indicates that the port is automatically trusted regardless of the global setting set through the **qos trust ports** command. (Applies to mobile ports and ports configured for 802.1Q.)

Examples

```
-> show qos port
Slot/  QoS             Deflt       Queues     Bandwidth
Port  Act Enabled  Trust P/DSCP  Deflt  Tot  Physical Reserved   Clsfy  Type
 1/1  No  Yes        No 0/ 0     4       0     0K    0K/<phy>    t   ethernet
 1/2  Yes Yes        No 0/ 0     4       0  1.00M    0K/<phy>    t   ethernet-1G
 3/1  Yes Yes        No 0/       4       0   100K    0K/<phy>    t   ethernet-100
 3/2  Yes Yes      +Yes 0/       4       0   100K    0K/<phy>    t   ethernet-100
 3/3  No  Yes        No 0/       4       0     0K    0K/<phy>    t   ethernet
 3/4  No  Yes        No 0/       4       0     0K    0K/<phy>    t   ethernet
 3/5  No  Yes        No 0/       4       0     0K    0K/<phy>    t   ethernet
 7/1  No  Yes        No 0/       4       0     0K    0K/<phy>    t   p-ethernet
```

```
-> show qos port 3/2
Slot/  QoS            Deflt       Queues    Bandwidth
Port  Act Enabled  Trust P/DSCP  Deflt ToS  Physical Reserved   Clsfy  Type
 3/2  Yes Yes        No 0/       4       0  100K    0K/<phy>    t   ethernet-100

->show qos port statistics
Slot/  QoS            Deflt       Queues    Bandwidth
Port  Act Enabled  Trust P/DSCP  Deflt Tot  Physical Reserved   Clsfy  Type
 1/1  No  Yes        No 0/ 0     4       0    0K    0K/<phy>    t   - ethernet
 1/2  Yes Yes        No 0/ 0     4       0 1.00M    0K/<phy>    t   - ethernet-1G
 3/1  Yes Yes        No 0/       4       0  100K    0K/<phy>    t   - ethernet-100
 3/2  Yes Yes        No 0/       4       0  100K    0K/<phy>    t   - ethernet-100
 3/3  No  Yes        No 0/       4       0    0K    0K/<phy>    t   - ethernet
 3/4  No  Yes        No 0/       4       0    0K    0K/<phy>    t   - ethernet
 3/5  No  Yes        No 0/       4       0    0K    0K/<phy>    t   - ethernet
 7/1  No  Yes        No 0/       4       0    0K    0K/<phy>    t   - ethernet
Prio Enq-Bytes Deq-Bytes  Enq-Pkts  Deq-Pkts Qid-Disc Wred-Disc   Overf-Disc
 0   7.66e+07  7.66e+07   7.24e+05 7.24e+05      0         0          0
 1      0         0          0        0          0         0          0
 2      0         0          0        0          0         0          0
 3      0         0          0        0          0         0          0
```

output definitions

Slot/Port	The slot and physical port number.
QoS	Whether or not the interface supports QoS.
Act	Whether or not the port is sending/receiving QoS traffic.
Enabled	Whether or not the port is enabled for QoS.
Trust	Whether the port is trusted or not trusted.
Default P	The default 802.1p setting for the port.
Default DSCP	The default ToS/DSCP setting for the port.
Default Queues	The number of default queues.
Tot Queues	The total number of queues.
Physical Bandwidth	The amount of physical bandwidth available on the port.
Reserved Bandwidth	Displays the amount of bandwidth reserved and whether it is physical (<**phy**>) or maximum virtual port bandwidth (<**max**>).
Clsfy	The default classification setting on a high-density gigabit port (**p** for 802.1p; **t** for ToS; **d** for DSCP). The field displays a hyphen (-) if the port is not located on a high-density gigabit interface.
Type	The interface type, **ethernet** or **wan**.
Prio	Displays for high-density gigabit ports only. The priority queues associated with the port (0 through 3, lowest to highest).
Enq-Bytes	Displays for high-density gigabit ports only. The number of bytes enqueued on each priority queue for the port.
Deq-Bytes	Displays for high-density gigabit ports only. The number of bytes dequeued on each priority queue for the port.
Enq-Pkts	Displays for high-density gigabit ports only. The number of packets enqueued on each priority queue for the port.

output definitions (continued)

Deq-Pkts	Displays for high-density gigabit ports only. The number of packets dequeued on each priority queue for the port.
Qid-Disc	Displays for high-density gigabit ports only. The number of packets discarded from the queue because the queue was full.
Wred-Disc	Displays for high-density gigabit ports only. The number of packets discarded from the queue based on the Weighted Random Early Detection (WRED) algorithm.
Overf-Disc	Displays for high-density gigabit ports only. The number of packets discarded from the queue because the queue buffer was full.

Release History

Release 5.1; command was introduced.

Related Commands

qos port	Configures a physical port for QoS.

MIB Objects

```
alaQoSPortTable
   alaQoSPortSlot
   alaQoSPortPort
   alaQoSPortEnabled
   alaQoSPortDefault8021p
   alaQoSPortDefaultDSCP
   alaQoSPortDefaultQueues
   alaQoSPortMaximumReservedBandwidth
   alaQoSPortMaximumDefaultBandwidth
   alaQoSPortDefaultClassification
   alaQoSPortFirPrio0EnqBytes
   alaQoSPortFirPrio0DeqBytes
   alaQoSPortFirPrio0EnqPkts
   alaQoSPortFirPrio0DeqPkts
   alaQoSPortFirPrio0QidDiscardPkts
   alaQoSPortFirPrio0WredDiscardPkts
   alaQoSPortFirPrio0OverflowDiscardPkts
   alaQoSPortFirPrio1EnqBytes
   alaQoSPortFirPrio1DeqBytes
   alaQoSPortFirPrio1EnqPkts
   alaQoSPortFirPrio1DeqPkts
   alaQoSPortFirPrio1QidDiscardPkts
   alaQoSPortFirPrio1WredDiscardPkts
   alaQoSPortFirPrio1OverflowDiscardPkts
   alaQoSPortFirPrio2EnqBytes
   alaQoSPortFirPrio2DeqBytes
   alaQoSPortFirPrio2EnqPkts
   alaQoSPortFirPrio2DeqPkts
   alaQoSPortFirPrio2QidDiscardPkts
   alaQoSPortFirPrio2WredDiscardPkts
   alaQoSPortFirPrio2OverflowDiscardPkts
   alaQoSPortFirPrio3EnqBytes
   alaQoSPortFirPrio3DeqBytes
```

```
alaQoSPortFirPrio3EnqPkts
alaQoSPortFirPrio3DeqPkts
alaQoSPortFirPrio3QidDiscardPkts
alaQoSPortFirPrio3WredDiscardPkts
alaQoSPortFirPrio3OverflowDiscardPkts
```

show qos port high-density-module

Displays information about the enqueuing thresholds on high-density QoS ports.

show qos port [*slot/port***] [statistics] high-density-module**

Syntax Definitions

slot/port	The physical slot and port number. For example: 3/1.
statistics	Displays additional information about high-density ports.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Information for all ports is displayed unless a particular port is specified.
- Use the **qos port** command to configure port parameters.
- For ports that are trusted (**Yes** displays in the Trust field), the Trust field includes one of the following characters:

character	definition
+	Indicates that the port is manually configured as trusted through the **qos port trusted** command; the port setting takes precedence over the global trust setting configured through the **qos trust ports** command.
*	Indicates that the port is automatically trusted regardless of the global setting set through the **qos trust ports** command. (Applies to mobile ports and ports configured for 802.1Q.)

Examples

```
-> show qos port 3/1 high-density-module
Slot/   ---------- Enqueuing Thresholds -------------
Port   Up0--Low0   Up1--Low1   Up2--Low2   Up3--Low3
  3/1    30   10     35   10      40   10    575  260
    Protocol IPX      - Classify:tos     Priorities P0-P7: 0 1 2 3 0 1 2
```

output definitions

Slot/Port	The slot and physical port number associated with the virtual port.
QoS	Whether or not the interface supports QoS.

output definitions (continued)

Up0--Low0	The value of the desired upper and lower enqueuing threshold on the specified port for frames with internal priority 0. The range is 0 to 4095 for each value. The threshold may be configured through the **qos port enqueuing thresholds** command.
Up1--Low1	The value of the desired upper and lower enqueuing threshold on the specified port for frames with internal priority 1. The range is 0 to 4095 for each value. The threshold may be configured through the **qos port enqueuing thresholds** command.
Up2--Low2	The value of the desired upper and lower enqueuing threshold on the specified port for frames with internal priority 2. The range is 0 to 4095 for each value. The threshold may be configured through the **qos port enqueuing thresholds** command.
Up3--Low3	The value of the desired upper and lower enqueuing threshold on the specified port for frames with internal priority 3. The range is 0 to 4095 for each value. The threshold may be configured through the **qos port enqueuing thresholds** command.
Protocol	The protocol associated with the high-density port. The protocol may be configured through the **qos port protocol priority** command.
Classify	How traffic with this protocol is classified on this port. The classification may be modified through the **qos port protocol priority** command.
Priorities	How the priority of incoming frames with this protocol is mapped to the internal priority on the port. This mapping may modified through the **qos port protocol priority** command.

Release History

Release 5.1; command was introduced.

Related Commands

qos port	Configures a physical port for QoS.
qos port enqueuing thresholds	Specifies the First In First Out (FIFO) thresholds on the port for enqueuing packets
qos port protocol priority	Specifies the internal priority for incoming priority frames of a particular protocol type on a QoS port.

MIB Objects

```
alaQoSPortTable
   alaQoSPortSlot
   alaQoSPortPort
   alaQoSPortEnqueuingThresholdP0Upper
   alaQoSPortEnqueuingThresholdP0Lower
   alaQoSPortEnqueuingThresholdP1Upper
   alaQoSPortEnqueuingThresholdP1Lower
   alaQoSPortEnqueuingThresholdP2Upper
   alaQoSPortEnqueuingThresholdP2Lower
   alaQoSPortEnqueuingThresholdP3Upper
```

```
alaQoSPortEnqueuingThresholdP3Lower
alaQoSProtocolId
alaQoSPortProtocolPriorityP0
alaQoSPortProtocolPriorityP1
alaQoSPortProtocolPriorityP2
alaQoSPortProtocolPriorityP3
alaQoSPortProtocolPriorityP4
alaQoSPortProtocolPriorityP5
alaQoSPortProtocolPriorityP6
alaQoSPortProtocolPriorityP7
alaQoSPortProtocolClassification
```

show qos port pdis

Displays priority descriptors for 802.1p or ToS traffic on high-density modules.

show qos port [*slot/port***] pdis**

Syntax Definitions

slot/port	The physical slot and port number. For example: 3/1

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

Use this command to display current priority descriptors, which determine how queuing is performed for particular traffic types on the port. The switch has a default priority descriptor scheme, which may be modified through the **qos port protocol priority** command.

Examples

```
-> show qos port 3/2 pdis
Current PDI entries in the High Density Module
           Ingress to Internal Priority Map
PDI Protocol *** 0  1  2  3  4  5  6  7 **** Classification Type
Port  3/2
 0  BPDU         0  0  1  1  2  2  3  3      802.1p
 1  LACPSNAP     3  3  3  3  3  3  3  3      802.1p
 2  LACPETH      3  3  3  3  3  3  3  3      802.1p
 3  IPV4         0  0  1  1  2  2  3  3      tos
 4  ARP          0  0  1  1  2  2  3  3      802.1p
 5  RARP         0  0  1  1  2  2  3  3      802.1p
 6  IPV6         0  0  1  1  2  2  3  3      802.1p
 7  IPX          1  1  2  2  3  3  0  0      802.1p
 8  APPLE        0  0  1  1  2  2  3  3      802.1p
 9  SNA          0  0  1  1  2  2  3  3      802.1p
 10 DECNET       0  0  1  1  2  2  3  3      802.1p
 11 User1        0  0  1  1  2  2  3  3      tos
 12 User2        0  0  1  1  2  2  3  3      tos
 13 User3        0  0  1  1  2  2  3  3      tos
 14 User4        0  0  1  1  2  2  3  3      tos
 15              0  0  1  1  2  2  3  3      tos
```

output definitions

PDI	Priority Descriptor Index; corresponds to the traffic protocol.
Protocol	The protocol for the traffic. In addition to the built-in protocols, four user-defined protocols may be configured.

output definitions (continued)

0 – 7	ToS or 802.1p values 0 through 7 mapped to internal priorities 0 through 3. (0 is lowest priority)
Classification Type	Whether the traffic priority is set with 802.1p or ToS/DSCP.

Release History

Release 5.1; command was introduced.

Related Commands

qos port	Configures a physical port for QoS.
qos port protocol priority	Specifies the internal priority for incoming priority frames of a particular protocol type on a QoS port.

MIB Objects

```
alaQoSPortPdiTable
   alaQoSPortPdiSlot
   alaQoSPortPdiPort
   alaQoSPortPdiId
   alaQoSPortPdiPriorityType
   alaQoSPortPdiPriorityP0
   alaQoSPortPdiPriorityP1
   alaQoSPortPdiPriorityP2
   alaQoSPortPdiPriorityP3
   alaQoSPortPdiPriorityP4
   alaQoSPortPdiPriorityP5
   alaQoSPortPdiPriorityP6
   alaQoSPortPdiPriorityP7
```

show qos queue

Displays information for all QoS queues.

show qos queue

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

All queue information is displayed.

Examples

```
-> show qos queue
Slot/              Bandwidth Max  Max          Packets
Port  VPN Pri Wt   Min   Max Bufs Depth      Xmit/Drop      Type Action
0/2     *  -   0    *  1.00G    *     *         */*          DRR (Default)
0/2     *  -   0    *  1.00G    *     *         */*          DRR (Default)
0/2     *  -   0    *  1.00G    *     *         */*          DRR (Default)
0/2     *  -   0    *  1.00G    *     *         */*          DRR (Default)
0/2     *  6   -    *  1.00G    *     *         */*          PRI (Default)
0/2     *  7   -    *  1.00G    *     *         */*          PRI (Default)
0/3     *  -   0    *  1.00G    *     *         */*          DRR (Default)
0/3     *  -   0    *  1.00G    *     *         */*          DRR (Default)
0/3     *  -   0    *  1.00G    *     *         */*          DRR (Default)
0/3     *  -   0    *  1.00G    *     *         */*          DRR (Default)
0/3     *  6   -    *  1.00G    *     *         */*          PRI (Default)
0/3     *  7   -    *  1.00G    *     *         */*          PRI (Default)
1/1     0  -   0    *   100M    *     *         */*          DRR (Default)
1/1     0  -   0    *   100M    *     *         */*          DRR (Default)
1/1     0  -   0    *   100M    *     *         */*          DRR (Default)
1/1     0  -   0    *   100M    *     *         */*          DRR (Default)
1/1     0  4   -    *   100M    *     *         */*          PRI (Default)
1/1     0  5   -    *   100M    *     *         */*          PRI (Default)
```

output definitions

Slot/Port	The physical slot/port numbers associated with the queue.
VPN	The virtual port number associated with the queue.

output definitions (continued)

Pri	The priority associated with the queue, configured through the **policy action priority** command. This configured priority value is mapped to a software queue value, which is displayed here. There are four software queues; the action priority is mapped as follows: action priority of 0–1 displays as priority 0 action priority of 2–3 displays as priority 2 action priority of 4–5 displays as priority 4 action priority of 6–7 displays as priority 6
Wt	The weight value assigned to the weighted round robin (WRR) queues when priority-WRR is the servicing mode for the port.
Bandwidth Min	The minimum bandwidth requirement for the queue (the bandwidth allowed by the lowest minimum configured for all actions associated with the queue).
Bandwidth Max	The maximum bandwidth requirement for the queue (the bandwidth allowed by the maximum configured for all actions associated with the queue). Configured through the **policy action maximum bandwidth** command.
Max Bufs	The number of buffers associated with the queue. Configured through the **policy action maximum buffers** command.
Max Depth	The maximum queue depth, in bytes. Configured through the **policy action maximum depth** command.
Packets Xmit/Drop	The number of packets transmitted/dropped from this queue.
(Type/Action)	The type of queue. For QoS queues, a second line displays parameters specified by the action. The types of queues are as follows: • **Default** —Set up for traffic that does not match a condition on the port. • **Flood**—Set up for flooded or broadcast traffic. • **Best Effort**—Set up for traffic that does not match a condition on the VPN. • **QOS**—Created by the switch because the traffic matched a condition. When traffic matches a condition and queue is set up, another line displays to show the parameters specified by the action corresponding to the condition. *An asterisk displays in fields where the parameter was not specified by the action.* In other words, the first line shows what is actually happening in the queue; the second line shows what the action specified.

Release History

Release 5.1; command was introduced.
Release 5.3.1; **Wt** field was added.

Related Commands

policy rule	Configures a policy rule on the switch. A rule is made up of a condition (for classifying incoming traffic) and an action (to be applied to outgoing traffic).

MIB Objects

```
alaQoSQueueTable
   alaQoSQueueId
   alaQoSQueueSlot
   alaQoSQueuePort
   alaQoSQueuePortId
   alaQoSQueueType
   alaQoSQueuePriority
   alaQoSQueueMinimumBandwidth
   alaQoSQueueMaximumBandwidth
   alaQoSQueueAverageBandwidth
   alaQoSQueueMaximumDepth
   alaQoSQueueMaximumBuffers
   alaQoSQueue8021p
   alaQoSQueuePacketsSent
   alaQoSQueuePacketsDropped
   alaQoSQueueMaxLength
   alaQoSQueueAverageLength
   alaQoSQueueCurrentLength
   alaQoSQueueAction
```

show qos slice

Displays information about buffers on QoS slices of QoS slots. A *slice* is a logical section of hardware and corresponds to particular ports on the interface.

show qos slice [*slot/slice***]**

Syntax Definitions

slot/slice	The slot number and slice for which you want to view information. On the OmniSwitch 7700/7800, each network interface module has one slice (slice 0). On the OmniSwitch 8800, each network interface module may have up to 4 slices (slices 0 to 3). On the OmniSwitch 6624/6648, each block of 24 ports makes up a slice (slice 0 and slice 1); the uplink slots are part of slice 0.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Information for all slots/slices is displayed unless a particular slot/slice is requested.
- This command is useful for finding out if particular interfaces are running out of buffers.
- To display enqueuing and discarding thresholds for high-density gigabit modules, use the **show qos slice high-density-module** command.

Examples

```
-> show qos slice
Slot/                  Buffers              Free        Threshold
Slice    Type    Max    Denied   Dropped  List1  List2   List1  List2
 1/0   coronado 2048        0         0    3595    499    1798    124
                                                         1258    124
                                                          719     75
                                                          179     64
 2/0   coronado 2048        0         0    3593    499    1798    124
                                                         1258    124
                                                          719     75
                                                          179     64
 2/1   coronado 2048        0         0    3594    499    1798    124
                                                         1258    124
                                                          719     75
                                                          179     64
 2/2   coronado 2048        0         0    3593    499    1798    124
                                                         1258    124
                                                          719     75
                                                          179     64
```

output definitions

Slot/Slice	The slot and slice number.
Type	The type of slice (**coronado**, **ixe2424**, etc).
Buffers Max	The maximum number of buffers supported by the slice of CPU on the slot.
Buffers Denied	The number of buffers denied on the slice.
Buffers Dropped	The number of buffers dropped on the slice.
Free List1	The number of free buffers.
Free List2	The number of free buffers.
Threshold List 1	The number of buffers that have reached the threshold.
Threshold List2	The number of buffers that have reached the threshold.

Release History

Release 5.1; command was introduced.

Related Commands

policy rule	Configures a policy rule on the switch. A rule is made up of a condition (for classifying incoming traffic) and an action (to be applied to outgoing traffic).
qos slice	Creates an entry in the protocol CAM of a high-density gigabit Ethernet slot/slice.

MIB Objects

```
alaQoSSlotTable
   alaQoSSlotSlot
   alaQoSSlotSlice
   alaQoSSlotType
   alaQoSSlotMaxBuffers
   alaQoSSlotFreeBuffers1
   alaQoSSlotFreeBuffers2
   alaQoSSlotThreshold1Low
   alaQoSSlotThreshold1Medium
   alaQoSSlotThreshold1High
   alaQoSSlotThreshold1Urgent
   alaQoSSlotThreshold2Low
   alaQoSSlotThreshold2Medium
   alaQoSSlotThreshold2High
   alaQoSSlotThreshold2Urgent
   alaQoSSlotBuffersDenied
   alaQoSSlotBuffersDeniedAverage
   alaQoSSlotBuffersDropped
   alaQoSSlotBuffersDroppedAverage
```

show qos slice high-density-module

Displays information about servicing thresholds and WRED thresholds for slots/slices on high-density gigabit modules. A *slice* is a logical section of hardware and corresponds to particular ports on the interface.

show qos slice [*slot/slice***] high-density-module**

Syntax Definitions

slot/slice	The slot number and slice for which you want to view information. On the OmniSwitch 7700/7800, each slot has one slice (slice 0). On the OmniSwitch 8800, each slot may have up to 4 slices (slices 0 to 3).

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Information for all high-density slot/slices is displayed unless a specific slot/slice is requested.
- The threshold values in the display reflect a current or average “chunk” count of buffer. A “chunk” is 64 bytes of the 256-Kbyte buffer on the high-density interface (4096 possible chunks). Every received packet on the high-density interface may be stored in a 64-byte chunk of the buffer.
- To display general statistics for slices, use the **show qos slice** command.

Examples

```
-> show qos slice high-density-module
Slot/ Servicing Thresholds  ----------------- WRED Thresholds
-----------
Slice  P1   P2   P3  Mode   Up0--Low0  Up1--Low1  Up2--Low2  Up3--Low4
Wgt
 3/0   94  182  360  pri w  4095 4095  4095 4095  4095 4095  4095 4095
4
    Protocol User1 - Ethertype:0600  DSAP:00  SSAP:00 802.3:Disabled
Priority
    Protocol User2 - Ethertype:0600  DSAP:00  SSAP:00 802.3:Disabled
Fallback
    DSCP Table  -
                  0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
                  1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
                  2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
                  3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3
```

output definitions

Slot/Slice	The slot and slice number.
Servicing Thresholds:	
P1	The value of the servicing threshold for incoming packets with internal priority 1. The threshold specifies a maximum number of “chunks” of buffer. (See Usage Guidelines for the definition of “chunk.”) The high-density module will continue queuing priority 1 packets until the threshold is reached. When the threshold is reached, packets with priority 1 are sent out. (P1 is set by the switch or user-configured based on the servicing algorithm specified through the **qos slice servicing mode** command.)
P2	The value of the servicing threshold for incoming packets with internal priority 2. The threshold specifies a maximum number of “chunks” of buffer. (See Usage Guidelines for the definition of “chunk.”) The high-density module will continue queuing priority 2 packets until the threshold is reached. When the threshold is reached, packets with priority 2 are sent out. (P2 is set by the switch or user-configured based on the servicing algorithm specified through the **qos slice servicing mode** command.)
P3	The value of the servicing threshold for incoming packets with internal priority 3. The threshold specifies a maximum number of “chunks” of buffer. (See Usage Guidelines for the definition of “chunk.”) The high-density module will continue queuing priority 3 packets until the threshold is reached. When the threshold is reached, packets with priority 3 are sent out. (P3 is set by the switch or user-configured based on the servicing algorithm specified through the **qos slice servicing mode** command.)
Mode	The servicing mode, or algorithm, used for this slot/slice. The servicing mode determines the values of the servicing thresholds. Possible modes are **pri w** (Priority Weighted Round Robin), **wrr** (Weighted Round Robin), or **strct** (strict priority).
WRED Thresholds:	
Up0--Low0	The upper and lower thresholds of the average buffer “chunk” count for frames with priority 0. (See Usage Guidelines for the definition of “chunk.”) When the lower threshold is reached, some frames with priority 0 are discarded; when the upper threshold is reached, all frames with priority 0 are discarded. The threshold is configurable through the **qos slice wred thresholds** command.
Up1--Low1	The upper and lower thresholds of the average buffer “chunk” count for frames with priority 1. (See Usage Guidelines for the definition of “chunk.”) When the lower threshold is reached, some frames with priority 1 are discarded; when the upper threshold is reached, all frames with priority 1 are discarded. The threshold is configurable through the **qos slice wred thresholds** command.
Up2--Low2	The upper and lower thresholds of the average buffer “chunk” count for frames with priority 2. (See Usage Guidelines for the definition of “chunk.”) When the lower threshold is reached, some frames with priority 2 are discarded; when the upper threshold is reached, all frames with priority 2 are discarded. The threshold is configurable through the **qos slice wred thresholds** command.

output definitions (continued)

Up3--Low3	The upper and lower thresholds of the average buffer "chunk" count for frames with priority 3. (See Usage Guidelines for the definition of "chunk.") When the lower threshold is reached, some frames with priority 3 are discarded; when the upper threshold is reached, all frames with priority 3 are discarded. The threshold is configurable through the **qos slice wred thresholds** command.
Wgt	The value (a negative power of 2) used by the switch to compute the average chunk count. The value may be modified through the **qos slice wred thresholds** command.
DSCP Table	The mapping of priority (0–3) to DSCP index values (0–63) on this slot/slice. There are 4 rows and 16 columns. The first row shows priorities for DSCP index values 0 to 15; the second row shows priorities for index values 16 to 31; the third row shows priorities for index values 32 to 47; the last row shows priorities for index values 48 to 63. The priority mapping may be modified through the **qos slice dscp** command.

Release History

Release 5.1; command was introduced.

Related Commands

qos slice servicing mode	Specifies the dequeuing algorithm for a slot/slice on a high-density gigabit module.
qos slice	Creates an entry in the protocol CAM of a high-density gigabit Ethernet slot/slice.
qos slice wred thresholds	Specifies the buffer accumulation thresholds and weight for the Weighted Random Early Detection (WRED) discarding algorithm on a high-density gigabit slot/slice.
qos slice dscp	Modifies the internal table for mapping DSCP values to internal priorities.

MIB Objects

```
alaQoSSlotTable
   alaQoSSlotSlot
   alaQoSSlotSlice
   alaQoSSlotCbqThresholdP1
   alaQoSSlotCbqThresholdP2
   alaQoSSlotCbqThresholdP3
   alaQoSSlotCbqThresholdMode
   alaQoSSlotWredThresholdP0Upper
   alaQoSSlotWredThresholdP0Lower
   alaQoSSlotWredThresholdP1Upper
   alaQoSSlotWredThresholdP1Lower
   alaQoSSlotWredThresholdP2Upper
   alaQoSSlotWredThresholdP2Lower
   alaQoSSlotWredThresholdP3Upper
   alaQoSSlotWredThresholdP3Lower
   alaQoSSlotWredAverageCounterWeight
```

show qos slice pcams

Displays the current CAM entries for high-density modules on the switch.

show qos slice [*slot/slice***] pcams**

Syntax Definitions

slot/slice	The slot number and slice for which you want to view information. On the OmniSwitch 7700/7800, each slot has one slice (slice 0). On the OmniSwitch 8800, each slot may have up to 4 slices (slices 0 to 3).

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Protocol CAM entries are used by the switch for calculating internal protocol numbers. Use the **qos slice** command to create user-defined entries. User-defined entries may be used to take precedence over built-in entries, which cannot be deleted.
- Each slice may have four additional user-configured entries—two priority entries and two fallback entries. Priority entries take precedence over default entries and display at the beginning of the list. (See entry 0 in the example below.) Fallback entries do not take precedence over default entries and display at the end of the list. The **qos slice** command is used to configure entries in the CAM.

Examples

```
-> show qos slice 3/0 pcams

Current CAM entries in the High Density Module
CAM #  Status  Ethertype  DSAP  SSAP      802.3   Protocol
Slice  3/0
   0  Active     0600      xx    xx               User1
   1  Inactive   xxxx      xx    xx
   2  Active     xxxx      42    42      Enabled   BPDU
   3  Active     8809      aa    aa      Enabled   LACPSNAP
   4  Active     8809      xx    xx      Disabled  LACPETH
   5  Active     0800      aa    aa      Enabled   IPV4
   6  Active     0800      xx    xx      Disabled  IPV4
   7  Active     0806      aa    aa      Enabled   ARP
   8  Active     0806      xx    xx      Disabled  ARP
   9  Active     8035      aa    aa      Enabled   RARP
  10  Active     8035      xx    xx      Disabled  RARP
  11  Active     86dd      aa    aa      Enabled   IPV6
  12  Active     86dd      xx    xx      Disabled  IPV6
  13  Active     8137      aa    aa      Enabled   IPX
  14  Active     xxxx      e0    e0      Enabled   IPX
  15  Active     xxxx      ff    ff      Enabled   IPX
  16  Active     8137      xx    xx      Disabled  IPX
```

```
 17  Active     80f3      aa    aa      Enabled   APPLE
 18  Active     809b      aa    aa      Enabled   APPLE
 19  Active     xxxx      04    04      Enabled   SNA
 20  Active     6003      xx    xx      Disabled  DECNET
 21  Active     0600      xx    xx                User2
 22  Inactive   xxxx      xx    xx
 23  Inactive   xxxx      xx    xx
```

output definitions

CAM	CAM index number, corresponds to the traffic protocol.
Status	Whether the entry is active or inactive. Default CAM entries are always active. Inactive entries are currently not used. Up to four user-configured entries (two priority, two fallback) may overwrite inactive entries.
Ethertype	The ethertype code for the entry.
DSAP	The destination Service Access Point (DSAP) for this entry.
SSAP	The source Service Access Point (SSAP) for this entry.
802.3	Whether 802.3 is enabled or disabled for this entry.
Protocol	The protocol associated with the entry.

Release History

Release 5.1; command was introduced.

Related Commands

qos slice	Creates an entry in the protocol CAM of a high-density gigabit Ethernet slot/slice.

MIB Objects

```
alaQoSSlotPcamTable
   alaQoSSlotPcamSlot
   alaQoSSlotPcamSlice
   alaQoSSlotPcamId
   alaQoSSlotPcamEthertype
   alaQoSSlotPcamDsap
   alaQoSSlotPcamSsap
   alaQoSSlotPcam8023Enabled
   alaQoSSlotPcamProtocolNumber
   alaQoSSlotPcamEnableEntry
   alaQoSSlotPcamEnable8023
   alaQoSSlotPcamEnableDsap
   alaQoSSlotPcamEnableSsap
```

show qos log

Displays the log of QoS events.

show qos log

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use this command to display the current QoS log. To clear the log, use the **qos clear log** command.

Examples

```
-> show qos log
**QOS Log**
Insert rule 0
Rule index at 0
Insert rule 1
Rule index at 1
Insert rule 2
Rule index at 2
Enable rule r1 (1) 1,1
Enable rule r2 (0) 1,1
Enable rule yuba1 (2) 1,1
Verify rule r1(1)
Enable rule r1 (1) 1,1
Really enable r1
Update condition c1 for rule 1 (1)
Verify rule r2(1)
Enable rule r2 (0) 1,1
Really enable r2
Update condition c2 for rule 0 (1)
Verify rule yuba1(1)
Enable rule yuba1 (2) 1,1
Really enable yuba1
Update condition yubamac for rule 2 (1)
QoS Manager started TUE MAR 10 13:46:50 2002

Match rule 2 to 1
Match rule 2 to 2
Match rule 2 to 3
```

Release History

Release 5.1; command was introduced.

Related Commands

qos clear log	Clears messages in the current QoS log.
qos log lines	Configures the number of lines in the QoS log.

MIB Objects

N/A

show qos config

Displays global information about the QoS configuration.

show qos config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use this command to view the current global configuration for QoS. Use the **show qos statistics** command to view statistics about the QoS software in the switch.

Examples

```
-> show qos config
QoS Configuration:
 Enabled            : Yes
 Pending changes    : policy
Classifier:
 Default queues          : 6
 Default queue service   : Strict Priority + Weighted Fair
        queue 0 weight   : 3
        queue 1 weight   : 3
        queue 2 weight   : 3
        queue 3 weight   : 3
 Trusted ports           :  No
 Classify bridged at L3  : Yes
 Flow table timeout      : 300 seconds
 Fragment table timeout  : 10 seconds
 Reflexive flow timeout  : n/a
 NAT flow timeout        : n/a
 Classify fragments          :  No
 Default bridged disposition : accept
 Default routed disposition  : accept
 Default IGMP disposition    : accept
Logging:
 Log lines      : 512
 Log level      : 7
 Log to console :  No
 Forward log    :  No
Stats interval  : 10 seconds
Debug           : info
```

output definitions

QoS Configuration	Whether or not QoS is enabled or disabled. Configured through the **qos** command.
Default queues	The number of default queues for QoS ports. Configured through the **qos default queues** command.
Default queue service	The default servicing mode for the switch (**Strict Priority** or **Strict Priority + Weighted Fair**).
queue 0 weight	The weighted value for WFQ 0. Only appears if the default servicing mode is set to priority-WRR.
queue 1 weight	The weighted value for WFQ 1. Only appears if the default servicing mode is set to priority-WRR.
queue 2 weight	The weighted value for WFQ 2. Only appears if the default servicing mode is set to priority-WRR.
queue 3 weight	The weighted value for WFQ 3. Only appears if the default servicing mode is set to priority-WRR.
Trusted Ports	The default trusted mode for switch ports. Configured through the **qos trust ports** command.
Classify bridged at L3	Whether or not bridged traffic is classified using Layer 3 information. Note that this field will always contain a **yes** value. Configured through the **qos classifyl3 bridged** command.
Flow table timeout	The number of seconds that the switch will wait for all packets of a flow to arrive. Configured through the **qos flow timeout** command.
Fragment table timeout	The number of seconds that the switch will wait for all fragments of a packet to arrive. Configured through the **qos fragment timeout** command.
Reflexive flow timeout	The number of seconds the switch will wait for anticipated or reflexive flows. Configured through the **qos reflexive timeout** command.
NAT flow timeout	The number of seconds the switch will wait for traffic from an address translation flow. Configured through the **qos nat timeout** command.
Classify fragments	Whether the switch will classify each fragment of a flow. Configured through the **qos classify fragments** command.
Default bridged disposition	Whether or not bridged traffic that does not match any policy will be accepted or denied on the switch Configured through the **qos default bridged disposition** command.
Default routed disposition	Whether or not routed traffic that does not match any policy will be accepted or denied on the switch. Configured through the **qos default routed disposition** command.
Default IGMP disposition	Whether or not multicast flows that do not match any policy will be accepted or denied on the switch. Configured through the **qos default multicast disposition** command.
Log lines	The number of lines included in the QoS log. Configured through the **qos log lines** command.
Log level	The level of log detail. Configured through the **qos log level** command.

output definitions (continued)

Log to console	Whether or not log messages are sent to the console. Configured through the **qos log console** command.
Forward log	Whether or not logged events are sent to the policy server software in the switch in real time. Configured through the **qos forward log** command.
Stats interval	How often the switch polls network interfaces for statistics about QoS events. Configured through the **qos stats interval** command.
Debug	The type of information that will be displayed in the QoS log. Configured through the **debug qos** command. A value of **info** indicates the default debugging type.

Release History

Release 5.1; command was introduced.
Release 5.3.1; **Default queue service**, **queue 0 weight, queue 1 weight, queue 2 weight, queue 3 weight** fields were added.

Related Commands

qos	Enables or disables QoS. This base command may be used with keyword options to configure QoS globally on the switch.
show qos statistics	Displays statistics about the QoS configuration.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigEnable
   alaQoSConfigLogLines
   alaQoSConfigLogLevel
   alaQoSConfigLogConsole
   alaQoSConfigFlowTimeout
   alaQoSConfigFragmentTimeout
   alaQoSConfigReflexiveTimeout
   alaQoSConfigClassifyFragments
   alaQoSConfigDefaultMulticastDisposition
   alaQoSConfigDefaultDisposition
   alaQoSConfigDebug
   alaQoSConfigStatsInterval
```

show qos statistics

Displays statistics about the QoS configuration.

show qos statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This command displays statistics about the global QoS configuration. Use the **show qos config** command to display information about configurable global parameters.

Examples

```
-> show qos statistics
QoS stats
                          Events   Matches     Drops
  L2                   :        15         0         0
  L3 Inbound           :         0         0         0
  L3 Outbound          :         0         0         0
  IGMP Join            :         0         0         0
  Fragments            : 0
  Bad Fragments        : 0
  Unknown Fragments    : 0
  Sent NI messages     : 9
  Received NI messages : 4322
  Failed NI messages   : 0
  Load balanced flows  : 0
  Reflexive flows      : 0
  Reflexive correction : 0
  Flow lookups         : 0
  Flow hits            : 0
  Max PTree nodes      : 0
  Max PTree depth      : 0
```

output definitions

Events	The number of Layer 2 or Layer 3 flows transmitted on the switch.
Matches	The number of Layer 2 or Layer 3 flows that match policies.
Drops	The number of Layer 2 or Layer 3 flows that were dropped.
L2	The number of Layer 2 events, matches, and drops.

output definitions (continued)

L3 Ingress	The number of Layer 3 ingress events, matches, and drops.
L3 Egress	The number of Layer 3 egress events, matches, and drops
IGMP join	The number of multicast events, matches, and drops.
Fragments	The number of fragments dropped.
Bad Fragments	The number of fragments received with an offset of 1.
Unknown Fragments	The number of out-of-order fragments received.
Sent NI messages	The number of messages sent to network interfaces.
Received NI messages	The number of messages received by network interfaces.
Failed NI messages	The number of failed message attempts to network interfaces.
Load balanced flows	The number of Server Load Balance flow entries.
Reflexive flows	The number of reflexive flows.
Reflexive correction	The number of reflexive flow corrections.
Flow lookups	The number of flow table lookups.
Flow hits	The number of flow table lookup hits.
Max PTree nodes	The highest number of nodes in the classifer tree.
Max Ptree depth	The length of the longest path in the classifer tree.

Release History

Release 5.1; command was introduced.

Related Commands

qos stats reset	Resets QoS statistic counters to zero.

MIB Objects

```
alaQoSConfigL2Events
alaQoSConfigL2matches
alaQoSConfigL2Drops
alaQoSConfigL3IngressEvents
alaQoSConfigL3IngressMatches
alaQoSConfigL3IngressDrops
alaQoSConfigL3EgressEvents
alaQoSConfigL3EgressMatches
alaQoSConfigL3EgressDrops
alaQoSConfigFragments
alaQoSConfigBadFragments
alaQoSConfigUnknownFragments
```

39 Policy Server Commands

This chapter describes CLI commands used for managing policies downloaded to the switch from an attached LDAP server. Policy rules may be created on an attached server through the PolicyView GUI application. Policy rules may also be created on the switch directly through CLI or SNMP commands. This chapter describes commands related to managing LDAP policies only. See Chapter 38, "QoS Commands," for information about commands for creating and managing policies directly on the switch.

ALCATEL-IND1-POLICY-MIBThe policy server commands are summarized here:

policy server load
policy server flush
policy server
show policy server
show policy server long
show policy server statistics
show policy server rules
show policy server events

policy server load

Downloads policies from a LDAP server. These policies are created through the PolicyView management application.

policy server load

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Policies are downloaded to the switch from the directory server with the highest preference setting; this server must be enabled and operational (able to bind).

Examples

```
-> policy server load
```

Release History

Release 5.1; command was introduced.

Related Commands

policy server flush	Removes all cached LDAP policy data from the switch.

MIB Objects

```
serverPolicyDecision
```

policy server flush

Removes all cached LDAP policy data from the switch.

policy server flush

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use this command to remove LDAP policies. Policies configured through the CLI or SNMP are not removed.

Examples

```
-> policy server flush
```

Release History

Release 5.1; command was introduced.

Related Commands

policy server load	Downloads policies from a LDAP server. These policies are created through the PolicyView management application.

MIB Objects

```
serverPolicyDecision
```

policy server

Configures operational parameters for an LDAP-enabled directory server on which policies are stored.

policy server *ip_address* **[port** *port_number***] [admin {up | down}] [preference** *preference***] [user** *user_name* **password** *password***] [searchbase** *search_string***] [ssl | no ssl]**

no policy server *ip_address* **[port** *port_number***]**

Syntax Definitions

ip_address	The IP address of the LDAP-enabled directory server.
port_number	The TCP/IP port number used by the switch to connect to the directory server.
up	Enables the specified policy server to download rules to the switch (servers are **up** by default.)
down	Prevents the specified policy server from downloading rules to the switch.
preference	Determines which directory server is used for policy downloads when multiple servers are configured. The range is 0–255. The server with the highest value is used as the policy server. If that server becomes unavailable, the server with the next highest preference value is used for policy downloads.
user_name	The user name for accessing the database entries on the directory server. When spaces are used in the user name, quotation marks must be included: **"Directory Manager"** is an example.
password	The password associated with the user name. The password must match the password defined on the directory server.
search_string	The root of the directory on the search that will be searched for policy information. Typically, the *search_string* includes **o=***organization* and **c=***country*. For example, **o=company** and **c=country**.
ssl	Enables a Secure Socket Layer between the switch and the policy server.
no ssl	Disables a Secure Socket Layer between the switch and the policy server.

Defaults

parameter	default
admin	**up**
port_number	389 (SSL disabled) 636 (SSL enabled)
preference	0
ssl | no ssl	**no ssl**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

If you change the port number, another entry is added to the policy server table; an existing port number is not changed. To remove a port number, use the **no** form of the **policy server** command with the relevant policy server IP address and the port number you want to remove.

Examples

```
-> policy server 222.22.22.2 port 345 user dirmgr password secret88 searchbase
ou=qos,o=company,c=country
```

Release History

Release 5.1; command was introduced.

Related Commands

show policy server	Displays information about policies downloaded from an LDAP server.

MIB Objects

```
DIRECTORYSERVERTABLE
   directoryServerAddress
   directoryServerPort
   directoryServerAdminStatus
   directoryServerPreference
   directoryServerUserId
   directoryServerAuthenticationType
   directoryServerPassword
   directoryServerSearchbase
   directoryServerEnableSSL
```

show policy server

Displays information about servers from which policies may be downloaded to the switch.

show policy server

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This command displays basic information about policy servers. Use the **show policy server long** command to display more details about the servers.

Examples

```
-> show policy server

Server   IP Address   port   enabled  status   primary
------+-------------+-----+---------+--------+--------
   1   208.19.33.112  389      Yes      Up        X
   2   208.19.33.66   400      No       Down      -
```

output definitions

Server	The index number corresponding to the LDAP server.
IP Address	The IP address of the LDAP server.
port	The TCP/IP port number used by the switch to connect to the policy server.
enabled	Whether or not the policy server is enabled.
status	The state of the policy server, **Unkn**, **Up** or **Down**.
primary	Indicates whether the server is the primary server; this server will be used for the next download of policies; only one server is a primary server.

Release History

Release 5.1; command was introduced.

Related Commands

policy server	Configures operational parameters for an LDAP-enabled directory server on which policies are stored.

MIB Objects

```
directoryServerTable
   directoryServerAddress
   directoryServerPort
   directoryServerAdminState
```

show policy server long

Displays more detailed information about an LDAP policy server.

show policy server long

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This command displays detailed information about policy servers. Use the **show policy server** command to display basic information about policy servers.

Examples

```
-> show policy server long
LDAP server 0
  IP address           : 155.132.44.98,
  TCP port             : 16652,
  Enabled              : Yes,
  Operational status   : Unkn,
  Preference           : 99,
  Authentication       : password,
  SSL                  : Disabled,
  login DN             : cn=Directory Manager,
  searchbase           : ou:4.1, cn=policyRoot, o=company.fr
  Last load time       : 09/13/01 16:38:18
LDAP server 1
  IP address           : 155.132.48.27,,
  TCP port             : 21890,
  Enabled              : Yes,
  Operational status   : Unkn,
  Preference           : 50,
  Authentication       : password,
  SSL                  : Disabled,
  login DN             : cn=Directory Manager,
  searchbase           : o=company.fr
  Last load time       : 00/00/00 00:00:00
```

output definitions

IP address	The IP address of the policy server.
TCP port	The TCP/IP port number used by the switch to connect to the policy server.
Enabled	Whether or not the policy server is enabled via the PolicyView application.
Operational status	The state of the policy server, **Up** or **Down**.
Preference	Determines which directory server is used for policy downloads when multiple servers are configured. The range is 0–255. The server with the highest value is used as the policy server. If that server becomes unavailable, the server with the next highest preference value is used for policy downloads.
Authentication	Displays **password** if a user name and password was specified for the server through the **policy server** command. Displays **anonymous** if a user name and password are not configured.
login DN	The directory user name.
searchbase	The searchbase name, which is the root of the directory that will be searched for policy download information.
Last load time	The date and time that policies were last downloaded. Values of zero indicate that no policies have been downloaded.

Release History

Release 5.1; command was introduced.

MIB Objects

```
directoryServerTable
   directoryServerAddress
   directoryServerPort
   directoryServerPreference
   directoryServerAuthenticationType
   directoryServerSearchbase
   directoryServerUserId
   directoryServerPassword
   directoryServerCacheChange
   directoryServerLastChange
   directoryServerAdminStatus
   directoryServerOperStatus
```

show policy server statistics

Displays statistics about policy directory servers.

show policy server statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This command displays statistics about server downloads. For information about server parameters, use the **show policy server** command.

Examples

```
-> show policy server statistics
Server   IP Address     port   accesses  delta   successes delta  errors  delta
------+-------------+-------+---------+-------+----------+-----+-------+------
   1     155.132.44.98  16652       793     793        295     295        0     0
   2     155.132.48.27  21890         0       0          0       0        0     0
```

output definitions

Server	The index number corresponding to the server.
IP Address	The IP address of the LDAP server.
port	The TCP/IP port number used by the switch to connect to the policy server.
accesses	The number of times the server was polled by the switch to download policies.
delta	The change in the number of accesses since the last time the policy server was accessed.
successes	The number of times the server was polled by the switch to download policies and the policies were successfully downloaded.
delta	The change in the number of sucessful policy downloads since the last time the policy server was accessed.
errors	The number of errors returned by the server.
delta	The change in the number of errors returned by the server since the last time the policy server was accessed.

Release History

Release 5.1; command was introduced.

Related Commands

policy server	Configures operational parameters for an LDAP-enabled directory server on which policies are stored.

MIB Objects

```
policyStatsTable
   policyStatsAddress
   policyStatsServerPort
   policyStatsAccessCount
   policyStatsSuccessAccessCount
   policyStatsNotFoundCount
```

show policy server rules

Displays the names of policies originating on a directory server that have been downloaded to the switch.

show policy server rules

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This command displays information about policies created on directory servers only. Chapter 38, "QoS Commands," for information about configuring and displaying policies directly on the switch.

Examples

```
-> show policy server rules
Num       name           prio        scope       status
---+------------------+-------+-------------+------------
1             QoSRule1    0      Provisioned    Active
2             QoSrule2    0      Provisioned    Active
```

Fields are defined here:

output definitions

Num	An index number corresponding to the policy rule.
name	The name of the policy rule; only rules configured through PolicyView are displayed in this table.
prio	The priority or preference of the rule. Indicates the order in which rules will be checked for matching to incoming traffic. If two or more rules apply to the traffic, the rule with the highest preference is applied. Preference is determined when the rule is created.
scope	The type of rule. **Provisioned** is the only type valid for the current release.
status	The status of the rule: **Active** indicates that the rule has been pushed to the QoS software in the switch and is available to apply to traffic; **notInService** means the rule may be pushed to the QoS software in the future but is not available yet (typically because of a variable validity period); **notReady** indicates that the rule will never be pushed to the QoS software because its validity period has expired or because it has been disabled through SNMP.

Release History

Release 5.1; command was introduced.

Related Commands

policy server load	Downloads policies from a LDAP server. These policies are created through the PolicyView management application.

MIB Objects

```
policyRuleNamesTable
   policyRuleNamesIndex
   policyRuleNamesName
   policyRuleOperStatus
```

show policy server events

Displays any events related to a directory server on which policies are stored.

show policy server events

Syntax Definitions

N/A

Defaults

The display is limited to 50 events.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

The Policy Manager initialization event is always the first event logged.

Examples

```
-> show policy server events
 Event Time                      event description
-----------------+---------------------------------------------
09/13/01 16:38:15 Policy manager log init
09/13/01 16:38:17 LDAP server 155.132.44.98/16652 defined
09/13/01 16:38:17 LDAP server 155.132.44.98/21890 defined
09/13/01 16:38:18 PDP optimization: PVP day-of-week all 1
09/13/01 16:38:18 PDP optimization: PVP Month all 1
09/13/01 16:38:18 PDP optimization: PVP Month all 1
09/13/01 16:38:18 PDP optimization: PVP Month all 1
09/13/01 16:38:18 PDP optimization: PVP Month all 1
09/13/01 16:38:18 IP address and mask make bad address change on desination IP
address 155.132.44.98:155.132.44.101
```

Fields are defined here:

output definitions

Event Time	The date and time the policy event occurred.
event description	A description of the event.

Release History

Release 5.1; command was introduced.

Related Commands

policy server	Configures operational parameters for an LDAP-enabled directory server on which policies are stored.

MIB Objects

```
policyEventTable
   policyEventCode
   policyEventDetailString
   policyEventIndex
   policyEventTime
```

40 IP Multicast Switching Commands

IP Multicast Switching (IPMS) is a one-to-many communication technique employed by emerging applications, such as video distribution, news feeds, conferencing, netcasting, and resource discovery (OSPF, RIP2, and BOOTP). Unlike unicast, which sends one packet per destination, multicast sends one packet to all devices in any subnetwork that has at least one device requesting the multicast traffic.

Alcatel's IPMS software is compatible with the following RFCs:

RFC 2236 — Internet Group Management Protocol, Version 2
RFC 2933 — Internet Group Management Protocol MIB
RFC 3376 — Internet Group Management Protocol, Version 3

MIB information for the IPMS commands is as follows:

Filename: AlcatelINDIpms1.mib
Module: ALCATEL-IPMS-IND1-MIB

The following table summarizes the available commands:

ip multicast switching
ip multicast igmp-proxy-version
ip multicast leave-timeout
ip multicast query-interval
ip multicast membership-timeout
ip multicast neighbor-timeout
ip multicast querier-timeout
ip multicast other-querier-timeout
ip multicast flow-timeout
ip multicast priority
ip multicast max-ingress-bandwidth
ip multicast static-neighbor
ip multicast static-querier
ip multicast static-member
ip multicast hardware-routing
show ip multicast switching
show ip multicast groups
show ip multicast neighbors
show ip multicast queriers
show ip multicast forwarding
show ip multicast policy-cache

ip multicast switching

Enables or disables IP multicast switching on a switch.

ip multicast switching

no ip multicast switching

Syntax Definitions

N/A

Defaults

The default is IP multicast disabled.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **no** form of the command to disable IP multicast switching.

Examples

```
-> ip multicast switching
-> no ip multicast switching
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip multicast switching	Displays the current IPMS configuration on a switch.

MIB Objects

```
alaIpmsConfig
   alaIpmsStatus
```

ip multicast igmp-proxy-version

Configures the default version of IGMP membership (either Version 2 or Version 3) reports sent to all dynamically learned multicast neighbors and queriers.

ip multicast igmp-proxy-version {v2 | v3}

ip multicast no igmp-proxy-version

Syntax Definitions

v2	Configures IGMP Version 2.
v3	Configures IGMP Version 3.

Defaults

parameter	default
v2 | v3	**v2**

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to restore the default version (Version 2) of IGMP.
- The command is not supported on OmniSwitch 6600 Family switches.

Examples

```
-> ip multicast igmp-proxy-version v3
-> ip multicast igmp-proxy-version v2
-> ip multicast no igmp-proxy-version
```

Release History

Release 5.1; command was introduced.

Related Commands

ip multicast switching	Enables and disables IP Multicast Switching (IPMS) on a switch.
show ip multicast switching	Displays the current IPMS configuration on a switch.

MIB Objects

```
alaIpmsConfig
   alaIpmsIGMPMembershipProxyVersion
```

ip multicast leave-timeout

Configures the delay in removing a group membership after a leave message has been processed and/or received.

ip multicast leave-timeout *seconds*

ip multicast no leave-timeout

Syntax Definitions

seconds	Configures the delay in removing a group membership after a leave message has been processed and/or received. The valid range for the leave timeout is 0–4294967295 seconds.

Defaults

parameter	default
seconds	1

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **no** form of the command to restore the interval timeout to its default (i.e., 1 second) value.

Examples

```
-> ip multicast leave-timeout 5
-> ip multicast no leave-timeout
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip multicast switching	Displays the current IPMS configuration on a switch.
show ip multicast groups	Displays the status and configuration of IPMS groups on this switch.

MIB Objects

```
alaIpmsConfig
   alaIpmsLeaveTimeout
```

ip multicast query-interval

Sets the time between IGMP queries.

ip multicast query-interval *seconds*

ip multicast no query-interval

Syntax Definitions

query_interval	The time (in seconds) between IGMP queries. The valid range for the query interval is 0–4294967295 seconds.

Defaults

parameter	default
seconds	125

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **no** form of the command to restore the query interval to its default (i.e., 125 seconds) value.

Examples

```
-> ip multicast query-interval 10
-> ip multicast no query-interval
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip multicast switching	Displays the current IPMS configuration on a switch.
show ip multicast groups	Displays the status and configuration of IPMS groups on this switch.

MIB Objects

```
alaIpmsConfig
   alaIpmsQueryInterval
```

ip multicast membership-timeout

Configures the time the switch will wait for an IGMP report before it drops a member from a multicast group.

ip multicast membership-timeout *seconds*

ip multicast no membership-timeout

Syntax Definitions

seconds	The time (in seconds) the switch will wait for an IGMP report before it drops a member from a multicast group. The valid range for the membership timeout is 0–4294967295 seconds.

Defaults

parameter	default
seconds	260

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **no** form of the command to restore the membership timeout to its default (i.e., 260 seconds) value.

Examples

```
-> ip multicast membership-timeout 100
-> ip multicast no membership-timeout
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip multicast switching	Displays the current IPMS configuration on a switch.
show ip multicast groups	Displays the status and configuration of IPMS groups on this switch.

MIB Objects

```
alaIpmsConfig
   alaIpmsMembershipTimer
```

ip multicast neighbor-timeout

Configures the time the switch will wait for a neighbor probe from a router before it removes the corresponding entry for the router from the neighbor table.

ip multicast neighbor-timeout *seconds*

ip multicast no neighbor-timeout

Syntax Definitions

seconds	The time (in seconds) the switch will wait for a neighbor probe from a router before it removes the corresponding entry for the router from the neighbor table. The valid range for the neighbor timeout is 0–4294967295 seconds.

Defaults

parameter	default
seconds	90

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **no** form of the command to restore the neighbor timeout to its default (i.e., 90 seconds) value.

Examples

```
-> ip multicast neighbor-timeout 10
-> ip multicast no neighbor-timeout
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip multicast switching	Displays the current IPMS configuration on a switch.
show ip multicast groups	Displays the status and configuration of IPMS groups on this switch.

MIB Objects

```
alaIpmsConfig
   alaIpmsNeighborTimer
```

ip multicast querier-timeout

Configures the time the switch will wait for an IGMP query from a device before it removes the corresponding entry for the device from the querier table.

ip multicast querier-timeout *seconds*

ip multicast no querier-timeout

Syntax Definitions

seconds	The timeout (in seconds) to receive IGMP queries. The valid range for the querier timeout is 0–4294967295 seconds.

Defaults

parameter	default
seconds	260

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **no** form of the command to restore the querier timeout to its default (i.e., 260 seconds) value.

Examples

```
-> ip multicast querier-timeout 120
-> ip multicast no querier-timeout
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip multicast switching	Displays the current IPMS configuration on a switch.
show ip multicast groups	Displays the status and configuration of IPMS groups on this switch.

MIB Objects

```
alaIpmsConfig
   alaIpmsQuerierTimer
```

ip multicast other-querier-timeout

Configures the timeout for which a currently elected querier is aged and a new multicast querier is elected.

ip multicast other-querier-timeout *seconds*

ip multicast no other-querier-timeout

Syntax Definitions

seconds	The timeout (in seconds) for which a currently elected querier is aged. The valid range for the querier timeout is 0–4294967295 seconds.

Defaults

parameter	default
seconds	255

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **no** form of the command to restore the querier timeout to its default (i.e., 255 seconds) value.

Examples

```
-> ip multicast other-querier-timeout 120
-> ip multicast no other-querier-timeout
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip multicast switching	Displays the current IPMS configuration on a switch.

MIB Objects

```
alaIpmsConfig
   alaIpmsOtherQuerierTimer
```

ip multicast flow-timeout

Configures the time in seconds a multicast flow entry is retained by a switch after the last packet in the flow is processed.

ip multicast flow-timeout *seconds*

Syntax Definitions

seconds	The timeout (in seconds) of a multicast flow entry. The valid range is 0-65535 seconds.

Defaults

parameter	default
seconds (OmniSwitch 7700/ 7800/8800)	120
seconds (OmniSwitch 6600)	64800

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- To restore the IP multicast flow-timeout value to the default (i.e., 120 seconds in OmniSwitch 7700/ 7800/8800 switches and 64800 seconds in OmniSwitch 6600 series), use **ip multicast flow-timeout**, followed by the value 0 (e.g., ip multicast flow-timeout 0).

Examples

```
-> ip multicast flow-timeout 100
-> ip multicast flow-timeout 0
```

Release History

Release 5.4.1; command was introduced.

Related Commands

show ip multicast switching	Displays the current IPMS configuration on a switch.

MIB Objects

```
alaIpmsConfig
     alaIpmsFlowTimer
```

ip multicast priority

Sets the IP multicast priority to the value you specify on all IPMS data queues used in the switch.

ip multicast priority {urgent | high | medium | low}

ip multicast no priority

Syntax Definitions

priority_value	The IP multicast priority on all data queues used in the switch.

Defaults

parameter	default
urgent | high | medium | low	**low**

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

The **no** form of the command restores the multicast priority back to its default (i.e., low) value.

Examples

```
-> ip multicast priority medium
-> ip multicast no priority
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip multicast switching	Displays the current IPMS configuration on a switch.
ip multicast max-ingress-bandwidth	Configures the maximum incoming bandwidth on all IPMS data queues used in the switch.

MIB Objects

```
alaIpmsConfig
   alaIpmsPriority
```

ip multicast max-ingress-bandwidth

Sets the maximum incoming bandwidth on all IPMS data queues used in the switch.

ip multicast max-ingress-bandwidth *megabits*

ip multicast no max-ingress bandwidth

Syntax Definitions

megabits	The maximum incoming bandwidth (in megabits) on all IPMS data queues used in the switch. The valid range for the *megabits* is 1–1000 megabits.

Defaults

parameter	default
megabits	10

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

The **no** form of the command restores the maximum ingress bandwidth back to its default (i.e., 10 megabits) value.

Examples

```
-> ip multicast max-ingress-bandwidth 256
-> ip multicast no max-ingress bandwidth
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip multicast switching	Displays the current IPMS configuration on a switch.
ip multicast priority	Configures the IP multicast priority to the value you specify on all IPMS data queues used in the switch.

MIB Objects

```
alaIpmsConfig
   alaIpmsMaxBandwidth
```

ip multicast static-neighbor

Configures the port as having a multicast routing neighbor.

ip multicast static-neighbor *vlan_id* **{***slot/port* **| linkagg** *agg_num***} [v2 | v3]**

ip multicast no static-neighbor *vlan_id* **{***slot/port* **| linkagg** *agg_num***} [v2 | v3]**

Syntax Definitions

vlan_id	The VLAN to include as a multicast routing neighbor. The valid *vlan_id* range is 0–4095.
slot/port	The slot/port number you want to configure as a multicast routing neighbor.
agg_num	The number of the aggregate group you want to configure as a multicast routing neighbor.
v2	Specifies IGMP Version 2.
v3	Specifies IGMP Version 3.

Defaults

parameter	default
v2 | v3	**v2**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The designated port will receive all multicast streams on the designated VLAN and will also receive IGMP reports for the VLAN.
- Use the **no** form of the command to reset the port to normal operation in regards multicast routing neighbors.
- The **v3** parameter is not relevant to OmniSwitch 6600 Family switches.

Examples

```
-> ip multicast static-neighbor 2 3/15
-> ip multicast static-neighbor 2 linkagg 7
-> ip multicast no static-neighbor 2 3/15 v3
-> ip multicast no static-neighbor 5 4/20
-> ip multicast no static-neighbor 5 linkagg 4
-> ip multicast no static-neighbor 5 4/20 v3
```

Release History

Release 5.1; command was introduced.
Release 5.1.6; **linkagg** parameter was added.

Related Commands

show ip multicast groups	Displays the status and configuration of IPMS groups on this switch.
ip multicast static-querier	Configures a port as having a multicast querier on it.

MIB Objects

```
alaIpmsStaticNeighborTable
   alaIpmsStaticNeighborVlan
   alaIpmsStaticNeighborIfIndex
   alaIpmsStaticNeighborIGMPVersion
   alaIpmsStaticNeighborRowStatus
```

ip multicast static-querier

Configures a port as having a multicast querier on it. The port will receive IGMP reports generated on the designated VLAN. Unlike a multicast neighbor, it will not receive all multicast streams.

ip multicast static-querier *vlan_id* **{***slot/port* **| linkagg** *agg_num***} [v2 | v3]**

ip multicast no static-querier *vlan_id* **{***slot/port* **| linkagg** *agg_num***} [v2 | v3]**

Syntax Definitions

vlan_id	The VLAN to include as a multicast querier. The valid *vlan_id* range is 0–4095.
slot/port	The slot/port number you want to configure as a multicast querier.
agg_num	The number of the aggregate group you want to configure as a multicast querier.
v2	Specifies IGMP Version 2.
v3	Specifies IGMP Version 3.

Defaults

parameter	default
v2 | v3	**v2**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to reset the port to normal operation in regards to the multicast querier feature.
- The **v3** parameter is not relevant to OmniSwitch 6600 Family switches.

Examples

```
-> ip multicast static-querier 2 4/10
-> ip multicast static-querier 2 linkagg 7
-> ip multicast static-querier 3 4/12 v3
-> ip multicast no static-querier 2 4/10
-> ip multicast no static-querier 2 linkagg 4
-> ip multicast no static-querier 3 4/12 v3
```

Release History

Release 5.1; command was introduced.
Release 5.1.6; **linkagg** parameter was added.

Related Commands

show ip multicast queriers	Displays all multicast queriers.
ip multicast static-neighbor	Configures a port as a multicast routing neighbor.

MIB Objects

```
alaIpmsStaticQuerierTable
   alaIpmsStaticQuerierVlan
   alaIpmsStaticNeighborIfIndex
   alaIpmsStaticQuerierIGMPVersion
   alaIpmsStaticQuerierRowStatus
```

ip multicast static-member

Configures a static multicast member.

ip multicast static-member *ip_address vlan_id* **{***slot/port* **| linkagg** *agg_num***}**

ip multicast no static-member *ip_address vlan_id* **{***slot/port* **| linkagg** *agg_num***}**

Syntax Definitions

ip_address	The IP address of the multicast member.
vlan_id	The VLAN to include as a static multicast member. The valid *vlan_id* range is 0–4095.
slot/port	The slot/port number you want to configure as a static multicast member.
agg_num	The number of the aggregate group you want to configure as a static multicast member.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **no** form of the command to reset the port to normal operation in regards to the static multicast member feature.

Examples

```
-> ip multicast static-member 11.0.0.1 2 4/10
-> ip multicast static-member 11.0.0.1 2 linkagg 7
-> ip multicast no static-member 11.0.0.1 2 4/10
-> ip multicast no static-member 11.0.0.1 2 linkagg 4
```

Release History

Release 5.1; command was introduced.
Release 5.3.1; **linkagg** parameter was added.

Related Commands

show ip multicast groups	Displays all detected multicast groups that have members.
ip multicast membership-timeout	Configures a port as a multicast routing neighbor.

MIB Objects

```
alaIpmsStaticMemberTable
   alaIpmsStaticMemberGroupAddr
   alaIpmsStaticMemberVlan
   alaIpmsStaticMemberIfIndex
   alaIpmsStaticMemberRowStatus
```

ip multicast hardware-routing

Enables or disables IP multicast hardware routing.

ip multicast hardware-routing

ip multicast no hardware-routing

Syntax Definitions

N/A

Defaults

IP multicast hardware routing is disabled by default.

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to disable IP multicast hardware routing.
- If hardware routing is enabled, you cannot route IP multicast packets in hardware if any ports are using 802.1Q tagging.
- If hardware routing is enabled, multicast packets cannot be fragmented.
- If hardware routing is enabled, IP Ethernet-II packets cannot be translated to IP Subnetwork Access Protocol (SNAP) and vice versa.

Examples

```
-> ip multicast hardware-routing
-> ip multicast no hardware-routing
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip multicast switching	Displays the current IPMS configuration on a switch.

MIB Objects

```
alaIpmsConfig
   alaIpmsHardwareRoute
```

show ip multicast switching

Displays the current IPMS configuration on a switch.

show ip multicast switching

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show ip multicast switching
IPMS Configuration

IPMS State:            Disabled
Hardware Routing:      Enabled
Priority:              low
Max Ingress Bandwidth: 10
Leave Timeout:         1
Flow Timeout:          20
Membership Timeout:    260
Neighbor Timeout:      90
Querier Timeout:       260
Other Querier Timeout: 255
Query Interval:        125
Default Proxy Version: IGMPv2
Learning Mode:         buffer
```

Output fields are described here:

output definitions

IPMS State	The current state of IPMS on this switch, which can be **Enabled** or **Disabled** (the default). You can enable and disable IPMS with the **ip multicast switching** command, which is described on page 40-2.
Hardware Routing	Displays if hardware routing is **Enabled** or **Disabled** (the default). You can enable and disable hardware routing with the **ip multicast hardware-routing** command, which is described on page 40-19.

output definitions (continued)

Priority	Displays the IP multicast priority on all IPMS data queues used in the switch, which can be **urgent**, **high** (the default), **medium**, or **low**. You can modify this parameter with the **ip multicast priority** command, which is described on page 40-11.
Max Ingress Bandwidth	Displays the maximum incoming bandwidth (in megabits) on all IPMS data queues used in the switch. (The default is 10 megabits.) You can modify this parameter with the **ip multicast max-ingress-bandwidth** command, which is described on page 40-12.
Leave Timeout	Displays the delay in removing a group membership after a leave message has been received and/or processed. (The default is 1 second.) You can modify this parameter with the **ip multicast leave-timeout** command, which is described on page 40-4.
Flow Timeout	Displays the time (in seconds) a multicast flow entry is retained by a switch after the last packet in the flow is processed. (The default is 120 seconds for OmniSwitch 7700/7800/8800 and 64800 seconds for OmniSwitch 6600). You can modify this parameter with **ip multicast flow-timeout**, which is described on page 40-10.
Membership Timeout	Displays the time (in seconds) the switch will wait for an IGMP report before it drops a member from a multicast group. (The default is 260 seconds.) You can modify this parameter with the **ip multicast membership-timeout** command, which is described on page 40-6.
Neighbor Timeout	Displays the time (in seconds) the switch will wait for a neighbor probe from a router before it removes the corresponding entry for the router from the neighbor table. (The default is 90 seconds.) You can modify this parameter with the **ip multicast neighbor-timeout** command, which is described on page 40-7.
Querier Timeout	Displays the time (in seconds) the switch will wait for an IGMP query from a device before it removes the corresponding entry for the device from the querier table. (The default is 260 seconds.) You can modify this parameter with the **ip multicast querier-timeout** command, which is described on page 40-8.
Other Querier Timeout	Displays the timeout for which a currently elected querier is aged and a new multicast querier is elected.You can modify this parameter with the **ip multicast other-querier-timeout** command, which is described on page 40-8.
Query Interval	Displays the time (in seconds) between IGMP queries. (The default is 125 seconds.) You can modify this parameter with the **ip multicast query-interval** command, which is described on page 40-5.
Default Proxy Version	Displays the default IGMP proxy version, which can be **IGMPv2** (the default) or **IGMPv3**. Use the **ip multicast igmp-proxy-version** command to modify this parameter. (This field is not relevant for OmniSwitch 6600 Family switches.)

Release History

Release 5.1; command was introduced.

Related Commands

ip multicast switching	Enables or disables IPMS on a switch.
ip multicast leave-timeout	Configures the delay in removing a group membership after a leave message has been received and/or processed.
ip multicast query-interval	Configures the time between IGMP queries.
ip multicast membership-timeout	Configures the time the switch will wait for an IGMP report before it drops a member from a multicast group.
ip multicast neighbor-timeout	Configures the time the switch will wait for a neighbor probe from a router before it removes the corresponding entry for the router from the neighbor table.
ip multicast querier-timeout	Configures the time the switch will wait for an IGMP query from a device before it removes the corresponding entry for the device from the querier table.
ip multicast other-querier-timeout	Configures the timeout for which a currently elected querier is aged and a new multicast querier is elected.
ip multicast flow-timeout	Configures the time in seconds a flow entry is retained by the switch after the last packet in the flow is processed.
ip multicast priority	Configures the IP multicast priority to the value you specify on all IPMS data queues used in the switch.
ip multicast max-ingress-bandwidth	Configures the maximum incoming bandwidth on all IPMS data queues used in the switch.
ip multicast hardware-routing	Enables or disables IP multicast hardware routing.
ip multicast igmp-proxy-version	Configures the default version of IGMP membership.

MIB Objects

```
alaIpmsConfig
   alaIpmsStatus
   alaIpmsHardwareRoute
   alaIpmsPriority
   alaIpmsMaxBandwidth
   alaIpmsLeaveTimeout
   alaIpmsFlowTimer
   alaIpmsMembershipTimer
   alaIpmsNeighborTimer
   alaIpmsQuerierTimer
   alaIpmsOtherQuerierTimer
   alaIpmsQueryInterval
   alaIpmsIGMPMembershipProxyVersion
```

show ip multicast groups

Displays all detected multicast groups that have members.

show ip multicast groups [*ip_address***]**

Syntax Definitions

ip_address	The IP address of the multicast group to be displayed. If you do not specify any multicast groups, all multicast groups will be displayed.

Defaults

parameter	default
ip_address	0.0.0.0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show ip multicast groups
                                  Source IP         Slot/
Destination IP     Client IP     (IGMPv3 only)  VLAN Port  Expire  Type
---------------+---------------+---------------+----+-----+------+-------
224.0.0.9            11.0.0.1   224.0.0.9      3    3/10  186    Dynamic
225.10.10.10         10.0.0.1                  2     3/9  254    Dynamic

-> show ip multicast groups 225.10.10.10
                                  Source IP         Slot/
Destination IP     Client IP     (IGMPv3 only)  VLAN Port  Expire  Type
---------------+---------------+---------------+----+-----+------+-------
225.10.10.10         10.0.0.1                  2     3/9  254    Dynamic
```

Output fields are described here:

output definitions

Destination IP	The IP address of the multicast group.
Client IP	The IP address of the device that is receiving the multicast stream.
Source IP (IGMPv3)	The IP address of the IGMPv3 requested source. This field will be blank if the IGMP membership version is IGMPv2 and not IGMPv3. (This field is not relevant for OmniSwitch 6600 Family switches.)
VLAN	The VLAN associated with the multicast member.
Slot/Port	The slot and port number for the multicast member.

output definitions (continued)

Expire	The number of seconds before this multicast member times out.
Type	This field indicates whether the multicast group was learned by configuration (**Static**) or by observation of multicast router traffic (**Dynamic**).

Release History

Release 5.1; command was introduced.
5.1.6 and 5.3.1; **Type** column added.

Related Commands

ip multicast leave-timeout	Configures the delay in removing a group membership after a leave message has been received and/or processed.
ip multicast query-interval	Configures the time between IGMP queries.
ip multicast membership-timeout	Configures the time the switch will wait for an IGMP report before it drops a member from a multicast group.
ip multicast igmp-proxy-version	Configures the default version of IGMP membership.

MIB Objects

```
alaIpmsGroupTable
   alaIpmsGroupDestIpAddr
   alaIpmsGroupClientIpAddr
   alaIpmsGroupClientMacAddr
   alaIpmsGroupClientVlan
   alaIpmsGroupClientIfIndex
   alaIpmsGroupIGMPVersion
   alaIpmsGroupIGMPv3SrcIP
   alaIpmsGroupIGMPv3SrcType
   alaIpmsGroupIGMPv3SrcTimeout
   alaIpmsGroupIGMPv3GroupType
   alaIpmsGroupTimeout
```

show ip multicast neighbors

Displays all neighboring multicast routers.

show ip multicast neighbors

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A.

Examples

```
-> show ip multicast neighbors
      Source IP     VLAN Slot/Port Expire  Type  Version
--------------------+----+---------+------+-------+-------
None                  2       3/1 Never  Static  IGMPv2
10.0.0.253            1       3/2    88  Dynamic IGMPv2
11.0.0.253            1       3/2    89  Dynamic IGMPv2
```

Output fields are described here:

output definitions

Source IP	The IP address of the multicast router neighbor.
VLAN	The VLAN associated with the multicast router neighbor.
Slot/Port	The slot and port number of the multicast router neighbor.
Expire	The number of seconds before this multicast router neighbor times out.
Type	This field indicates whether the multicast router neighbor was learned by configuration (**Static**) or by observation of multicast router traffic (**Dynamic**).
Version	The default IGMP proxy version, which can be **IGMPv2** (the default) or **IGMPv3**. (This field is not relevant for OmniSwitch 6600 Family switches.)

Release History

Release 5.1; command was introduced.

Related Commands

ip multicast neighbor-timeout	Configures the time the switch will wait for a neighbor probe from a router.
ip multicast static-neighbor	Configures a port as a multicast routing neighbor.

MIB Objects

```
alaIpmsNeighbor
   alaIpmsNeighborIpAddr
   alaIpmsNeighborVlan
   alaIpmsNeighborIfIndex
   alaIpmsNeighborType
   alaIpmsNeighborTimeout
alaIpmsStaticNeighborTable
   alaIpmsStaticNeighborIGMPVersion
```

show ip multicast queriers

Displays all the multicast queriers.

show ip multicast queriers

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show ip multicast queries
      Source IP     VLAN Slot/Port Expire  Type   Version
--------------------+----+---------+------+-------+--------
None                   2       3/1 Never  Static   IGMPv2
10.0.0.253             1       3/2   146  Dynamic  IGMPv2
11.0.0.253             1       3/2   147  Dynamic  IGMPv2
```

Output fields are described here:

output definitions

Source IP	The IP address for the multicast querier.
VLAN	The VLAN associated with the multicast querier.
Slot/Port	The slot and port number for the multicast querier.
Expire	The number of seconds before this multicast querier out.
Type	This field indicates whether the multicast querier was learned by configuration (**Static**) or by observation of multicast router traffic (**Dynamic**).
Version	The default IGMP proxy version, which can be **IGMPv2** (the default) or **IGMPv3**. (This field is not relevant for OmniSwitch 6600 Family switches.)

Release History

Release 5.1; command was introduced.

Related Commands

ip multicast querier-timeout	Configures the time the switch will wait for an IGMP query from a device.
ip multicast static-querier	Configures a port as having a multicast querier on it.

MIB Objects

```
alaIpmsQuerierTable
   alaIpmsQuerierIpAddr
   alaIpmsQuerierVlan
   alaIpmsQuerierIfIndex
   alaIpmsQuerierType
   alaIpmsQuerierTimeout
alaIpmsStaticQuerierTable
   alaIpmsStaticQuerierIGMPVersion
```

show ip multicast forwarding

Displays the IPMS multicast forwarding table.

show ip multicast forwarding [*ip_address***]**

Syntax Definitions

ip_address	The IP address of the multicast group to be displayed. If you do not specify any multicast groups then the forwarding table for all multicast groups will be displayed.

Defaults

parameter	default
ip_address	0.0.0.0

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

No multicast group is specified:

```
-> show ip multicast forwarding
                                    Source              Destination
  Multicast Group       Source IP   Type VLAN Slot/PortType VLAN Slot/Port
------------------+------------------+----+----+---------+----+----+---------
      224.2.190.33      211.200.1.102 NATV    3     1/13 NATV    2      1/5
      224.2.190.33      211.200.1.102 NATV    3     1/13 NATV    4     1/11
      224.2.246.33      141.100.1.100 NATV    4     1/11 NATV    2      1/5
      224.2.246.33      141.100.1.100 NATV    4     1/11 NATV    3     1/13
      224.2.246.33      211.200.1.102 NATV    3     1/13 NATV    2      1/5
      224.2.246.33      211.200.1.102 NATV    3     1/13 NATV    4     1/11
```

A single multicast group is specified:

```
-> show ip multicast forwarding 224.2.190.33
                                    Source              Destination
  Multicast Group       Source IP   Type VLAN Slot/PortType VLAN Slot/Port
------------------+------------------+----+----+---------+----+----+---------
      224.2.190.33      211.200.1.102 NATV    3     1/13 NATV    2      1/5
      224.2.190.33      211.200.1.102 NATV    3     1/13 NATV    4     1/11
```

Output fields are described here:

output definitions

Multicast Group	The IP address of the multicast group (also known as the "destination IP" address).
Source IP	The IP address of the device that is generating the multicast stream. On OmniSwitch 6600 Family switches this filed will always display **N/A**.
Source Type	The type of flow for the source device, which can be **NATV** (native), **IPIP** (tunneled), or **RPTN** (routed).
Source VLAN	The source device's VLAN associated with the multicast member.
Source Slot/Port	The source device's slot and port number for the multicast member. On OmniSwitch 6600 Family switches this field will always display **N/A**.
Destination Type	The type of flow for the destination device, which can be **NATV** (native), **IPIP** (tunneled), or **RPTN** (routed).
Destination VLAN	The destination device's VLAN associated with the multicast member.
Destination Slot/Port	The destination device's slot and port number for the multicast member.

Release History

Release 5.1; command was introduced.

Related Commands

ip multicast max-ingress-bandwidth	Sets the maximum incoming bandwidth for all IP multicast traffic forwarded in the switch.
show ip multicast groups	Displays the status and configuration of IPMS groups on this switch.
show ip multicast queriers	Displays the active policies being enforced in the IPMS policy cache.

MIB Objects

```
alaIpmsSourceTable
   alaIpmsForwardDestIpAddr
   alaIpmsForwardSrcIpAddr
   alaIpmsForwardDestVlan
   alaIpmsForwardSrcVlan
   alaIpmsForwardSrcIfIndex
   alaIpmsForwardUniIpAddr
   alaIpmsForwardDestType
   alaIpmsForwardSrcType
   alaIpmsForwardDestIfIndex
   alaIpmsForwardDestTunIpAddr
```

show ip multicast policy-cache

Displays the active policies being enforced in the IPMS policy cache.

show ip multicast policy-cache

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show ip policy-cache
Policy  Group Address    Src Address      Vlan   Port   Disp   Time
-------+----------------+----------------+------+------+------+------
MBR     224.0.0.9        11.0.0.1         3      3/10   ACPT   139
MBR     225.10.10.10     10.0.0.1         2      3/9    ACPT   137
```

Output fields are described here:

output definitions

Policy	This field displays the type of multicast policy. In the current release, it is only possible to create group membership policies (**MBR**).
Group Address	The IP address for the multicast group (also known as the “destination IP” address).
Src Address	The IP address of the device requesting group membership.
Vlan	The VLAN associated with the multicast member.
Port	The port instance for this multicast group.
Disp	The field displays if the switch will forward (**ACPT**) or not forward (**DROP**) traffic to the device.
Time	The number of seconds before this multicast member times out.

Release History

Release 5.1; command was introduced.

Related Commands

ip multicast priority	Sets the IP multicast priority to the value you specify on all IPMS data queues used in the switch.
show ip multicast groups	Displays the status and configuration of IPMS groups on this switch.
ip multicast priority	Sets the IP multicast priority to the value you specify on all IPMS data queues used in the switch.

MIB Objects

```
alaIpmsForwardTable
   alaIpmsPolicyDestIpAddr
   alaIpmsPolicySrcIpAddr
   alaIpmsPolicySrcVlan
   alaIpmsPolicySrcIfIndex
   alaIpmsPolicyUniIpAddr
   alaIpmsPolicySrcType
   alaIpmsPolicyPolicy
```

41 Server Load Balancing Commands

Server Load Balancing (SLB) allows clients to send requests to servers logically grouped together in clusters. Each cluster logically aggregates a set of servers running identical applications with access to the same content (e.g., web servers). Clients access clusters through the use of a Virtual IP (VIP) address.

Note. SLB is supported on OmniSwitch 7700, 7800, and 8800 switches but not on OmniSwitch 6600 Family switches.

MIB information for the SLB commands is as follows:

Filename AlcatellIND1Slb.mib
Module: ALCATEL-IND1-SLB-MIB

A summary of available commands is listed here:

Global SLB Commands	**ip slb admin** **show ip slb**
SLB Cluster Commands	**ip slb cluster** **ip slb cluster admin status** **ip slb cluster ping period** **ip slb cluster ping timeout** **ip slb cluster ping retries** **ip slb cluster distribution** **ip slb cluster sticky time** **ip slb cluster probe** **show ip slb clusters** **show ip slb cluster**

SLB Server Commands	**ip slb server ip cluster** **ip slb server ip cluster probe** **show ip slb cluster server** **show ip slb servers**
SLB Probe Commands	**ip slb probe** **ip slb probe timeout** **ip slb probe period** **ip slb probe port** **ip slb probe retries** **ip slb probe username** **ip slb probe password** **ip slb probe url** **ip slb probe status** **ip slb probe send** **ip slb probe expect** **show ip slb probes**

ip slb admin

Enables or disables Server Load Balancing (SLB) on a switch.

ip slb admin {enable | disable}

Syntax Definitions

enable	Enables Server Load Balancing on a switch.
disable	Disables Server Load Balancing on a switch.

Defaults

parameter	default
enable | disable	disabled

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

Server Load Balancing is enabled on an entire switch. You *cannot* enable it on a per port or per NI basis.

Examples

```
-> ip slb admin enable
-> ip slb admin disable
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip slb	Displays the status of Server Load Balancing on a switch.
ip slb cluster	Configures a Server Load Balancing cluster on a switch.
ip slb server ip cluster	Adds, deletes, or modifies parameters of physical servers in logical Server Load Balancing clusters.

MIB Objects

```
slbFeature
   slbAdminStatus
```

ip slb cluster

Configures or removes a Server Load Balancing (SLB) cluster on a switch.

ip slb cluster *name* **vip** *ip_address*

no ip slb cluster *name*

Syntax Definitions

name	The name of the Server Load Balancing (SLB) cluster. The name can consist of a maximum of 23 characters. Spaces must be enclosed within quotation marks (e.g., “mail server”).
ip_address	The Virtual IP (VIP) address for the Server Load Balancing cluster. This IP address must be in dotted decimal format.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- You enable Server Load Balancing with the **ip slb admin** command, which is described on page 41-3, before SLB clusters are activated. (However, you can configure clusters and add servers to cluster before enabling SLB on a switch.)
- A maximum of 15 (fifteen) Server Load Balancing clusters may be configured on an OmniSwitch 7700/7800/8800 switch.
- The VIP address of the SLB cluster *must* be an address in the same subnet as the servers.
- You use the **ip slb server ip cluster** command, which is described on page 41-17, to assign physical servers to a logical Server Load Balancing cluster.
- Use the **no** form of the command to delete a Server Load Balancing cluster.

Examples

```
-> ip slb cluster corporate_servers vip 1.2.3.4
-> ip slb cluster "mail servers" vip 1.2.3.6
-> no ip slb cluster hr_servers
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip slb clusters	Displays the status and configuration of all Server Load Balancing clusters on a switch.
show ip slb cluster	Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.
ip slb admin	Enables or disables Server Load Balancing on a switch.
ip slb server ip cluster	Adds, deletes, or modifies parameters of physical servers in logical Server Load Balancing clusters.

MIB Objects

```
slbClusterTable
   slbClusterVIP
   slbClusterRowStatus
```

ip slb cluster admin status

Administratively enables or disables a Server Load Balancing (SLB) cluster on a switch.

ip slb cluster *cluster_name* **admin status {enable | disable}**

Syntax Definitions

cluster_name	The name of the Server Load Balancing (SLB) cluster.
enable	Administratively enables a Server Load Balancing cluster on a switch.
disable	Administratively disables a Server Load Balancing cluster on a switch.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> ip slb cluster hr_servers admin status enable
-> ip slb cluster "mail servers" admin status disable
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip slb clusters	Displays the status and configuration of all Server Load Balancing clusters on a switch.
show ip slb cluster	Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.
ip slb server ip cluster	Adds, deletes, or modifies parameters of physical servers in logical Server Load Balancing clusters.

MIB Objects

```
slbClusterTable
   slbClusterAdminStatus
```

ip slb cluster ping period

Modifies the number of seconds to check the health of the servers in a Server Load Balancing cluster.

ip slb cluster *cluster_name* **ping period** *seconds*

Syntax Definitions

cluster_name	The name of the Server Load Balancing (SLB) cluster.
seconds	The number of seconds for the ping period. Specifying 0 (zero) will disable the ping. The valid range for the ping period is 0–600 seconds.

Defaults

parameter	default
seconds	60

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

If you do not set the ping period to 0, then ping period *must* be greater than or equal to the ping timeout value divided by 1000. The ping timeout value can be modified with the **ip slb cluster ping time-out** command, which is described on page 41-9.

Examples

```
-> ip slb cluster hr_servers ping period 120
-> ip slb cluster "mail servers" ping period 0
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip slb clusters	Displays the status and configuration of all Server Load Balancing clusters on a switch.
show ip slb cluster	Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.
ip slb cluster ping timeout	Modifies the ping timeout value.
ip slb cluster ping retries	Modifies the number of ping retries.

MIB Objects

```
slbClusterTable
   slbClusterPingPeriod
```

ip slb cluster ping timeout

Modifies the timeout value for the ping for a Server Load Balancing (SLB) cluster before it retries.

ip slb cluster *cluster_name* **ping timeout** *milliseconds*

Syntax Definitions

cluster_name	The name of the Server Load Balancing (SLB) cluster.
milliseconds	The number of milliseconds for the ping timeout. The valid range for the ping timeout value is 0 to 1000 times the ping period. For example, if the ping period is 10 seconds, then maximum value for the ping timeout is 10000.

Defaults

parameter	default
milliseconds	3000

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

The ping period can be modified with the **ip slb cluster ping period** command, which is described on page 41-7.

Examples

```
-> ip slb cluster "mail servers" ping timeout 1000
-> ip slb cluster hr_servers ping timeout 6000
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip slb clusters	Displays the status and configuration of all Server Load Balancing clusters on a switch.
show ip slb cluster	Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.
ip slb cluster ping period	Modifies the ping period value.
ip slb cluster ping retries	Modifies the number of ping retries.

MIB Objects

```
slbClusterTable
   slbClusterPingTimeout
```

ip slb cluster ping retries

Modifies the number of ping attempts for a Server Load Balancing (SLB) cluster.

ip slb cluster *cluster_name* **ping retries** *count*

Syntax Definitions

cluster_name	The name of the Server Load Balancing (SLB) cluster.
count	The number of ping retries. The valid range for the ping retry value is 0–255.

Defaults

parameter	default
count	3

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> ip slb cluster "mail servers" ping retries 5
-> ip slb cluster hr_servers ping retries 10
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip slb clusters	Displays the status and configuration of all Server Load Balancing clusters on a switch.
show ip slb cluster	Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.
ip slb cluster ping period	Modifies the ping period value.
ip slb cluster ping timeout	Modifies the ping timeout value.

MIB Objects

```
slbClusterTable
   slbClusterPingRetries
```

ip slb cluster distribution

Modifies the distribution algorithm for a Server Load Balancing (SLB) cluster. This algorithm is used to select the target server within an SLB cluster.

ip slb cluster *cluster_name* **distribution {round robin | server failover}**

Syntax Definitions

cluster_name	The name of the Server Load Balancing (SLB) cluster.
round robin	This algorithm loops on in-service servers, taking into account their respective administrative weight.
server failover	This algorithm selects the first in-service server (in the ordered list of servers) in a pool of servers.

Defaults

parameter	default
round robin | server failover	**round robin**

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> ip slb cluster "mail servers" distribution round robin
-> ip slb cluster hr_servers distribution server failover
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip slb clusters	Displays the status and configuration of all Server Load Balancing clusters on a switch.
show ip slb cluster	Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.
ip slb cluster sticky time	Modifies the maximum delay with no activity a client is kept attached to a physical server.

MIB Objects

```
slbClusterTable
   slbClusterRedirectAlgorithm
```

ip slb cluster sticky time

Modifies the maximum delay with no activity a client is kept attached to a physical server (i.e., "sticky time") for a Server Load Balancing (SLB) cluster.

ip slb cluster *cluster_name* **sticky time** *seconds*

Syntax Definitions

cluster_name	Specifies the name of the Server Load Balancing (SLB) cluster.
seconds	Specifies the number of seconds for idle connections. The valid range for idle connections is 0–86400. Setting this value to 0 means infinity (i.e., the client will always be attached to this server).

Defaults

parameter	default
seconds	1200

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

Although you can set the sticky time to any integer between 0 and 86400, in the current release actual values are determined by the aging period for the switch's Hardware Routing Engine (HRE). On the OmniSwitch 7700/7800/8800, aging for HRE entries is done every 30 seconds. Therefore, when you configure a sticky time it will always be rounded up to a multiple of 30 seconds. For example, configuring a sticky time of 1, 8, 15, 26, or 30 seconds will have the same result (i.e., it will be 30 seconds).

Examples

```
-> ip slb cluster "mail servers" sticky time 600
-> ip slb cluster hr_servers sticky time 3000
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip slb clusters	Displays the status and configuration of all Server Load Balancing clusters on a switch.
show ip slb cluster	Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.
ip slb cluster distribution	Modifies the distribution algorithm.

MIB Objects

```
slbClusterTable
   slbClusterIdleTimer
```

ip slb cluster probe

Configures a probe for a Server Load Balancing (SLB) cluster.

ip slb cluster *cluster_name* **probe** *probe_name*

Syntax Definitions

cluster_name	The name of the Server Load Balancing (SLB) cluster.
probe_name	The name of the Server Load Balancing (SLB) probe.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

You must create the probe with the **ip slb probe** before you can use this command.

Examples

```
-> ip slb cluster mail_servers probe mail_server_probe
```

Release History

Release 5.1.6; command was introduced.

Related Commands

show ip slb clusters	Displays the status and configuration of all Server Load Balancing clusters on a switch.
ip slb probe	Configures and deletes SLB probes.
show ip slb cluster	Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.
ip slb server ip cluster	Adds, deletes, or modifies parameters of physical servers in logical Server Load Balancing clusters.

MIB Objects

```
slbClusterTable
   slbClusterProbeName
```

ip slb server ip cluster

Adds a physical server to a Server Load Balancing (SLB) cluster, deletes a physical server from an SLB cluster, or modifies the administrative status and/or administrative weight of a physical server in an SLB cluster.

ip slb server ip *ip_address* **cluster** *cluster_name* **[admin status {enable | disable}] [weight** *admin_weight***]**

no ip slb server ip *ip_address* **cluster** *cluster_name*

Syntax Definitions

ip_address	The IP address for the physical server.
cluster_name	The name of the Server Load Balancing (SLB) cluster.
enable	Enables a server.
disable	Disables a server.
admin_weight	The administrative weight for this physical server. The valid range for the administrative weight is 0–100.

Defaults

The defaults for the **ip slb server ip cluster** command are shown below:

parameter	default
admin status	enable
weight	10

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- A maximum of 75 physical servers can be added to an OmniSwitch 7700/7800/8800 switch.
- Please note that administrative weights are relative. For example, say Servers A and B have respective weights of 10 and 20 within a cluster. In this example, Server A would get half the traffic of server B. Since administrative weights are relative, assigning Servers A and B respective weights of 1 and 2, 5 and 10, or 25 and 50, etc., would produce identical results.
- Assigning an administrative weight of 0 (zero) to a server will prevent this server from being assigned any new connections.
- Use the **no** form of the command to remove a physical server from a Server Load Balancing cluster.

Examples

```
-> ip slb server ip 10.255.11.127 cluster corporate_servers
-> ip slb server ip 10.255.11.109 cluster "mail servers" admin status disable
-> ip slb server ip 10.255.11.135 cluster hr_servers admin status enable weight 50
-> ip slb server ip 10.255.11.101 cluster "mail servers" weight 5
-> no ip slb server ip 10.255.11.105 cluster hr_servers
```

Release History

Release 5.1; command was introduced.

Related Commands

show ip slb clusters	Displays the status and configuration of all Server Load Balancing clusters on a switch.
show ip slb cluster	Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.
ip slb admin	Enables or disables Server Load Balancing on a switch.
ip slb cluster	Configures Server Load Balancing clusters.

MIB Objects

```
slbServerTable
   slbServerRowStatus
   slbServerAdminStatus
   slbServerAdminWeight
```

ip slb server ip cluster probe

Configures a probe for a Server Load Balancing (SLB) server.

ip slb server ip *ip_address* **cluster** *cluster_name* **probe** *probe_name*

Syntax Definitions

ip_address	The IP address for the physical server.
cluster_name	The name of the Server Load Balancing (SLB) cluster.
probe_name	The name of the Server Load Balancing (SLB) probe.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

You must create the probe with the **ip slb probe** before you can use this command.

Examples

```
-> ip slb server ip 10.255.11.127 cluster corporate_servers probe p_http
```

Release History

Release 5.1.6; command was introduced.

Related Commands

show ip slb clusters	Displays the status and configuration of all Server Load Balancing clusters on a switch.
show ip slb cluster	Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.
ip slb probe	Configures and deletes SLB probes.
ip slb admin	Enables or disables Server Load Balancing on a switch.
ip slb cluster	Configures Server Load Balancing clusters.

MIB Objects

```
slbServerTable
   slbServerProbeName
```

ip slb probe

Configures and deletes a Server Load Balancing (SLB) probe used to check the health of servers or clusters.

ip slb probe *probe_name* **{ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp}**

no ip slb probe *probe_name*

Syntax Definitions

probe_name	Specifies the name of the Server Load Balancing (SLB) probe.
ftp	Specifies an FTP probe.
http	Specifies an HTTP probe.
https	Specifies an HTTPS probe.
imap	Specifies an IMAP probe.
imaps	Specifies an IMAPS probe.
nntp	Specifies an NNTP probe.
ping	Specifies a ping probe.
pop	Specifies a POP probe.
pops	Specifies a POPS probe.
smtp	Specifies an SMTP probe.
tcp	Specifies a TCP probe.
udp	Specifies a UDP probe.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to delete an SLB probe.
- A maximum of 20 probes can be configured on a switch.

Examples

```
-> ip slb probe mail_server_probe smtp
-> no ip slb probe mail_server_probe
```

Release History

Release 5.1.6; command was introduced.

Related Commands

show ip slb probes	Display the configuration of SLB probes.

MIB Objects

```
slbProbeTable
   slbProbeName
   slbProbeMethod
```

ip slb probe timeout

Configures the timeout used to wait for Server Load Balancing (SLB) probe answers.

ip slb probe *probe_name* **{ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp} timeout** *seconds*

Syntax Definitions

probe_name	Specifies the name of the Server Load Balancing (SLB) probe.
ftp	Specifies an FTP probe.
http	Specifies an HTTP probe.
https	Specifies an HTTPS probe.
imap	Specifies an IMAP probe.
imaps	Specifies an IMAPS probe.
nntp	Specifies an NNTP probe.
ping	Specifies a ping probe.
pop	Specifies a POP probe.
pops	Specifies a POPS probe.
smtp	Specifies an SMTP probe.
tcp	Specifies a TCP probe.
udp	Specifies a UDP probe.
seconds	Specifies the timeout in seconds, which can be 0–3600000.

Defaults

parameter	default
seconds	3000

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> ip slb probe mail_server smtp timeout 12000
```

Release History

Release 5.1.6; command was introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
show ip slb probes	Display the configuration of SLB probes.

MIB Objects

```
slbProbeTable
   slbProbeName
   slbProbeMethod
   slbProbeTimeout
```

ip slb probe period

Configures the Server Load Balancing (SLB) probe period to check the health of servers.

ip slb probe *probe_name* **{ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp} period** *seconds*

Syntax Definitions

probe_name	Specifies the name of the Server Load Balancing (SLB) probe.
ftp	Specifies an FTP probe.
http	Specifies an HTTP probe.
https	Specifies an HTTPS probe.
imap	Specifies an IMAP probe.
imaps	Specifies an IMAPS probe.
nntp	Specifies an NNTP probe.
ping	Specifies a ping probe.
pop	Specifies a POP probe.
pops	Specifies a POPS probe.
smtp	Specifies an SMTP probe.
tcp	Specifies a TCP probe.
udp	Specifies a UDP probe.
seconds	Specifies the period in seconds, which can be 0–3600.

Defaults

parameter	default
seconds	60

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> ip slb probe web_server http period 120
```

Release History

Release 5.1.6; command was introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
show ip slb probes	Display the configuration of SLB probes.

MIB Objects

```
slbProbeTable
   slbProbeName
   slbProbeMethod
   slbProbePeriod
```

ip slb probe port

Configures the TCP/UDP port the Server Load Balancing (SLB) probe should be sent on.

ip slb probe *probe_name* **{ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp} port** *port_number*

Syntax Definitions

probe_name	Specifies the name of the Server Load Balancing (SLB) probe.
ftp	Specifies an FTP probe.
http	Specifies an HTTP probe.
https	Specifies an HTTPS probe.
imap	Specifies an IMAP probe.
imaps	Specifies an IMAPS probe.
nntp	Specifies an NNTP probe.
ping	Specifies a ping probe.
pop	Specifies a POP probe.
pops	Specifies a POPS probe.
smtp	Specifies an SMTP probe.
tcp	Specifies a TCP probe.
udp	Specifies a UDP probe.
port_number	Specifies the TDP/UDP port number, which can be 0–65535.

Defaults

parameter	default
port_number	0

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> ip slb probe mis_server udp port 200
```

Release History

Release 5.1.6; command was introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
show ip slb probes	Display the configuration of SLB probes.

MIB Objects

```
slbProbeTable
   slbProbeName
   slbProbeMethod
   slbProbePort
```

ip slb probe retries

Configures the number of Server Load Balancing (SLB) probe retries before deciding that a server is out of service.

ip slb probe *probe_name* **{ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp} retries** *retries*

Syntax Definitions

probe_name	Specifies the name of the Server Load Balancing (SLB) probe.
ftp	Specifies an FTP probe.
http	Specifies an HTTP probe.
https	Specifies an HTTPS probe.
imap	Specifies an IMAP probe.
imaps	Specifies an IMAPS probe.
nntp	Specifies an NNTP probe.
ping	Specifies a ping probe.
pop	Specifies a POP probe.
pops	Specifies a POPS probe.
smtp	Specifies an SMTP probe.
tcp	Specifies a TCP probe.
udp	Specifies a UDP probe.
retries	Specifies the number of retries, which can be 0–255.

Defaults

parameter	default
retries	3

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> ip slb probe mail_server smtp retries 5
```

Release History

Release 5.1.6; command was introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
show ip slb probes	Display the configuration of SLB probes.

MIB Objects

```
slbProbeTable
   slbProbeName
   slbProbeMethod
   slbProbeRetries
```

ip slb probe username

Configures a user name sent to a server as credentials for an HTTP GET operation to verify the health of the server.

ip slb probe *probe_name* **{http | https} username user_name**

Syntax Definitions

probe_name	Specifies the name of the Server Load Balancing (SLB) probe.
http	Specifies an HTTP probe.
https	Specifies an HTTPS probe.
user_name	Specifies user name.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> ip slb probe web_server http username subnet1
```

Release History

Release 5.1.6; command was introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
show ip slb probes	Display the configuration of SLB probes.

MIB Objects

```
slbProbeTable
   slbProbeName
   slbProbeMethod
   slbProbeHttpUsername
```

ip slb probe password

Configures a password sent to a server as credentials for an HTTP GET to verify the health of the server.

ip slb probe *probe_name* **{http | https} password** *password*

Syntax Definitions

probe_name	Specifies the name of the Server Load Balancing (SLB) probe.
http	Specifies an HTTP probe.
https	Specifies an HTTPS probe.
password	Specifies the password.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

The password is encrypted in the configuration file so it is not readable.

Examples

```
-> ip slb probe web_server http password h1f45xc
```

Release History

Release 5.1.6; command was introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
show ip slb probes	Display the configuration of SLB probes.

MIB Objects

```
slbProbeTable
   slbProbeName
   slbProbeMethod
   slbProbeHttpPassword
```

ip slb probe url

Configures a URL sent to a server for an HTTP GET to verify the health of the server.

ip slb probe *probe_name* **{http | https} url** *url*

Syntax Definitions

probe_name	Specifies the name of the Server Load Balancing (SLB) probe.
http	Specifies an HTTP probe.
https	Specifies an HTTPS probe.
url	Specifies the URL of the server.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
->ip slb probe web_server http url pub/index.html
```

Release History

Release 5.1.6; command was introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
show ip slb probes	Display the configuration of SLB probes.

MIB Objects

```
slbProbeTable
   slbProbeName
   slbProbeMethod
   slbProbeHttpUrl
```

ip slb probe status

Configures the expected status returned from an HTTP GET to verify the health of a server.

ip slb probe *probe_name* **{http | https} status** *status_value*

Syntax Definitions

probe_name	Specifies the name of the Server Load Balancing (SLB) probe.
http	Specifies an HTTP probe.
https	Specifies an HTTPS probe.
status_value	Specifies the expected status returned, which can be 0–4294967295.

Defaults

parameter	default
status_value	200

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> ip slb probe web_server http status 404
```

Release History

Release 5.1.6; command was introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
show ip slb probes	Display the configuration of SLB probes.

MIB Objects

```
slbProbeTable
   slbProbeName
   slbProbeMethod
   slbProbePeriod
   slbProbeHttpStatus
```

ip slb probe send

Configures an ASCII string sent to a server to invoke a response from it and to verify its health.

ip slb probe *probe_name* **{http | https | tcp | udp} send** *send_string*

Syntax Definitions

probe_name	Specifies the name of the Server Load Balancing (SLB) probe.
http	Specifies an HTTP probe.
https	Specifies an HTTPS probe.
tcp	Specifies a TCP probe.
udp	Specifies a UDP probe.
send_string	Specifies the ASCII string sent to a server to invoke a response.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> ip slb probe web_server http send test
```

Release History

Release 5.1.6; command was introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
show ip slb probes	Display the configuration of SLB probes.

MIB Objects

```
slbProbeTable
   slbProbeName
   slbProbeMethod
   slbProbeSend
```

ip slb probe expect

Configures an ASCII string used to compare a response from a server to verify the health of the server.

ip slb probe *probe_name* **{http | https | tcp | udp} expect** *expect_string*

Syntax Definitions

probe_name	Specifies the name of the Server Load Balancing (SLB) probe.
http	Specifies an HTTP probe.
https	Specifies an HTTPS probe.
tcp	Specifies a TCP probe.
udp	Specifies a UDP probe.
expect_name	Specifies the ASCII string used to compare a response from a server.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> ip slb probe web_server http expect test
```

Release History

Release 5.1.6; command was introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
show ip slb probes	Display the configuration of SLB probes.

MIB Objects

```
slbProbeTable
   slbProbeName
   slbProbeMethod
   slbProbeExpect
```

show ip slb

Displays the status of Server Load Balancing on a switch.

show ip slb

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show ip slb
Admin status                    : Enabled,
Operational status              : In Service,
Number of clusters              = 3
```

Output fields are described here:

output definitions

Admin status	The current administrative status of Server Load Balancing (SLB) on this switch. This field will display **Enabled** if SLB is enabled on this switch or **Disabled** if it is disabled.
Operational status	The current operational status of Server Load Balancing (SLB) on this switch, which will be **In service** (at least one SLB cluster is in service) or **Out of service** (all SLB clusters are out of service).
Number of clusters	The total number of Server Load Balancing (SLB) clusters on this switch. A maximum of 15 SLB clusters can added to an OmniSwitch 7700/7800/8800 switch.

Release History

Release 5.1; command was introduced.

Related Commands

show ip slb servers	Displays the status of all physical servers belonging to Server Load Balancing clusters on a switch.
show ip slb clusters	Displays the status and configuration of all Server Load Balancing clusters on a switch.
show ip slb cluster	Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.
show ip slb cluster server	Displays detailed status and configuration information for a single physical server in a Server Load Balancing cluster.

MIB Objects

```
slbFeature
   slbAdminStatus
   slbOperStatus
   slbClustersCount
```

show ip slb clusters

Display the status and basic configuration for all Server Load Balancing (SLB) clusters on a switch.

show ip slb clusters

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show ip slb clusters
                                Admin    Operational         #     %
Cluster Name     VIP            Status   Status              Srv   Avail
-----------------+---------------+--------+-------------------+-----+---------
WorldWideWeb     128.241.130.204  Enabled  In Service          3     95
Intranet         128.241.130.205  Enabled  In Service          2     100
FileTransfer     128.241.130.206  Enabled  Out of Service      2     50
```

Output fields are described here:

output definitions

Cluster Name	The name of this Server Load Balancing (SLB) cluster.
VIP	The virtual IP (VIP) address for this Server Load Balancing (SLB) cluster.
Admin Status	The current administrative status of this Server Load Balancing (SLB) cluster, which can be **Enabled** or **Disabled**.
Operational Status	The current operational status of this Server Load Balancing (SLB) cluster, which can be **In Service** (i.e., at least one physical server is operational in the cluster) or **Out of Service**.
# Srv	The total number of physical servers that belong to this Server Load Balancing (SLB) cluster. A maximum of 75 physical servers can added to an OmniSwitch 7700/7800/8800 switch.
% Avail	The percentage of flows successfully routed to this SLB cluster.

Release History

Release 5.1; command was introduced.

Related Commands

show ip slb servers	Displays the status of all physical servers belonging to Server Load Balancing clusters on a switch.
show ip slb cluster	Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.
show ip slb cluster server	Displays detailed status and configuration information for a single physical server in a Server Load Balancing cluster.

MIB Objects

```
slbClusterTable
   slbClusterName
   slbClusterVIP
   slbClusterAdminStatus
   slbClusterOperStatus
   slbClusterNumberOfServers
   slbClusterNewFlows
```

show ip slb cluster

Displays detailed statistics and configuration information for a single Server Load Balancing (SLB) cluster.

show ip slb cluster *name*

Syntax Definitions

name	Specifies the name of the Server Load Balancing (SLB) cluster.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show ip slb cluster Intranet
Cluster Intranet
  VIP                           : 128.241.130.205,
  Admin status                  : Enabled,
  Operational status            : In Service,
  Routed flows success ratio (%) = 100,
  Ping period (seconds)         = 60,
  Ping timeout (milliseconds)   = 3000,
  Ping retries                  = 3,
  Redirect algorithm            : round robin,
  Sticky time (seconds)         = 600,
  Probe                         = None,
  Number of flows               = 45768,
  Number of servers             = 2
    Server 128.241.130.4
      Admin status = Enabled, Operational Status = In Service,
      Weight = 10, Number of flows = 2000, Availability (%) = 98
    Server 128.241.130.5
      Admin status = Enabled, Operational Status = Discovery,
      Weight = 10, Number of flows = 0, Availability (%) = 0
```

Output fields are described here:

output definitions

Cluster	The name of this Server Load Balancing (SLB) cluster.
VIP	The virtual IP (VIP) address for this Server Load Balancing (SLB) cluster.

output definitions (continued)

Admin status	The current administrative status of this Server Load Balancing (SLB) cluster, which can be **Enabled** or **Disabled**.
Operational status	The current operational status of this Server Load Balancing (SLB) cluster, which can be **In Service** (i.e., at least one physical server is operational in the cluster) or **Out of Service**.
Routed flows success ratio (%)	The percentage of flows successfully routed to this Server Load Balancing (SLB) cluster.
Ping period (seconds)	The ping period (in seconds) used by this Server Load Balancing (SLB) cluster to check the health of physical servers.
Ping timeout (milliseconds)	The timeout (in milliseconds) used by this Server Load Balancing (SLB) cluster to wait for ping answers from physical servers.
Ping retries	The number of ping retries that this Server Load Balancing (SLB) cluster will execute before switching the status to **No answer**.
Redirect algorithm	The load balancing algorithm, which can be **round robin** (the default where SLB delivers connections evenly among the physical servers) or **server failover** (where SLB gives new connections only if previous connections to the server have failed), used by this Server Load Balancing (SLB) cluster.
Sticky time (seconds)	The maximum delay (in seconds) with no activity a client is kept attached to a physical server.
Probe	The probe configured for this cluster.
Number of flows	The number of flows balanced for this Server Load Balancing (SLB) cluster.
Number of servers	The total number of physical servers that belong to this Server Load Balancing (SLB) cluster.
Server	The IP address for this physical server.
Admin Status	The administrative state of this physical server, which can be **Enabled** or **Disabled**.
Operational Status	The operational state of this server, which can be **Disabled** (this server has been administratively disabled), **No Answer** (this server has not responded to ping requests), **Link Down** (there is a bad connection to this server), **In Service** (this server is being used for SLB cluster client connections), **Discovery** (the SLB cluster is pinging this physical server), or **Retrying** (the SLB cluster is making another attempt to bring up the server).
Weight	The administrative weight of this real server used by the Server Load Balancing (SLB) algorithms. A weight of 0 (zero) indicates that no new connections will be assigned to this server. Higher weight values indicate that this server can accept more work.
Number of flows	The number of flows balanced by this physical server.
Availability (%)	The percentage of time that this physical server has been available for processing client requests. In other word, the actual ratio of up time (**In Service** plus **Retrying**) versus down time (**No Answer** plus **Link Down**). Please note that the **Disabled** and the initial **Discovery** states are not counted as down time.

Release History

Release 5.1; command was introduced.
Release 5.1.6: **Probe** field added.

Related Commands

show ip slb servers	Displays the status of all physical servers belonging to Server Load Balancing clusters on a switch.
show ip slb clusters	Displays detailed status and configuration information for all Server Load Balancing clusters on a switch.
show ip slb cluster server	Displays detailed status and configuration information for a single physical server in a Server Load Balancing cluster.
ip slb cluster probe	Configures a probe for an SLB cluster.

MIB Objects

```
slbClusterTable
   slbClusterName
   slbClusterVIP
   slbClusterAdminStatus
   slbClusterOperStatus
   slbClusterUpTime
   slbClusterPingPeriod
   slbClusterPingTimeout
   slbClusterPingRetries
   slbClusterRedirectAlgorithm
   slbClusterIdleTimer
   slbClusterNumberOfServers
   slbClusterProbeName
   slbClusterNewFlows
   slbClusterRowStatus
slbServerTable
   slbServerClusterName
   slbServerIpAddress
   slbServerAdminStatus
   slbServerOperStatus
   slbServerAdminWeight
```

show ip slb cluster server

Displays detailed statistics and configuration information for a single physical server in a Server Load Balancing (SLB) cluster.

show ip slb cluster *name* **server** *ip_address*

Syntax Definitions

name	Specifies the name of the Server Load Balancing (SLB) cluster.
ip_address	Specifies the IP address for the physical server.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show ip slb cluster Intranet server 128.220.40.4
Cluster cl1
  VIP 128.220.40.205
    Server 128.220.40.4
      Admin weight                            = 10,
      MAC addr                                : 00:00:1f:40:53:6a,
      Slot number                             = 1,
      Port number                             = 4,
      Admin status                            : Enabled,
      Oper status                             : In Service,
      Probe                                   = phhtp,
      Availability time (%)                   = 95,
      Ping failures                           = 0,
      Last ping round trip time (milliseconds) = 20,
      Link down count                         = 1,
      Number of flows                         = 200,
      Probe status                            = ,
```

Output fields are described here:

output definitions

Cluster	The name of the Server Load Balancing (SLB) cluster.
VIP	The virtual IP (VIP) address for this Server Load Balancing (SLB) cluster.
Server	The IP address for this physical server.
Admin weight	The administrative weight of this physical server used by the Server Load Balancing (SLB) algorithms. A weight of 0 (zero) indicates that no new connections will be assigned to this server. Higher weight values indicate that this server can accept more work.
MAC addr	The MAC address of this physical server.
Slot number	The slot number of the network interface (NI) board that this physical server is attached to.
Port number	The port number that this physical server is attached to.
Admin status	The current administrative status of this physical server, which can be **Enabled** or **Disabled**.
Oper status	The operational state of this server, which can be **Disabled** (this server has been administratively disabled), **No Answer** (this server has not responded to ping requests), **Link Down** (there is a bad connection to this server), **In Service** (this server being used for SLB cluster client connections), **Discovery** (the SLB cluster is pinging this physical server), or **Retrying** (the SLB cluster is making another attempt to bring up the server).
Probe	The name of the probe configured for this server.
Availability time (%)	The percentage of time that this physical server has been available for processing client requests. In other word, the actual ratio of up time (**In Service** plus **Retrying**) versus down time (**No Answer** plus **Link Down**). Please note that the **Disabled** and the initial **Discovery** states are not counted as down time.
Ping failures	The total number of pings that have failed on this physical server.
Last ping round trip time (milliseconds)	The total amount of time (in milliseconds) measured for the last valid ping to this physical server to make a round trip.
Link down count	The total number of times that the link from the switch to this physical server has been down.
Number of flows	The total number of data flows directed to this physical server.
Probe status	The status of the probe configured for this server.

Release History

Release 5.1; command was introduced.
Release 5.1.6; **Probe** and **Probe** status fields were added.

Related Commands

show ip slb servers	Displays the status of all physical servers belonging to Server Load Balancing clusters on a switch.
show ip slb clusters	Displays detailed status and configuration information for all Server Load Balancing clusters on a switch.
show ip slb cluster	Displays detailed status and configuration information for a single Server Load Balancing cluster.

MIB Objects

```
slbClusterTable
   slbClusterVIP
slbServerTable
   slbServerClusterName
   slbServerIpAddress
   slbServerAdminStatus
   slbServerOperStatus
   slbServerAdminWeight
   slbServerMacAddress
   slbServerSlotNumber
   slbServerPortNumber
   slbServerUpTime
   slbServerProbeName
   slbServerLastRTT
   slbServerPingFails
   slbServerPortDown
   slbServerFlows
   slbServerProbeStatus
```

show ip slb servers

Displays the status and configurations of all physical servers in Server Load Balancing clusters.

show ip slb servers

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> show ip slb servers
                                    Admin     Operational     %
IP addr              Cluster Name   Status    Status          Avail
---------------------+--------------+---------+---------------+-----------
128.220.40.4         Intranet       Enabled   In Service      98
128.220.40.5         Intranet       Enabled   Retrying        80
128.220.40.6         FileTransfer   Enabled   No answer       50
128.220.40.7         FileTransfer   Disabled  Disabled        ---
128.220.40.1         WorldWideWeb   Enabled   In Service      100
128.220.40.2         WorldWideWeb   Enabled   Discovery       50
128.220.40.3         WorldWideWeb   Enabled   Link Down       75
```

Output fields are described here:

output definitions

IP addr	The IP address for this physical server.
Cluster Name	The name of the Server Load Balancing (SLB) cluster that this physical server belongs to.
Admin Status	The current administrative status of this physical server, which can be **Enabled** or **Disabled**.

output definitions (continued)

Operational Status	The operational state of this server, which can be **Disabled** (this server has been administratively disabled), **No Answer** (this server has not responded to ping requests), **Link Down** (there is a bad connection to this server), **In Service** (this server being used for SLB cluster client connections), **Discovery** (the SLB cluster is pinging this physical server), or **Retrying** (the SLB cluster is making another attempt to bring up the server).
% Avail	The percentage of time that this physical server has been available for processing client requests. In other word, the actual ratio of up time (**In Service** plus **Retrying**) versus down time (**No Answer** plus **Link Down**). Please note that the **Disabled** and the initial **Discovery** states are not counted as down time.

Release History

Release 5.1; command was introduced.

Related Commands

show ip slb cluster server	Displays the detailed status and configuration of a single physical server in a Server Load Balancing cluster.
show ip slb clusters	Displays detailed status and configuration information for all Server Load Balancing clusters on a switch.
show ip slb cluster	Displays detailed status and configuration information for a single Server Load Balancing cluster.

MIB Objects

```
slbServers
   slbServerIpAddress
   slbServerClusterName
   slbServerAdminStatus
   slbServerOperStatus
   slbServerFlows
```

show ip slb probes

Display the configuration of Server Load Balancing (SLB) probes.

show ip slb probes *probe_name*

Syntax Definitions

probe_name	Specifies the name of the Server Load Balancing (SLB) probe.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

If you do not specify the name of an SLB probe then all SLB probes will be displayed.

Examples

No probe name is specified:

```
-> show ip slb probes
Probe Name              Period  Retries Timeout Method
----------------------+-------+-------+--------+------
web_server                60000       3   12000   HTTP
mail_server               60000       3    3000   SMTP
mis_servers             3600000       5   24000   Ping
```

Output fields are described here:

output definitions

Probe Name	The user-specified name of the probe.
Period	The period (in seconds) to check the health of servers.
Retries	The number of probe retries before deciding that a server is out of service.
Timeout	The timeout (in seconds) used to wait for probe answers.
Method	The type of probe.

A non HTTP/HTTPS probe name is specified:

```
-> show ip slb probes mail_server
Probe mail_server
  Type                          = SMTP,
  Period (seconds)              = 60,
  Timeout (milliseconds)        = 3000,
  Retries                       = 3,
  Port                          = 0,
```

An HTTP/HTTPS probe name is specified:

```
-> show ip slb probes phttp
Probe phttp
  Type                          = HTTP,
  Period (seconds)              = 60,
  Timeout (milliseconds)        = 3000,
  Retries                       = 3,
  Port                          = 0,
  Username                      = ,
  Password                      = ,
  Expect                        = ,
  Status                        = 200,
  URL                           = /,
```

Output fields are described here:

output definitions

Probe	The user-specified name of the probe.
Type	The type of probe.
Period	The period (in seconds) to check the health of servers.
Timeout	The timeout (in seconds) used to wait for probe answers.
Retries	The number of probe retries before deciding that a server is out of service.
Port	The TCP/UDP port that the probe is sent on.
Username	The configured user name sent to a server as credentials for an HTTP GET operation for the probe.
Password	The configured password for the probe.
Expect	The configured ASCII string used to compare a response from a server to verify the health of the server.
Status	The expected status returned from an HTTP GET to verify the health of a server.
URL	The configured URL sent to a server for an HTTP GET to verify the health of the server.

Release History

Release 5.1.6; command was introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
ip slb probe period	Configures the probe period to check the health of servers.
ip slb probe timeout	Configures the timeout used to wait for probe answers.
ip slb probe retries	Configures the number of probe retries before deciding that a server is out of service.
ip slb probe port	Configures the TCP/UDP port that the probe should be sent on.
ip slb probe username	Configures a user name sent to a server as credentials for an HTTP GET operation
ip slb probe password	Configures a password sent to a server as credentials for an HTTP GET to verify the health of the server
ip slb probe expect	Configures an ASCII string used to compare a response from a server to verify the health of the server.
ip slb probe status	Configures the expected status returned from an HTTP GET to verify the health of a server.
ip slb probe url	Configures a URL sent to a server for an HTTP GET to verify the health of the server.

MIB Objects

```
slbProbeTable
   slbProbeName
   slbProbeMethod
   slbProbePeriod
   slbProbeTimeout
   slbProbeRetries
   slbProbePort
   slbProbeHttpUsername
   slbProbeHttpPassword
   slbProbeExpect
   slbProbeHttpStatus
   slbProbeHttpUrl
```

42 High Availability VLAN Commands

High availability (HA) VLANs, unlike standard VLANs, allow you to send traffic intended for a single destination address to multiple switch ports.

MIB information is as follows:

Filename: AlcatelIND1VlanManager.mib
Module: ALCATEL-IND1-VLAN-MGR-MIB

Filename: AlcatelIND1MacAddress.mib
Module: ALCATEL-IND1-MAC-ADDRESS-MIB

A summary of the available commands is listed here:

vlan port-mac ingress-port
vlan port-mac egress-port
mac-address-table port-mac vlan mac
vlan port-mac bandwidth
show mac-address-table port-mac

Note. High availability VLAN commands are not compatible with other VLAN commands (i.e., commands with the **vlan** prefix) except for the **no** form of the **vlan** command. In addition, high availability VLANs are supported on OmniSwitch 7700, 7800, and 8800 switches, but not OmniSwitch 6600 Family switches.

vlan port-mac ingress-port

Adds and removes ingress ports from a high availability (HA) VLAN.

vlan *vid* **port-mac ingress-port** *slot1/port1***[-***port1a***] [***slot2/port2***[-***port2a***]...]**

vlan *vid* **port-mac no ingress-port** *slot1/port1***[-***port1a***] [***slot2/port2***[-***port2a***]...]**

Syntax Definitions

vid	An existing VLAN ID number (1–4094).
*slot1/port1***[-***port1a***]**	The ingress slot and port combination to be included in this HA VLAN. You may enter multiple ports and port ranges.
*slot2/port2***[-***port2a***]**	Additional ingress slot and port combinations may be included with this HA VLAN. You may enter multiple ports and port ranges.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the **vlan port-mac ingress-port** command to remove one or more ingress ports from an HA VLAN.
- Note that removing the last ingress/egress port from an HA VLAN is not allowed. Deleting the VLAN is required when there is only one ingress/egress port left in the VLAN.
- This command only applies to fixed ports on second-generation Network Interface (NI) modules. Mobile ports, 802.1Q tagged ports, link aggregate ports, Learned Port Security (LPS) ports, and ports that mirror or are mirrored are not eligible for transition to an ingress port state.
- It is not necessary to specify ports in any sequential order or only ports that reside on the same second-generation NI module.
- Using this command on a standard VLAN converts that VLAN into an HA VLAN.
- All HA VLAN related ports must first belong to the same default VLAN before they are configured as ingress, egress, or inter-switch ports for the HA VLAN.
- A port can be designated as both an ingress and egress port, these states are not mutually exclusive.
- If a packet received on an ingress port is not destined for the high availability VLAN MAC address, the packet is bridged as regular traffic to all ports in the VLAN, not just egress ports.

Examples

```
-> vlan 10 port-mac ingress-port 3/1
-> vlan 15 port-mac ingress-port 2/1 2/5 6/1
-> vlan 1200 port-mac ingress-port 3/1-5
-> vlan 1200 port-mac ingress-port 3/1-5 4/2 4/7 5/1-4
-> vlan 10 port-mac no ingress-port 3/1
-> vlan 15 port-mac no ingress-port 2/1 2/5 6/1
-> vlan 1200 port-mac no ingress-port 3/1-5
-> vlan 1200 port-mac no ingress-port 3/1-5 4/2 4/7 5/1-4
```

Release History

Release 5.1; command was introduced.

Related Commands

vlan	Creates and deletes VLANs.
vlan port-mac egress-port	Adds and deletes egress ports from an HA VLAN.
show mac-address-table port-mac	Displays the configuration and status of HA VLANs on a switch.

MIB Objects

```
vlanHAPortTable
   vlanHAPortVlanId
   vlanHAPortType
   vlanHAPortIfIndex
```

vlan port-mac egress-port

Adds and removes egress ports from a high availability (HA) VLAN.

vlan *vid* **port-mac egress-port** *slot1/port1***[-***port1a***] [***slot2/port2***[-***port2a***]...]**

vlan *vid* **port-mac no egress-port** *slot1/port1***[-***port1a***] [***slot2/port2***[-***port2a***]...]**

Syntax Definitions

vid	An existing VLAN ID number (1–4094).
*slot1/port1***[-***port1a***]**	The egress slot and port combination to be included in this HA VLAN. You may enter multiple ports and port ranges.
*slot2/port2***[-***port2a***]**	Additional egress slot and port combinations may be included with this HA VLAN. You may enter multiple ports and port ranges.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the **vlan port-mac egress-port** command to remove one or more egress ports from an HA VLAN.
- Note that removing the last ingress/egress port from an HA VLAN is not allowed. Deleting the VLAN is required when there is only one ingress/egress port left in the VLAN.
- This command only applies to fixed ports on second-generation Network Interface (NI) modules. Mobile ports, 802.1Q tagged ports, link aggregate ports, Learned Port Security (LPS) ports, and ports that mirror or are mirrored are not eligible for transition to an egress port state.
- It is not necessary to specify ports in any sequential order or only ports that reside on the same second-generation NI module.
- Using this command on a standard VLAN converts that VLAN into an HA VLAN.
- All HA VLAN related ports must first belong to the same default VLAN before they are configured as ingress, egress, or inter-switch ports for the HA VLAN.
- A port can be designated as both an ingress and egress port, these states are not mutually exclusive.
- Traffic received on egress ports is bridged as regular traffic, regardless of their ingress or egress port state.

Examples

```
-> vlan 20 port-mac egress-port 1/1
-> vlan 125 port-mac egress-port 4/1 4/5 8/1
-> vlan 3000 port-mac egress-port 2/1-5
-> vlan 3000 port-mac egress-port 2/1-5 3/2 3/7 4/1-4
-> vlan 20 port-mac no egress-port 1/1
-> vlan 125 port-mac no egress-port 4/1 4/5 8/1
-> vlan 3000 port-mac no egress-port 2/1-5
-> vlan 3000 port-mac no egress-port 2/1-5 3/2 3/7 4/1-4
```

Release History

Release 5.1; command was introduced.

Related Commands

vlan	Creates and deletes VLANs.
vlan port-mac ingress-port	Adds and deletes ingress ports from an HA VLAN.
show mac-address-table port-mac	Displays the configuration and status of HA VLANs on a switch.

MIB Objects

```
vlanHAPortTable
   vlanHAPortVlanId
   vlanHAPortType
   vlanHAPortIfIndex
```

mac-address-table port-mac vlan mac

Adds and removes MAC addresses from a high availability (HA) VLAN. This association identifies the specified MAC address as a destination MAC

mac-address-table port-mac vlan *vid* **mac** *mac_address1* **[***mac_address2***...]**

mac-address-table port-mac vlan *vid* **no mac** *mac_address1* **[***mac_address2***...]**

Syntax Definitions

vid	An existing VLAN ID number (1–4094).
mac_address1	A valid MAC address to associate with the HA VLAN (for example, 00:95:2A:3C:10.2E or 01:11:22:33:44:55).
mac_address2	Additional MAC addresses to associate with this HA VLAN.

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the **mac-address-table port-mac vlan** command to remove one or more destination MAC addresses from an HA VLAN.
- Note that removing the last MAC address from an HA VLAN is not allowed. Deleting the VLAN is required when there is only one MAC address left.
- Both unicast and multicast MAC addresses are supported.

Examples

```
-> mac-address-table port-mac vlan 10 mac 01:11:22:33:44:55
-> mac-address-table port-mac vlan 10 mac 00:11:22:33:44:55 00:13:14:34:34:78
07:23:45:67:11:21
-> mac-address-table port-mac vlan 10 no mac 01:11:22:33:44:55
-> mac-address-table port-mac vlan 10 no mac 00:11:22:33:44:55 00:13:14:34:34:78
07:23:45:67:11:21
```

Release History

Release 5.1; command was introduced.

Related Commands

show mac-address-table port-mac	Displays the configuration and status of HA VLANs on a switch.
show mac-address-table	Displays Source Learning MAC Address Table information.

MIB Objects

```
slMacToPortMacTable
   vlanHAPortVlanId
   slMacToPortMacAddress
```

vlan port-mac bandwidth

Configures the bandwidth for the ingress flood queue associated with high availability (HA) VLANs.

vlan *vid* **port-mac bandwidth** *mbps*

Syntax Definitions

vid	An existing HA VLAN ID number (1–4094).
mbps	Bandwidth value for the specified HA VLAN flood queue (1mbps – 1000mbps).

Defaults

By default, the flood queue bandwidth for an HA VLAN is set to 15 mbps.

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

- The VLAN ID specified with this command must be the ID for an HA VLAN. An HA VLAN contains at least one ingress or egress port and one MAC address.
- The ingress flood queue is created when the first HA VLAN is configured on the switch, and deleted when the last HA VLAN is removed from the switch.

Examples

```
-> vlan 10 port-mac bandwidth 50
-> vlan 200 port-mac bandwidth 1000
```

Release History

Release 5.1.6; command was introduced.

Related Commands

vlan port-mac ingress-port	Adds and removes ingress ports from an HA VLAN.
vlan port-mac egress-port	Adds and removes egress ports from an HA VLAN.
mac-address-table port-mac vlan mac	Adds and removes MAC addresses from an HA VLAN.

MIB Objects

```
vlanTable
   vlanNumber
   vlanHABandwidth
```

show mac-address-table port-mac

Displays the configuration and status of high availability (HA) VLANs on a switch.

show mac-address-table port-mac [vlan *vid***]**

Syntax Definitions

vid	An existing VLAN ID number (1–4094).

Defaults

N/A

Platforms Supported

OmniSwitch 7700, 7800, 8800

Usage Guidelines

If you specify a VLAN number, only information for that HA VLAN will be displayed. If you do not specify a VLAN number, information for all HA VLANs will be displayed.

Examples

```
-> show mac-address-table port-mac
Port mac configuration for vlan 10

Bandwidth : 15 MB/sec

   Ingress Port list:
           3/5   3/7
   Egress Port list:
           3/9  3/6
   Mac Address list:
           00:DA:95:3C:44:55
           00:13:14:34:5E:78
           01:23:45:C1:17:21

Port mac configuration for vlan 20

Bandwidth : 15 MB/sec

   Ingress Port list:
           1/4  8/2
   Egress Port list:
           4/9  4/6
   Mac Address list:
           00:11:22:33:44:05
           07:23:14:34:31:25
           00:23:45:67:43:04
```

```
-> show mac-address-table port-mac vlan 10
Port mac configuration for vlan 10

Bandwidth : 15 MB/sec

   Ingress Port list:
           3/5   3/7
   Egress Port list:
           3/9  3/6
   Mac Address list:
           00:DA:95:3C:44:55
           00:13:14:34:5E:78
           01:23:45:C1:17:21
```

Output fields are described here:

output definitions

Bandwidth	The bandwidth size for the HA VLAN ingress flood queue. You can change this value with the **vlan port-mac bandwidth**.
Ingress Port list	The ingress ports assigned to this HA VLAN. You can assign ingress ports with the **vlan port-mac ingress-port** command, which is described on page 42-2.
Egress Port list	The egress ports assigned to this HA VLAN. You can assign egress ports with the **vlan port-mac egress-port** command, which is described on page 42-4.
MAC Address list	The MAC addresses associated with this HA VLAN.

Release History

Release 5.1; command was introduced.
Release 5.1.6; **bandwidth** field added.

Related Commands

vlan	Creates and deletes VLANs.
show mac-address-table	Displays Source Learning MAC Address Table information.
show vlan	Displays a list of existing VLANs.
show vlan port	Displays VLAN port assignments.

MIB Objects

```
vlanHAPortTable
   vlanHAPortVlanId
   vlanHAPortType
   vlanHAPortIfIndex
slMacToPortMacTable
   vlanHAPortVlanId
   slMacToPortMacAddress
vlanTable
   vlanNumber
```

43 AAA Commands

This chapter includes descriptions for authentication, authorization, and accounting (AAA) commands. The commands are used for configuring the type of authentication as well as the AAA servers and the local user database on the switch.

- Authenticated VLANs. Authenticates users through the switch into particular VLANs. User information is stored on an external RADIUS or LDAP server.
- Authenticated Switch Access. Authenticates users into the switch to manage the switch. User information is stored on a RADIUS, LDAP, or ACE/Server; or information may be stored locally in the switch user database.
- Local user database. User information may be configured for Authenticated Switch Access. For functional management access, users may be allowed to access specific command families or domains. Alternately, users may be configured with a profile that specifies access to particular ports or VLANs.

ALCATEL-IND1-AAA-MIBA summary of the available commands is listed here:

Authentication servers	**aaa radius-server** **aaa ldap-server** **aaa ace-server clear** **show aaa server**
Authenticated VLANs	**aaa authentication vlan single-mode** **aaa authentication vlan multiple-mode** **aaa vlan no** **aaa accounting vlan** **aaa avlan dns** **aaa avlan default dhcp** **avlan default-traffic** **avlan port-bound** **avlan auth-ip** **aaa avlan http language** **show aaa authentication vlan** **show aaa accounting vlan** **show avlan user** **show aaa avlan config** **show aaa avlan auth-ip**
Authenticated Switch Access	**aaa authentication** **aaa authentication default** **aaa accounting session** **show aaa authentication** **show aaa accounting**

802.1X Port-Based Network Access Control	**aaa authentication 802.1x** **aaa authentication mac** **aaa accounting 802.1x** **show aaa authentication 802.1x** **show aaa authentication mac** **show aaa accounting 802.1x**
Local user database and partitioned management	**user** **password** **user password-size min** **user password-expiration** **show user** **show user password-size** **show user password-expiration** **show aaa priv hexa**
End-user profiles	**user** **end-user profile** **end-user profile port-list** **end-user profile vlan-range** **show end-user profile**

aaa radius-server

Configures or modifies a RADIUS server for Authenticated VLANs, Authenticated Switch Access, or 802.1X port access control.

aaa radius-server *server* **[host {***hostname* | *ip_address***} [***hostname2* | *ip_address2***]] [key** *secret***] [retransmit** *retries***] [timeout** *seconds***] [auth-port** *auth_port***] [acct-port** *acct_port***]**

no aaa radius server *server*

Syntax Definitions

server	The name of the RADIUS server.
hostname	The host name (DNS name) of the primary RADIUS server. The host name or IP address is required when creating a server.
ip_address	The IP address of the primary RADIUS server. An IP address or host name is required when creating a server.
hostname2	The host name (DNS name) of an optional backup RADIUS server.
ip_address2	The IP address of an optional backup RADIUS server.
secret	The shared secret known to the switch and the server, but which is not sent over the network. Can be any text or hexadecimal string but MUST match the secret configured on the server. The secret is case-sensitive. Required when creating a server.
retries	The number of retries the switch makes to authenticate a user before trying the backup server (*hostname2* or *ip_address2*).
seconds	The timeout for server replies to authentication requests.
auth_port	The UDP destination port for authentication requests.
acct_port	The UDP destination port for accounting requests.

Defaults

parameter	default
retries	3
seconds	2
auth_port	1645
acct_port	1646

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- A host name (or IP address) and a secret are required when configuring a server.
- The server and the backup server must both be RADIUS servers.
- Use the **no** form of the command to remove a RADIUS server from the configuration. Only one server may be deleted at a time.
- Always edit password/key information before applying an ASCII text file produced via the **configuration snapshot aaa** command. Server information saved with this command or displayed with the **show configuration snapshot aaa** command contains hashed (encrypted) password/key values. AAA expects this information encrypted only at boot-up time, while at run time the information should be in plain text. If the encrypted password/key values are not changed to plain text, server configuration may fail when the snapshot file is applied to the switch.

Examples

```
-> aaa radius-server pubs2 host 10.10.2.1 key wwwtoe timeout 5
-> no aaa radius-server pubs2
```

Release History

Release 5.1; command was introduced.

Related Commands

show aaa server	Displays information about AAA servers.
aaa authentication vlan single-mode	Specifies the AAA servers to be used in single-authority mode for Authenticated VLANs.
aaa authentication vlan multiple-mode	Specifies the AAA servers to be used for Authenticated VLANs in multiple-authority mode.
aaa authentication	Specifies the AAA servers to be used for Authenticated Switch Access.
aaa accounting vlan	Specifies the accounting servers to be used for Authenticated VLANs.
aaa accounting session	Specifies the accounting servers to be used for Authenticated Switch Access.

MIB Objects

```
aaaServerTable
   aaasProtocol
   aaasHostName
   aaasIpAddress
   aaasHostName2
   aaasIpAddress2
   aaasRadKey
   aaasRetries
   aaasTimout
   aaasRadAuthPort
   aaasRadAcctPort
```

aaa ldap-server

Configures or modifies an LDAP server for Authenticated VLANs or Authenticated Switch Access.

aaa ldap-server *server_name* **[host {***hostname* | *ip_address***} [{***hostname2* | *ip_address2***}]] [dn** *dn_name***] [password** *super_password***] [base** *search_base***] [retransmit** *retries***] [timeout** *seconds***] [ssl | no ssl] [port** *port***]**

no aaa ldap-server *server-name*

Syntax Definitions

server_name	The name of the LDAP server.
hostname	The host name (DNS) of the primary LDAP server. The host name or IP address is required when creating a new server.
ip_address	The IP address of the primary LDAP server.
hostname2	The host name (DNS) of the backup LDAP server.
ip_address2	The IP address of a backup host for the LDAP server.
dn_name	The super-user or administrative distinguished name in the format recognized by the LDAP-enabled directory servers. For example: **cn=manager**. Must be different from the *search-base* name and must be in a format supported by the server. Required when creating a new server.
super_password	The super-user password recognized by the LDAP-enabled directory servers. The password may be clear text or hexadecimal format. Required when creating a new server.
search_base	The search base recognized by the LDAP-enabled directory servers. For example, **o=company** or **c=country**. Must be different from the *dn_name*. Required when creating a new server.
retries	The number of retries the switch makes to the LDAP server to authenticate a user before trying the backup server.
seconds	The timeout in seconds for server replies to authentication requests from the switch.
ssl	Enables a secure switch layer (SSL) between the switch and the LDAP server.
no ssl	Disables a secure switch layer (SSL) between the switch and the LDAP server.
port	The port number for the primary LDAP server and any backup server. Must match the port number configured on the server.

Defaults

Defaults for optional parameters are as follows:

parameter	default
port	389 (SSL disabled) 636 (SSL enabled)
retries	3
seconds	2
ssl | no ssl	no ssl

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The *dn_name* must be different from the *search_base* name.
- Use the **no** form of the command to remove an LDAP server from the configuration. Only one server may be removed at a time.
- The port number configured on the switch must match the port number configured for the server.
- Always edit password/key information before applying an ASCII text file produced via the **configuration snapshot aaa** command. Server information saved with this command or displayed with the **show configuration snapshot aaa** command contains hashed (encrypted) password/key values. AAA expects this information encrypted only at boot-up time, while at run time the information should be in plain text. If the encrypted password/key values are not changed to plain text, server configuration may fail when the snapshot file is applied to the switch.

Examples

```
-> aaa ldap-server topanga5 host 10.10.3.4 dn cn=manager password tpub base c=us
retransmit 4
-> no aaa ldap-server topanga5
```

Release History

Release 5.1; command was introduced.

Related Commands

show aaa server	Displays information about AAA servers.
aaa authentication vlan single-mode	Specifies the AAA servers to be used in single-authority mode for Authenticated VLANs.
aaa authentication vlan multiple-mode	Configures AAA servers for Authenticated VLANs in multiple-authority mode.
aaa authentication	Specifies the AAA servers to be used for authenticated switch access.
aaa accounting vlan	Specifies the accounting servers to be used for Authenticated VLANs.
aaa accounting session	Specifies the accounting servers to be used for Authenticated Switch Access.

MIB Objects

```
aaaServerTable
   aaasProtocol
   aaasHostName
   aaasIpAddress
   aaasHostName2
   aaasIpAddress2
   aaasLdapPort
   aaasLdapDn
   aaasLdapPasswd
   aaasLdapSearchBase
   AaasLdapServType
   aaasRetries
   aaasTimeout
   aaasLdapEnableSsl
```

aaa ace-server clear

Clears the ACE secret on the switch. An ACE/Server generates “secrets” that it sends to clients for authentication. The secret cannot be configured on the switch but may be cleared on the switch.

aaa ace-server clear

Syntax Defintions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Clear the ACE secret on the switch if the server and the switch get out of synch. See RSA Security’s ACE/Server documentation for more information.
- If you clear the secret on the switch, it must also be cleared on the server.

Examples

```
-> aaa ace-server clear
```

Release History

Release 5.1; command was introduced.

Related Commands

aaa authentication	Specifies servers for Authenticated Switch Access.
show aaa server	Displays information about AAA servers configured for the switch.

MIB Objects

```
aaaServerTable
   aaasAceClear
```

aaa authentication vlan single-mode

Specifies the AAA servers to be used in single-authority mode for Authenticated VLANs.

aaa authentication vlan single-mode *server1* **[***server2***] [***server3***] [***server4***]**

no aaa authentication vlan

Syntax Definitions

server1	The name of the RADIUS or LDAP authentication server used for authenticating users through all authenticated VLANs on the switch. At least one server is required. RADIUS and LDAP server names are set up through the **aaa radius-server** and **aaa ldap-server** commands.
server2...server4	The names of backup servers for authenticating users through authenticated VLANs. Up to 3 backups may be specified; include a space between each server name. These backups are only used if *server1* becomes unavailable. They are polled in the order they are listed in this command. The first available server becomes the authentication server.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to disable authenticated VLANs in single mode.
- The servers may be RADIUS or LDAP servers, or both. Up to 4 servers (total) may be configured in single mode. Each server name should be separated by a space.
- The switch uses ***only the first available server*** in the list to check for user information. For example, if *server1* is not available, the switch will poll *server2*. If user information is not found on the first available server, the authentication request will fail.
- RADIUS and LDAP servers may each have an additional backup specified through the **aaa radius-server** and **aaa ldap-server** commands.

Examples

```
-> aaa authentication vlan single-mode pubs1 pubs2 pubs3
```

Release History

Release 5.1; command was introduced.

Related Commands

aaa radius-server	Configures or modifies a RADIUS server for authenticated VLANs or Authenticated Switch Access.
aaa ldap-server	Configures or modifies an LDAP server for authenticated VLANs or Authenticated Switch Access.
show aaa server	Displays information about a particular AAA server or AAA servers.
show aaa authentication vlan	Displays information about servers configured for authenticated VLANs.

MIB Objects

```
aaaAuthVlanTable
   aaatvName1
   aaatvName2
   aaatvName3
   aaatvName4
```

aaa authentication vlan multiple-mode

Specifies the AAA servers to be used in multiple-authority mode for Authenticated VLANs.

aaa authentication vlan multiple-mode *vlan_id server1* **[***server2***] [***server3***] [***server4***]**

no aaa authentication vlan *vlan_id*

Syntax Definitions

vlan_id	The VLAN associated with the server or chain of servers.
server1	The name of the RADIUS or LDAP authentication server used for this authenticated VLAN in multiple mode. At least one server is required. RADIUS and LDAP server names are set up through the **aaa radius-server** and **aaa ldap-server** commands.
server2...server4	The names of backup servers for authenticating users through this VLAN. Up to 3 backups may be specified; include a space between each server name. These backups are only used if *server1* becomes unavailable. They are polled in the order they are listed in this command. The first available server becomes the authentication server.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to remove authenticated VLANs in multiple mode.
- The servers may be RADIUS or LDAP servers, or both. Up to 4 servers (total) may be configured for each VLAN in multiple mode. Each server name should be separated by a space.
- The switch uses ***only the first available server*** in the list to check for user information. For example, if *server1* is not available, the switch will poll *server2*. If user information is not found on the first available server, the authentication request will fail.
- RADIUS and LDAP servers may each have an additional backup specified through the **aaa radius-server** and **aaa ldap-server** commands.

Examples

```
-> aaa authentication vlan multiple-mode 2 pubs1 pubs2
```

Release History

Release 5.1; command was introduced.

Related Commands

aaa radius-server	Configures or modifies a RADIUS server for authenticated VLANs or Authenticated Switch Access.
aaa ldap-server	Configures or modifies an LDAP server for authenticated VLANs or Authenticated Switch Access.
show aaa server	Displays information about a particular AAA server or AAA servers.
show aaa authentication vlan	Displays information about servers configured for authenticated VLANs.

MIB Objects

```
aaaAuthVlanTable
   aaatvName1
   aaatvName2
   aaatvName3
   aaatvName4
```

aaa vlan no

Removes a user from an Authenticated VLAN. You must know the MAC address associated with the user.

aaa avlan no [mac-address] *mac_address*

Syntax Definitions

mac-address	Optional syntax.
mac_address	The MAC address of the user who should be removed from an authenticated VLAN.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **show avlan user** command to display user MAC addresses.

Examples

```
-> aaa avlan no 00:20:da:05:f6:23
```

Release History

Release 5.1; command was introduced.

Related Commands

aaa authentication vlan single-mode	Specifies the AAA servers to be used in single-authority mode for Layer 2 Authentication.
aaa authentication vlan multiple-mode	Specifies the AAA servers to be used in multiple-authority mode for authenticated VLANs.
show avlan user	Displays MAC addresses for authenticated VLAN users on the switch.

MIB Objects

```
aaaAuthenticatedUserTable
   aaadMac
```

aaa avlan dns

Configures a DNS host name. When clients authenticate via a Web browser, they will be able to enter the DNS host name rather than enter the IP address.

aaa avlan dns [name] *dns_name*

no aaa avlan dns [name]

Syntax Definitions

dns_name	The name of the DNS host.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **no** form of the command to remove a host name from the configuration.

Examples

```
-> aaa avlan dns wolfie
-> no aaa avlan dns
```

Release History

Release 5.1; command was introduced.

Related Commands

show aaa avlan config	Displays the current DNS and DHCP configuration for authenticated VLANs.

MIB Objects

```
aaaAvlanConfigTable
   aaaAvlanDnsName
```

aaa avlan default dhcp

Configures the gateway address for a DHCP server.

aaa avlan default dhcp [gateway] *ip_address*

no aaa avlan default dhcp [gateway]

Syntax Definitions

ip_address	The IP address of the AVLAN default gateway.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **no** form of the command to remove an AVLAN default gateway from the configuration.

Examples

```
-> aaa avlan dhcp 128.23.4.1
-> no aaa avlan dhcp
```

Release History

Release 5.1; command was introduced.

Related Commands

show aaa avlan config	Displays the current DNS and DHCP configuration for authenticated VLANs.

MIB Objects

```
aaaAvlanConfigTable
   aaaAvlanDhcpDefGateway
```

aaa authentication

Configures the interface for Authenticated Switch Access and specifies the server(s) to be used. This type of authentication gives users access to manage the switch.

aaa authentication {console | telnet | ftp | http | snmp | ssh | default} *server1* **[***server2***...] [local]**

no aaa authentication [console | telnet | ftp | http | snmp | ssh | default]

Syntax Definitions

console	Configures Authenticated Switch Access through the console port.
telnet	Configures Authenticated Switch Access for any port used for Telnet.
ftp	Configures Authenticated Switch Access for any port used for FTP.
http	Configures Authenticated Switch Access for any port used for Web-based management.
snmp	Configures Authenticated Switch Access for any port used for SNMP.
ssh	Configures Authenticated Switch Access for any port used for Secure Shell.
default	Configures Authenticated Switch Access for any port using any service (**telnet**, **ftp**, etc.). Note that SNMP access is enabled only if an LDAP or local server is specified with the command.
server1	The name of the authentication server used for Authenticated Switch Access. At least one server is required. The server may be a RADIUS or LDAP server, an ACE/Server, or the local user database. RADIUS and LDAP server names are set up through the **aaa radius-server** and **aaa ldap-server** commands. If an ACE/Server will be used, specify **ace** for the server name. (Only one ACE/Server may be specified.)
server2...	The names of backup servers for Authenticated Switch Access. Up to 3 backups may be specified (including **local**). These backups are only used if *server1* becomes unavailable. They are polled in the order they are listed in this command. The first available server becomes the authentication server.
local	Specifies that the local user database will be a backup for the authentication servers. If you want to use the local user database as the only authentication server, specify **local** for *server1*.

Defaults

- At switch startup, Authenticated Switch Access is available through console port via the local database. Authentication for other management interfaces (Telnet, FTP, etc.) is disabled.
- The default user on the switch is **admin**, and **switch** is the password.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The server type may be RADIUS, LDAP, ACE/Server, or the local user database. Up to 4 servers may be configured for an interface type; at least one is required. Each server name should be separated by a space.
- The switch uses ***only the first available server*** in the list to check for user information. For example, if *server1* is not available, the switch will poll *server2*. If user information is not found on the first available server, the authentication request will fail.
- RADIUS and LDAP servers may each have an additional backup specified through the **aaa radius-server** and **aaa ldap-server** commands.
- If the local switch database will be used as the only authentication server, specify **local** for *server1*. If **local** is specified as a backup server, it should be entered last in the list of servers. The local user database is always available if the switch is up.
- Only LDAP or the local database may be used for authenticated SNMP management.
- An ACE/Server cannot be specified for SNMP access.
- If Secure Shell (**ssh**) is enabled, Telnet and FTP should be disabled.

Examples

```
-> aaa authentication telnet pubs1
-> no aaa authentication telnet
-> aaa authentication default pubs2 pubs3
```

Release History

Release 5.1; command was introduced.

Related Commands

aaa radius-server	Configures or modifies a RADIUS server for authenticated VLANs or Authenticated Switch Access.
aaa ldap-server	Configures or modifies an LDAP server for authenticated VLANs or Authenticated Switch Access.
user	Configures user information for the local database on the switch.
show aaa server	Displays information about servers configured for Authenticated Switch Access.

MIB Objects

```
aaaAuthSATable
   aaatsName1
   aaatsName2
   aaatsName3
   aaatsName4
```

aaa authentication default

Sets the authenticated switch access type to the default server setting.

aaa authentication {console | telnet | ftp | http | snmp | ssh } default

Syntax Definitions

console	Configures the default Authenticated Switch Access server setting for the console port.
telnet	Configures the default Authenticated Switch Access server setting for Telnet.
ftp	Configures the default Authenticated Switch Access server setting for FTP.
http	Configures the default Authenticated Switch Access server setting for Web-based management.
snmp	Configures the default Authenticated Switch Access server setting for any port used for SNMP.
ssh	Configures the default Authenticated Switch Access server setting for any port used for Secure Shell.

Defaults

By default, the default Authenticated Switch Access server setting does not include any servers.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **aaa authentication** command to set the default servers.

Examples

```
-> aaa authentication telnet default
-> aaa authentication default default
```

Release History

Release 5.1; command was introduced.

Related Commands

aaa radius-server	Configures or modifies a RADIUS server for authenticated VLANs or Authenticated Switch Access.
aaa ldap-server	Configures or modifies an LDAP server for authenticated VLANs or Authenticated Switch Access.
user	Configures user information for the local database on the switch.
show aaa server	Displays information about servers configured for Authenticated Switch Access.

MIB Objects

```
aaaAuthSATable
   aaatsName1
   aaatsName2
   aaatsName3
   aaatsName4
```

aaa authentication 802.1x

Enables/disables the switch for 802.1X authentication.

aaa authentication 802.1x *server1* **[***server2***] [***server3***] [***server4***]**

no aaa authentication 802.1x

Syntax Definitions

server1	The name of the RADIUS authentication server used for 802.1X authentication. (*Note that only RADIUS servers are supported for 802.1X authentication.*) At least one server is required. RADIUS server names are set up through the **aaa radius-server** command.
server2...server4	The names of backup servers for authenticating 802.1X users. Up to 3 backups may be specified; include a space between each server name. These backups are only used if *server1* becomes unavailable. They are polled in the order they are listed in this command. The first available server becomes the authentication server.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **vlan port 802.1x** command to enable or disable ports for 802.1X. Use the **802.1x** command to configure authentication parameters for a dedicated 802.1X port.
- Up to 4 RADIUS servers (total) may be specified. At least one server is required. Each server name should be separated by a space.
- The switch uses ***only the first available server*** in the list to check for user information. For example, if *server1* is not available, the switch will poll *server2*. If user information is not found on the first available server, the authentication request will fail.
- RADIUS servers may each have an additional backup specified through the **aaa radius-server** command.
- Before any device is authenticated through an 802.1X port, the port will only process 802.1X frames (EAPoL frames) from an unknown source.
- Note that multiple supplicants can be authenticated on a given 802.1X port. Each supplicant MAC address received on the port is authenticated and learned separately. Only those that authenticate successfully are allowed on the port, as described above. Those that fail authentication are blocked on the 802.1X port.

Examples

```
-> aaa authentication 802.1x open-global rad1 rad2
-> no aaa authentication 802.1x
```

Release History

Release 5.1; command was introduced.
Release 5.1.6 and 5.3.1; command modified.

Related Commands

802.1x	Configures 802.1X parameters on a particular slot/port. Typically used for port access control on a dedicated 802.1X port.
aaa radius-server	Configures or modifies a RADIUS server for Authenticated VLANs, Authenticated Switch Access, or 802.1X port access control.
vlan port 802.1x	Enables or disables 802.1X port-based access control on a mobile port.
show aaa authentication 802.1x	Displays information about the global 802.1X configuration on the switch.

MIB Objects

```
AaaAuth8021XTable
   aaatxName1
   aaatxName2
   aaatxName3
   aaatxName4
   aaatxOpen
```

aaa authentication mac

Enables/Disables the switch for MAC authentication. This type of authentication is available in addition to 802.1x authentication and is designed to handle devices that do not support an 802.1x authentication method (non-supplicants).

aaa authentication MAC *server1* **[***server2***] [***server3***] [***server4***]**

no aaa authentication MAC

Syntax Definitions

server1	The name of the RADIUS authentication server used for MAC authentication. (*Note that only RADIUS servers are supported for MAC authentication.*) At least one server is required. RADIUS server names are set up through the **aaa radius-server** command.
server2...server4	The names of backup servers used for MAC authentication. Up to 3 backups may be specified; include a space between each server name. These backups are only used if *server1* becomes unavailable. They are polled in the order they are listed in this command. The first available server becomes the authentication server.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Up to 4 RADIUS servers (total) may be specified. At least one server is required. Each server name should be separated by a space.
- Use the **no** form of this command to disable MAC authentication for the switch.
- The switch uses ***only the first available server*** in the list to check for user information. For example, if *server1* is not available, the switch will poll *server2*. If user information is not found on the first available server, the authentication request will fail.
- RADIUS servers may each have an additional backup specified through the **aaa radius-server** command.
- MAC authentication verifies the source MAC address of a non-supplicant device via a remote RADIUS server. Similar to 802.1x authentication, this method sends RADIUS frames to the server with the MAC address embedded in the username and password attributes.
- Note that the same RADIUS servers can be used for 802.1x (supplicant) and MAC (non-supplicant) authentication. Using different servers for each type of authentication is allowed but not required.
- Use the **vlan port 802.1x** command to enable or disable ports for 802.1X. Use the **802.1x non-supplicant policy authentication** command to configure a MAC authentication policy for a dedicated 802.1X port.

- Multiple supplicants and non-supplicants can be authenticated on a given 802.1X port. Each device MAC address received on the port is authenticated and learned separately. If no MAC authentication policies exist on the port, non-supplicants are blocked.

Examples

```
-> aaa authentication mac rad1 rad2
-> no aaa authentication mac
```

Release History

Release 5.4.1; command was introduced.

Related Commands

802.1x	Configures 802.1X parameters on a particular slot/port. Typically used for port access control on a dedicated 802.1X port.
802.1x non-supplicant policy authentication	Configures MAC authentication device classification policies for non-supplicants.
aaa radius-server	Configures or modifies a RADIUS server for Authenticated VLANs, Authenticated Switch Access, or 802.1X port access control.
vlan port 802.1x	Enables or disables 802.1X port-based access control on a mobile port.
show aaa authentication 802.1x	Displays information about the global 802.1X configuration on the switch.

MIB Objects

```
AaaAuthMACTable
   aaaMacSrvrName1
   aaaMacSrvrName2
   aaaMacSrvrName3
   aaaMacSrvrName4
```

aaa accounting 802.1x

Enables/disables accounting for 802.1X authentication sessions. Accounting servers keep track of network resources (time, packets, bytes, etc.) and user activity.

aaa accounting 802.1x *server1* **[***server2***...] [local]**

no aaa accounting 802.1x

Syntax Definitions

server1	The name of the RADIUS or LDAP server used for 802.1X accounting. At least one server is required. RADIUS and LDAP server names are set up through the **aaa radius-server** and **aaa ldap-server** commands.
server2...	The names of backup servers for 802.1X accounting. Up to 3 backups may be specified (including **local**); include a space between each server name. These backups are only used if *server1* becomes unavailable. They are polled in the order they are listed in this command. The first available server becomes the accounting server.
local	Local accounting is done through the Switch Logging feature in the switch. See Chapter 46, "Switch Logging Commands," for information about Switch Logging commands.

Defaults

Accounting is disabled by default.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to disable accounting for 802.1X ports.
- Up to 4 accounting servers (total) may be specified. At least one server is required. Each server name should be separated by a space.
- The servers may be RADIUS or LDAP servers, and/or the local Switch Logging facility.
- If **local** is specified as *server1*, the switch will ***only*** use the local Switching Logging facility for accounting.
- If **local** is specified as a backup, it should be entered last in the list of servers. The Switch Logging facility is always available if the switch is up.
- The switch uses ***only the first available server*** in the list for accounting. For example, if *server1* is not available, the switch will use *server2*.
- RADIUS and LDAP servers may each have an additional backup specified through the **aaa radius-server** and **aaa ldap-server** commands.

Examples

```
-> aaa accounting 802.1x rad1 local
-> no aaa accounting 802.1x
```

Release History

Release 5.1; command was introduced.

Related Commands

802.1x	Configures 802.1X parameters on a particular slot/port. Typically used for port access control on a dedicated 802.1X port.
aaa radius-server	Configures or modifies a RADIUS server for Authenticated VLANs, Authenticated Switch Access, or 802.1X port access control.
show aaa accounting 802.1x	Displays information about accounting servers for 802.1X sessions.

MIB Objects

```
AaaAcct8021XTable
   aaacxName1
   aaacxName2
   aaacxName3
   aaacxName4
```

aaa accounting vlan

Specifies a server or servers to be used for accounting with Authenticated VLANs. Accounting servers keep track of network resources (time, packets, bytes, etc.) and user activity.

aaa accounting vlan [*vlan_id***] *server1* [*server2*...] [local]**

no accounting vlan [*vlan_id***]**

Syntax Definitions

vlan_id	Required only for multiple mode. The VLAN associated with the accounting server or chain of accounting servers.
server1	The name of the RADIUS or LDAP server used for accounting with Authenticated VLANs. At least one server is required. RADIUS and LDAP server names are set up through the **aaa radius-server** and **aaa ldap-server** commands. If the local accounting feature will be used as the only accounting mechanism, specify **local** for *server1*.
server2...	The names of backup servers. Up to 3 backups may be specified (including **local**); include a space between each server name. Backups are only used if *server1* becomes unavailable. They are polled in the order they are listed in this command. The first available server becomes the accounting server.
local	Local accounting is done through the Switch Logging feature in the switch. See Chapter 46, "Switch Logging Commands," for information about Switch Logging commands.

Defaults

Accounting is disabled by default.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to disable accounting for authenticated VLANs.
- Up to 4 accounting servers (total) may be specified. At least one server is required. Each server name should be separated by a space.
- The servers may be RADIUS or LDAP servers, and/or the local Switch Logging facility.
- If **local** is specified as *server1*, the switch will ***only*** use the local Switching Logging facility for accounting.
- If **local** is specified as a backup, it should be entered last in the list of servers. The Switch Logging facility is always available if the switch is up.
- The switch uses ***only the first available server*** in the list for accounting. For example, if *server1* is not available, the switch will use *server2*.

- RADIUS and LDAP servers may each have an additional backup specified through the **aaa radius-server** and **aaa ldap-server** commands.

Examples

```
-> aaa accounting vlan ldap1 ldap2 ldap3 radius1
-> no accounting vlan
-> aaa accounting vlan 4 radius1 ldap2 local
```

Release History

Release 5.1; command was introduced.

Related Commands

aaa radius-server	Configures or modifies a RADIUS server for authenticated VLANs or Authenticated Switch Access.
aaa ldap-server	Configures or modifies an LDAP server for authenticated VLANs or Authenticated Switch Access.
show aaa accounting	Displays information about accounting servers configured for authenticated VLANs.

MIB Objects

```
aaaAcctVlanTable
   aaacvName1
   aaccvName2
   aaacvName3
   aaacvName4
```

aaa accounting session

Configures an accounting server or servers for authenticated switch sessions. Accounting servers keep track of network resources (time, packets, bytes, etc.) and user activity.

aaa accounting session *server1* **[***server2***...] [local]**

no accounting session

Syntax Definitions

server1	The name of the RADIUS or LDAP server used for accounting of authenticated switch sessions. At least one server is required. RADIUS and LDAP server names are set up through the **aaa radius-server** and **aaa ldap-server** commands.
server2...	The names of backup servers. Up to 3 backups may be specified (including **local**); each server name should be separated by a space. These backups are only used if *server1* becomes unavailable. They are polled in the order they are listed in this command. The first available server becomes the accounting server.
local	Local accounting is done through the Switching Logging feature on the switch. See Chapter 46, "Switch Logging Commands," for information about Switch Logging commands.

Defaults

Accounting is disabled by default.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to disable accounting for Authenticated Switch Access.
- Up to 4 accounting servers (total) may be specified. At least one server is required. Each server name should be separated by a space.
- The servers may be RADIUS or LDAP servers, and/or the local Switch Logging facility.
- If **local** is specified as *server1*, the switch will ***only*** use the local Switching Logging facility for accounting.
- If **local** is specified as a backup, it should be entered last in the list of servers. The Switch Logging facility is always available if the switch is up.
- The switch uses ***only the first available server*** in the list for accounting. For example, if *server1* is not available, the switch will use *server2*.
- RADIUS and LDAP servers may each have an additional backup specified through the **aaa radius-server** and **aaa ldap-server** commands.

Examples

```
-> aaa accounting session ldap1 radius2 local
-> no aaa accounting session
```

Release History

Release 5.1; command was introduced.

Related Commands

show aaa accounting	Displays information about accounting servers configured for Authenticated Switch Access.

MIB Objects

```
aaaAcctsaTable
   aaacsName1
   aaacsName2
   aaacsName3
   aaacsName4
```

avlan default-traffic

Configures whether or not users are able to traffic in the default VLAN before they are actually authenticated.

avlan default-traffic {enable | disable}

Syntax Defintions

enable	Enables the switch to allow users authenticating through the switch to traffic in the default VLAN prior to authentication.
disable	Disables the switch so that users authenticating through the switch cannot traffic in the default VLAN prior to authentication.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- When this command is enabled, users are members of the default VLAN before authentication. After authenticating, users are no longer authorized for the default VLAN.
- When this command is disabled after being enabled, existing users in the default VLAN are not flushed.
- The default VLAN is configurable per port through the **vlan port default** command.
- The **avlan default-traffic** command allows Telnet and HTTP clients to obtain an IP address from a DHCP server in the default VLAN.

Examples

```
-> avlan default-traffic enable
```

Release History

Release 5.1; command was introduced.

Related Commands

vlan port default	Configures a new default VLAN for a single port or an aggregate of ports.
show aaa avlan config	Displays the current global configuration parameters for authenticated VLANs.

MIB Objects

```
aaaAvlanConfigTable
   aaaAvlanDefaultTraffic
```

avlan port-bound

Configures whether or not port mobility rules apply to authenticated ports.

avlan port-bound {enable | disable}

Syntax Defintions

enable	Enables authenticated ports to use port mobility rules.
disable	Disables authenticated ports from using port mobility rules.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

When this command is enabled, a limited number of port mobility binding rule types may be applied to authenticated ports. The types are as follows:

- port-MAC-IP address binding rule
- port-MAC binding rule
- port-IP address binding rule
- port-MAC-protocol binding rule

A MAC range rule type, is not supported on an OmniSwitch 6600, OmniSwitch 7700/7800, or an OmniSwitch 8800.

For more information about commands for configuring port binding rules, see Chapter 20, “Port Mobility Commands.”

Examples

```
-> avlan port-bound enable
```

Release History

Release 5.1; command was introduced.

Related Commands

vlan binding mac-ip-port	Defines a binding MAC-IP-port rule for an existing VLAN. Device frames received on the specified mobile port must also contain a source MAC address and source IP address that matches the MAC and IP address specified in the rule.
vlan binding mac-port-protocol	Defines a binding MAC-port-protocol rule for an existing VLAN. Device frames received on the specified mobile port must contain a source MAC address and protocol type that matches the MAC address and protocol type value specified in the rule.
vlan binding mac-port	Defines a binding MAC-port rule for an existing VLAN. Device frames received on the specified mobile port must contain a source MAC address that matches the MAC address specified in the rule.
vlan binding ip-port	Defines a binding IP-port rule for an existing VLAN. Device frames received on the specified mobile port must contain a source IP address that matches the IP address specified in the rule.
show aaa avlan config	Displays the current global configuration parameters for authenticated VLANs.

MIB Objects

```
aaaAvlanConfigTable
   aaaAvlanPortBound
```

avlan auth-ip

Configures an IP address to be used for VLAN authentication.

avlan *vlan_id* **auth-ip** *ip_address*

Syntax Defintions

vlan_id	The ID of the authenticated VLAN.
ip_address	The IP address to be used for authentication on this VLAN. The IP address must have the same mask as the router port address for the authenticated VLAN.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If an IP address is not configured for an authenticated VLAN, the switch automatically configures the address with an authentication address based on the router port address (*x.x.x*.253).
- The IP address of the authenticated VLAN must have the same mask as the router port address. For example, if the router port address of the authenticated VLAN is 10.10.2.4, then the IP address must be 10.10.2.*x*.
- VLANs are set up for authentication through the **vlan authentication** command.

Examples

```
-> avlan 3 auth-ip 10.10.2.4
```

Release History

Release 5.1; command was introduced.

Related Commands

vlan authentication	Enables or disables authentication for a VLAN.
show aaa avlan auth-ip	Displays the IP addresses for authenticated VLANs.

MIB Objects

```
aaaAvlanConfigTable
   aaaAvlanAddress
```

aaa avlan http language

Configures the switch to display username and password prompts based on the contents of a translation file (labels.txt).

aaa avlan http language

Syntax Defintions

N/A

Defaults

By default, the switch displays the HTTP client login page username and password prompts in English.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- When this command is entered, the next WebView session on the switch will use the username and password strings contained in the **label.txt** file.
- The label.txt file is available on the switch in the /flash/switch directory when the **Fsecu.img**, **Esecu.img**, or **Hsecu.img** file is installed with the **install** command. The label.txt file may be modified with any text editor and may contain strings for the username and password prompts in the format:

  Username="*username_string*"
  Password="*password_string*"
- If the **aaa avlan http language** command is specified, but the label.txt file does not exist on the switch or the file is empty (the default), the switch will use the English-language text defaults for the HTTP client login page.

Examples

```
-> aaa avlan http language
```

Release History

Release 5.1; command was introduced.

Related Commands

install	Installs an image file from the switch's working directory.

MIB Objects

```
aaaAvlanConfigTable
   aaaAvlanLanguage
```

user

Configures or modifies user entries in the local user database. Use the **no** form of the command to remove the user from the local database.

user *username* **[password** *password***] [expiration {***day* **|** *date***}] [read-only | read-write [***families... | domains...***| all | none]] [no snmp | no auth | sha | md5 | sha+des | md5+des] [end-user profile** *name***]**

no user *username*

Syntax Definitions

username	The name of the user (maximum is 31 alphanumeric characters). Used for logging into the switch. Required to create a new user entry or for modifying a user.
password	The user's password in clear text or hexadecimal (corresponding to encrypted form). Required to create a new user entry. The default minimum length is 8 alphanumeric characters. The maximum is 47 characters on OmniSwitch 6600, 7700, 7800, and 8800 switches.
day	The number of days before this user's current password expires. The range is 1 to 150 days.
date	The date (in the format *mm/dd/yyyy hh:mm*) that the user's current password will expire.
read-only	Specifies that the user will have read-only access to the switch.
read-write	Specifies that the user will have read-write access to the switch.
families	Determines the command families available to the user on the switch. Each command family should be separated by a space. Command families are subsets of domains. See Usage Guidelines for more details.
domains	Determines the command domains available to the user on the switch. Each domain should be separated by a space. See the Usage Guidelines for more details.
all	Specifies that all command families and domains are available to the user.
none	Specifies that no command families or domains are available to the user.
no snmp	Denies the specified user SNMP access to the switch.
no auth	Specifies that the user has SNMP access without any required SNMP authentication and encryption protocol.
sha	Specifies that the SHA authentication algorithm should be used for authenticating SNMP PDU for the user.
md5	Specifies that the MD5 authentication algorithm should be used for authenticating SNMP PDU for the user.

sha+des	Specifies that the SHA authentication algorithm and DES encryption standard should be used for authenticating and encrypting SNMP PDU for the user.
md5+des	Specifies that the MD5 authentication algorithm and the DES encryption standard should be used for authenticating and encrypting SNMP PDU for the user.
name	The name of an end-user profile associated with this user. Configured through the **end-user profile** command. Cannot be associated with the user if command families/domains are associated with the user.

Defaults

By default, if a user is created without indicating the read and write privileges and SNMP access, the user will be given privileges based on the *default user account*. The default user account may be modified, but by default it has the following privileges:

parameter	default
read-only | read-write	read-only
no snmp | no auth | sha | md5 | sha+des | md5+des	no snmp

For more information about the default user account, see the *Switch Management Guide*.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- In addition to the syntax listed for the command, the syntax **authkey** *key* will display in an ASCII text file produced via the **snapshot** command if the user is allowed SNMPv3 access to the switch.The authentication key is in hexadecimal form, and is deducted from the user's password with SHA or MD5 hash and encrypted with DES encryption. The key parameter only appears in configuration files that are resulting from a snapshot. The key is computed by the switch based on the user's SNMP access and will only appear in the ASCII text file; it is not displayed through the CLI. (*This key is used for both Auth Password and Priv Password in the OmnVista NMS application.*)
- At least one user with SHA/MD5 authentication and/or DES encryption must be configured on the switch for SNMPv3 communication with OmniVista.
- Use **user** *username password* to reset a user's password configured through the **password** command.
- Typically the password should be a string of non-repeating characters. The CLI uses the first occurrence of the character series to uniquely identify the password. For example, the password *tpubtpub* is the same as *tpub*. A better password might be *tpub345*.
- The password expiration date will display in an ASCII text file produced via the **snapshot** command.
- A password expiration for the user's current password may be configured with the **expiration** option. However, if the password is changed, or the global password expiration setting is configured with the **user password-expiration** command, the user's password expiration will be configured with the global expiration setting.

- When modifying a user's SNMP access, the user password must be re-entered (or a new one configured). This is required because the hash algorithm used to save the password in the switch depends on the SNMP authentication level.
- At initial startup, the default user on the switch is **admin** with a password of **switch**. The switch will not recreate this user at any successive startup as long as there exists at least one user defined with write access to all commands. (Note that if password expiration is configured for the **admin** user, or configured globally through the **user password-expiration** command, when the **admin** user's password expires, the **admin** user will have access only through the console port.)
- Either privileges or an end-user profile may be associated with a user; both cannot be configured for the same user.
- New users or updated user settings are saved *automatically*; that is, these settings do not require the **write memory**, **copy running-config working**, or **configuration snapshot** command to save user settings over a reboot.

Possible values for domains and families are listed in the table here:

Domain	Corresponding Families
domain-admin	file telnet dshell debug
domain-system	system aip snmp rmon webmgt config
domain-physical	chassis module interface pmm health
domain-network	ip rip ospf bgp vrrp ip-routing ipx ipmr ipms
domain-layer2	vlan bridge stp 802.1q linkagg ip-helper
domain-service	dns
domain-policy	qos policy slb
domain-security	session avlan aaa

Examples

```
-> user techpubs password writer read-only config
-> no user techpubs
```

Release History

Release 5.1; command was introduced.

Related Commands

password	Configures the current user's password.
show user	Displays information about users configured in the local database on the switch.

MIB Objects

```
aaaUserTable
   aaauPassword
   aaauReadRight
   aaauWriteRight
   aaauSnmpLevel
   aaauSnmpAuthKey
   aaauPasswordExpirationDate
```

password

Configures the current user's password.

password

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If the **snapshot** command is used to capture the switch configuration, the text of the password is not displayed in the file. Instead an authentication key is included in the file.
- The **password** command does not require a password in-line; instead, after the command is entered, the system displays a prompt for the password. Enter any alphanumeric string. (The string displays on the screen as asterisks.) The system displays a prompt to verify the new password.
- A new password cannot be identical to the current password; it cannot be identical to any of the three passwords that preceded the current password.
- The password may be up to 47 characters on OmniSwitch 6600, 7700, 7800, and 8800 switches. The default minimum password length is 8 characters.
- Password settings are saved *automatically*; that is, the **write memory**, **copy running-config working**, or **configuration snapshot** command is not required to save password settings over a reboot.

Examples

```
-> password
enter old password: ********
enter new password: *********
reenter new password: *********
->
```

Release History

Release 5.1; command was introduced.

Related Commands

user	Configures entries in the local user database. May be used by a system administrator to change any user's password in addition to configuring user privileges or profile.

MIB Objects

```
aaaUserTable
   aaauPassword
   aaauOldPassword
```

user password-size min

Configures the minimum number of characters required when configuring a user password.

user password-size min *size*

Syntax Definitions

size	The number of characters required when configuring a user password through the **password** command or when setting up a user password through the **user** command.

Defaults

parameter	default
size	8

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

The maximum password size is 47 characters on OmniSwitch 6600, 7700, 7800, and 8800 switches. Use the **user password-size min** command to change the minimum character length for the password.

Examples

```
-> user password-size min 9
```

Release History

Release 5.1; command was introduced.

Related Commands

user	Configures entries in the local user database. May be used by a system administrator to change any user's password in addition to configuring user privileges or profile.
show user password-size	Displays the minimum number of characters that are required for a user password.

MIB Objects

```
aaaAsaConfig
   aaaAsaPasswordSizeMin
```

user password-expiration

Configures an expiration date for user passwords stored locally on the switch or disables password expiration.

user password-expiration {*day* | **disable}**

Syntax Definitions

day	The number of days before locally configured user passwords will expire. The range is 1 to 150 days.
disable	Disables password expiration for users configured locally on the switch.

Defaults

parameter	default
day | **disable**	disable

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The **user password-expiration** command sets a default password expiration for users configured locally on the switch.
- Password expiration may be configured on a per-user basis through the **user** command; the user setting overrides the **user password-expiration** setting until the user password is changed or the **user password-expiration** command is entered again.

Examples

```
-> user password-expiration 2
-> user password-expiration disable
```

Release History

Release 5.1; command was introduced.

Related Commands

user	Configures entries in the local user database. May be used by a system administrator to change any user's password in addition to configuring user privileges or profile.
show user password-expiration	Displays the expiration date for passwords configured for user accounts stored on the switch.

MIB Objects

```
aaaAsaConfig
   aaaAsaDefaultPasswordExpirationInDays
```

end-user profile

Configures or modifies an end user profile, which specifies access to command areas. The profile may be attached to a customer login user account.

end-user profile *name* **[read-only [***area* **| all]] [read-write [***area* **| all]] [disable [***area* **| all]]**

no end-user profile *name*

Syntax Definitions

name	The name of the end-user profile, up to 32 alphanumeric characters.
area	Command areas on the switch to which the user is allowed or denied access. Areas include **physical**, **vlan-table**, **basic-ip-routing**, **ip-routes-table**, **mac-filtering-table**, **spantree**.

Defaults

Areas are disabled for end-user profiles by default.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **no** form of the command to delete an end-user profile.
- An end-user profile may not be attached to a user that is already configured with functional privileges.
- If a profile is deleted, but the profile name is still associated with a user, the user will not be able to log into the switch.
- Use the **end-user profile port-list** and **end-user profile vlan-range** commands to configure ports and VLANs to which this profile will have access. By default, new profiles do not allow access to any ports or VLANs.

Examples

```
-> end-user profile bsmith read-only basic-ip-routing ip-routes-table
-> no end-user profile bsmith
```

Release History

Release 5.1; command was introduced.

Related Commands

end-user profile port-list	Configures a range of ports associated with an end-user profile.
end-user profile vlan-range	Configures a range of VLANs associated with an end-user profile.
user	Configures or modifies user entries in the local user database.
show end-user profile	Displays information about end-user profiles.

MIB Objects

```
endUserProfileTable
   endUserProfileName
   endUserProfileAreaPhysical
   endUserProfileAreaVlanTable
   endUserProfileAreaBasicIPRouting
   endUserProfileAreaIpRoutesTable
   endUserProfileAreaMacFilteringTable
   endUserProfileAreaSpantree
endUserProfileSlotPortTable
   endUserProfileSlotNumber
   endUserProfilePortList
endUserProfileVlanIdTable
   endUserProfileVlanIdStart
   endUserProfileVlandIdEnd
```

end-user profile port-list

Configures a range of ports associated with an end-user profile.

end-user profile *name* **port-list** *slot1***[**/*port_range1***] [***slot2***[**/*port_range2***] ...]**

end-user profile *name* **no port-list** *slot1* **[***slot2***...]**

Syntax Definitions

name	The name of an existing or a new end-user profile.
slot1	The slot number associated with the profile.
port_range1	The port or port range associated with slot1. Ports are separated by a hyphen, for example **2-4**.
slot2	Additional slots may be associated with the profile.
port_range2	Additional ports may be associated with additional slot numbers associated with the profile.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **no** form of the command to remove a port list or lists from an end-user profile. Note that the **no** form removes all the ports on a given slot or slots.

Examples

```
-> end user profile Prof1 port-list 2/1-3 3 4/1-5
-> end user profile Prof1 no port-list 4
```

Release History

Release 5.1; command was introduced.

Related Commands

end-user profile	Configures or modifies an end user profile, which specifies access to command areas.
end-user profile vlan-range	Configures a range of VLANs associated with an end-user profile.
show end-user profile	Displays information about end-user profiles.

MIB Objects

```
endUserProfileTable
   endUserProfileName
endUserProfileSlotPortTable
   endUserProfileSlotNumber
   endUserProfilePortList
```

end-user profile vlan-range

Configures a range of VLANs associated with an end-user profile.

end-user profile *name* **vlan-range** *vlan_range* **[***vlan_range2...***]**

end-user profile *name* **no vlan-range** *vlan1* **[***vlan2..***]**

Syntax Definitions

name	The name of an existing or a new end-user profile.
vlan_range	The VLAN range associated with the end-user profile; values are separated by a hyphen. For example: **3-6** indicates VLAN 3, VLAN 4, VLAN 5, and VLAN 6.
vlan_range2...	Optional additional VLAN ranges associated with the end-user profile. Up to 16 ranges total may be configured.
vlan1	The VLAN range to be deleted from the profile. Only the start of the range may be entered.
vlan2...	Additional VLAN ranges to be deleted. Only the start of the range may be entered.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **no** form of the command to remove a VLAN range or ranges from an end-user profile. Note that only the start of the VLAN range must be entered to remove the range.

Examples

```
-> end-user profile Prof1 vlan-range 2-4 7-8
-> end-user profile Prof1 no vlan-range 7
```

Release History

Release 5.1; command was introduced.

Related Commands

end-user profile	Configures or modifies an end user profile, which specifies access to command areas.
end-user profile port-list	Configures a range of ports associated with an end-user profile.
show end-user profile	Displays information about end-user profiles.

MIB Objects

```
endUserProfileTable
   endUserProfileName
endUserProfileVlanIdTable
   endUserProfileVlanIdStart
   endUserProfileVlandIdEnd
```

show aaa server

Displays information about a particular AAA server or AAA servers.

show aaa server [*server_name***]**

Syntax Definitions

server_name	The server name, which is defined through the **aaa radius-server** or **aaa ldap-server** commands or automatically set as **ace** for ACE servers.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- If you do not include a server name in the syntax, information for all servers displays.
- To display information about an ACE server, use **ace** as the *server_name*. Information for ACE is only available if ACE is specified for Authenticated Switch Access through the **aaa authentication** command.

Examples

```
-> show aaa server
Server name = ldap2
   Server type         = LDAP,
   Host name 1         = ors40535,
   Retry number        = 3,
   Timeout (in sec)    = 2,
   Port                = 389,
   Domain name         = manager,
   Search base         = c=us,
Server name = rad1
   Server type         = RADIUS,
   IP Address 1        = 10.10.2.1,
   IP Address 2        = 10.10.3.5,
   Retry number        = 3,
   Timeout (in sec)    = 2,
   Authentication port = 1645,
   Accounting port     = 1646
```

```
-> show aaa server ldap2
Server name = ldap2
   Server type         = LDAP,
   Host name 1         = ors40535,
   Retry number        = 3,
   Timeout (in sec)    = 2,
   Port                = 389,
   Domain name         = manager,
   Search base         = c=us,
```

RADIUS and LDAP parameters are configured through the **aaa radius-server** and **aaa ldap-server** commands. Parameters for the ACE server are automatically set by the switch.

output definitions

Server name	The name of the server. The switch automatically assigns “ace” to an ACE server. A RADIUS or LDAP server name is defined through the **aaa radius-server** and **aaa ldap-server** commands respectively.
Server type	The type of server (ACE, LDAP, or RADIUS).
Host name	The name of the primary LDAP or RADIUS host.
`IP address`	The IP address(es) of the server.
Retry number	The number of retries the switch makes to authenticate a user before trying the backup server.
Timeout	The timeout for server replies to authentication requests.
Port	The port number for the primary LDAP server.
Domain name	The super-user or administrative distinguished name in the format recognized by the LDAP-enabled directory servers.
Search base	The search base recognized by the LDAP-enabled directory servers.
Authentication port	The UDP destination port for authentication requests.
`Accounting port`	The UDP destination port for accounting requests.

Release History

Release 5.1; command was introduced.

Related Commands

aaa radius-server	Configures or modifies a RADIUS server for authenticated VLANs or Authenticated Switch Access.
aaa ldap-server	Configures or modifies an LDAP server for authenticated VLANs or Authenticated Switch Access.

MIB Objects

```
aaaServerTable
   aaasHostName
   aaasIpAddress
   aaasHostName2
   aaasIpAddress2
   aaasRadKey
   aaasRetries
   aaasTimout
   aaasRadAuthPort
   aaasRadAcctPort
   aaasLdapPort
   aaasLdapDn
   aaasLdapPasswd
   aaasLdapSearchBase
   AaasLdapServType
   aaasLdapEnableSsl
```

show aaa authentication vlan

Displays information about authenticated VLANs and the authentication server configuration.

show aaa authentication vlan

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **show aaa authentication vlan** command to display information about authentication servers configured in single mode or for authentication servers configured for each VLAN for authentication in multiple mode.

Examples

```
-> show aaa authentication vlan
Authenticated vlan = 23,
   1rst authentication server  = radius1,
   2nd authentication server   = ldap3
Authenticated vlan = 24,
   1rst authentication server  = radius1,
   2nd authentication server   = ldap3.
Authenticated vlan = 25,
   1rst authentication server  = radius1,
   2nd authentication server   = ldap3
Authenticated vlan = 26,
   1rst authentication server  = radius1,
   2nd authentication server   = ldap3
Authenticated vlan = 33,
   1rst authentication server  = radius1
   2nd authentication server   = ldap3
```

output definitions

Authenticated vlan	The VLAN number.
1st authentication server	The first server to be polled for authentication information.
2nd authentication server	The next server to be polled for authentication information.

Release History

Release 5.1; command was introduced.

Related Commands

aaa authentication vlan single-mode	Specifies the AAA servers to be used in single-authority mode for Layer 2 Authentication.
aaa authentication vlan multiple-mode	Specifies the AAA servers to be used in multiple-authority mode for authenticated VLANs.

MIB Objects

```
aaaAuthVlanTable
   aaatvName1
   aaatvName2
   aaatvName3
   aaatvName4
```

show aaa authentication

Displays information about the current authenticated switch session.

show aaa authentication

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **show aaa authentication** command to display authentication information about switch management services (Telnet, FTP, console port, Secure Shell, etc.).

Examples

```
-> show aaa authentication
Service type = Default
   1rst authentication server  = RadiusServer
   2nd authentication server   = local
Service type = Console
   1rst authentication server  = local
Service type = Telnet
   Authentication = Use Default,
   1rst authentication server  = RadiusServer
   2nd authentication server   = local
Service type = FTP
   Authentication = Use Default,
   1rst authentication server  = RadiusServer
   2nd authentication server   = local
Service type = Http
   Authentication = Use Default,
   1rst authentication server  = RadiusServer
   2nd authentication server   = local
Service type = Snmp
   Authentication = Use Default,
   1rst authentication server  = RadiusServer
   2nd authentication server   = local
Service type = Ssh
   Authentication = Use Default,
   1rst authentication server  = RadiusServer
   2nd authentication server   = local
```

output definitions

Authentication	Displays **denied** if the management interface is disabled. Displays **Use Default** if the management interface is configured to use the default configuration.
1st authentication server	The first server to be polled for authentication information.
2nd authentication server	The next server to be polled for authentication information.

Release History

Release 5.1; command was introduced.

Related Commands

aaa authentication	Configures the interface for Authenticated Switch Access and specifies the server(s) to be used.

MIB Objects

```
aaaAuthSATable
   aaatsName1
   aaatsName2
   aaatsName3
   aaatsName4
```

show aaa authentication 802.1x

Displays information about the global 802.1X configuration on the switch.

show aaa authentication 802.1x

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This command displays information about 802.1X settings configured through the **aaa authentication 802.1x** command.

Examples

```
-> show aaa authentication 802.1x
1rst authentication server = nms-avlan-30,
port usage                 = unique
```

output definitions

1st authentication server	The first server to be polled for authentication information. Any backup servers are also displayed on subsequent lines.
port usage	Whether 802.1X ports on the switch will only accept frames from the supplicant's MAC address after successful authentication (**unique**); or the switch will accept any frames on 802.1X ports after successful authentication (**global**)

Release History

Release 5.1; command was introduced.

Related Commands

aaa authentication 802.1x	Enables/disables the switch for 802.1X authentication.

MIB Objects

```
AaaAuth8021XTable
   aaatxName1
   aaatxName2
   aaatxName3
   aaatxName4
   aaatxOpen
```

show aaa authentication mac

Displays a list of RADIUS servers configured for MAC based authentication.

show aaa authentication mac

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This command displays MAC authentication servers configured through the **aaa authentication mac** command.

Examples

```
-> show aaa authentication mac
1rst authentication server = rad1,
```

output definitions

1st authentication server	The first server to be polled for authentication information. Any backup servers are also displayed on subsequent lines.

Release History

Release 5.4.1; command was introduced.

Related Commands

aaa authentication mac	Enables/disables the switch for MAC based authentication.

MIB Objects

```
AaaAuthMACTable
   aaaMacSrvrName1
   aaaMacSrvrName2
   aaaMacSrvrName3
   aaaMacSrvrName4
```

show aaa accounting 802.1x

Displays information about accounting servers for 802.1X sessions.

show aaa authentication 802.1x

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Accounting servers are configured through the **aaa radius-server** and **aaa ldap-server** commands.

Examples

```
-> show aaa accounting 802.1x
1rst authentication server = onyx,
2nd accounting server      = odyssey
3rd accounting server      = local
```

output definitions

1st authentication server	The first server to be polled for accounting of 802.1X sessions. Any backup servers are also displayed on subsequent lines.

Release History

Release 5.1; command was introduced.

Related Commands

aaa accounting 802.1x	Enables/disables accounting for 802.1X authentication sessions.

MIB Objects

```
AaaAcct8021XTable
   aaacxName1
   aaacxName2
   aaacxName3
   aaacxName4
```

show aaa accounting vlan

Displays information about accounting servers configured for authenticated VLANs. Accounting servers keep track of network resources (time, packets, bytes, etc.) and user activity.

show aaa accounting vlan

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **show aaa accounting vlan** command to display accounting information for all servers configured for authenticated VLANs.

Examples

```
-> show aaa accounting vlan
Authenticated vlan = 23,
   1rst accounting server      = RadiusServer
   2nd accounting server       = local
Authenticated vlan = 24,
   1rst accounting server      = RadiusServer,
   2nd accounting server       = local
Authenticated vlan = 25,
   1rst accounting server      = RadiusServer,
   2nd accounting server       = local
Session (telnet, ftp,...),
   1rst accounting server      = RadiusServer,
   2nd accounting server       = local
```

output definitions

`Authenticated vlan`	Indicates servers for authenticated VLANs.
Session	Indicates servers for Authenticated Switch Access session.
1st authentication server	The first server to be polled for authentication information.
2nd authentication server	The next server to be polled for authentication information.

Release History

Release 5.1; command was introduced.

Related Commands

aaa accounting vlan	Specifies an accounting server or servers to be used for authenticated VLANs.

MIB Objects

```
aaaAcctVlanTable
   aaacvName1
   aaacvName2
   aaacvName3
   aaacvName4
```

show aaa accounting

Displays information about accounting servers configured for authenticated VLANs, Authenticated Switch Access, and 802.1X port-based network access control. Accounting servers keep track of network resources (time, packets, bytes, etc.) and user activity.

show aaa accounting

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the **show aaa accounting** command to dis7play accounting servers configured for management session types (Telnet, FTP, console port, HTTP, or SNMP) and 802.1X port-based network access control.

Examples

```
-> show aaa accounting
Authenticated vlan = 23,
   1rst accounting server      = RadiusServer
   2nd accounting server       = local
Authenticated vlan = 24,
   1rst accounting server      = RadiusServer,
   2nd accounting server       = local
Authenticated vlan = 25,
   1rst accounting server      = RadiusServer,
   2nd accounting server       = local
Session (telnet, ftp,...),
   1rst accounting server      = RadiusServer,
   2nd accounting server       = local
```

output definitions

`Authenticated vlan`	Indicates servers for authenticated VLANs.
Session	Indicates servers for Authenticated Switch Access session.
1st authentication server	The first server to be polled for authentication information.
2nd authentication server	The next server to be polled for authentication information.

Release History

Release 5.1; command was introduced.

Related Commands

aaa accounting session	Configures accounting servers for Authenticated Switch Access sessions.
aaa accounting 802.1x	Enables/disables accounting for 802.1X authentication sessions.

MIB Objects

```
aaaAcctSATable
   aaacsName1
   aaacsName2
   aaacsName3
   aaacsName4
```

show user

Displays information about all users or a particular user configured in the local user database on the switch.

show user [*username***]**

Syntax Definitions

username	The name of the user. Used for logging into the switch.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use this command to display information about read/write access and partitioned management access (domains and families) or end-user profiles associated with users.

Examples

```
-> show user
User name = Customer1
   Password expiration     = none,
   END user profile        = Profile1
   SNMP authentication     = NONE, Snmp encryption = NONE
User name = admin
   Password expiration     = none,
   Read Only for domains   = All ,
   Read/Write for domains  = All ,
   Snmp not allowed.
User name = public
   Password expiration     = none,
   Read Only for domains   = All ,
   Read/Write for domains  = All ,
   Snmp authentication     = NONE, SNMP encryption = NONE
User name = jennifer
   Password expiration     = 1/4/1970 1:19 (3 days from now)
   Read Only for domains   = ,
   Read only for families  = avlan ,
   Read/Write for families = qos ,
   Snmp authentication     = NONE, Snmp encryption = NONE
User name = tbertovic
   Password expiration     = none,
   Read Only for domains   = None,
   Read/Write for domains  = Policy ,
   Snmp authentication     = MD5, Snmp encryption = DES
```

output definitions

END user profile	The name of an end-user profile associated with the user.
Password expiration	The date and time on which the password will expire. This field only displays if the password expiration is configured specifically for a user, or a default password expiration is configured globally on the switch through the **user password-expiration** command. (Note that the date/time are based on the switch's default system date/time or the system date/time configured through the **system date** and **system time** commands.)
Read Only for domains	The command domains available with the user's read-only access. See the table on the next page for a listing of valid domains.
Read/Write for domains	The command domains available with the user's read-write access. See the table on the next page for a listing of valid domains.
Read Only for families	The command families available with the user's read-only access. See the table on the next page for a listing of valid families.
Read/Write for families	The command families available with the user's read-write access. See the table on the next page for a listing of valid families.
Snmp authentication	The level of SNMP authentication, if any, configured for the user.

Possible values for command domains and families are listed here:

Domain	Corresponding Families
domain-admin	file telnet dshell debug
domain-system	system aip snmp rmon webmgt config
domain-physical	chassis module interface pmm health
domain-network	ip rip ospf bgp vrrp ip-routing ipx ipmr ipms
domain-layer2	vlan bridge stp 802.1q linkagg ip-helper
domain-service	dns
domain-policy	qos policy slb
domain-security	session avlan aaa

Release History

Release 5.1; command was introduced.

Related Commands

user	Configures user entries in the local user database.

MIB Objects

```
aaaUserTable
   aaauReadRight
   aaauWriteRight
   aaauProfile
   aaauSnmpLevel
   aaauSnmpAuthkey
```

show user password-size

Displays the minimum number of characters that are required for a user password.

show user password-size

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use this command to display the current minimum number of characters required when configuring user passwords.

Examples

```
-> show user password-size
password, minimum size 9
```

Release History

Release 5.1; command was introduced.

Related Commands

user	Configures or modifies user entries in the local user database.
password	Configures the current user's password.

MIB Objects

```
aaaAsaConfig
   aaaAsaPasswordSizeMin
```

show user password-expiration

Displays the expiration date for passwords configured for user accounts stored on the switch.

show user password-expiration

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This command displays the default password expiration, which is configured through the **user password-expiration** command.

Examples

```
-> show user password-expiration
User password expiration is set to 3 days.
```

Release History

Release 5.1; command was introduced.

Related Commands

user password-expiration	Configures an expiration date for user passwords stored locally on the switch or disables password expiration.
user	Configures or modifies user entries in the local user database.
password	Configures the current user's password.

MIB Objects

```
aaaAsaConfig
   aaaAsaDefaultPasswordExpirationInDays
```

show avlan user

Displays MAC addresses for authenticated VLAN users on the switch.

show avlan user [vlan *vlan_id* **| slot** *slot***]**

Syntax Definitions

vlan_id	The VLAN number. Information displays about users in this VLAN.
slot	The slot number. Information displays about users with access on this slot.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Information may be displayed for all users or for users associated with a particular VLAN or slot.

Examples

```
-> show avlan user
name                 Mac Address          Slot    Port    Vlan
-----------------------------------------------------------------
user0                27:bc:86:90:00:00    02      02      23
user1                27:bc:86:90:00:01    02      03      12
user2                27:bc:86:90:00:02    02      05      15
user3                27:bc:86:90:00:03    04      09      10
user4                27:bc:86:90:00:04    03      02      23

-> show avlan user 23
name                 Mac Address          Slot    Port    Vlan
-----------------------------------------------------------------
avlan_0              27:bc:86:90:00:00    02      02      23
```

output definitions

name	The name of the authenticated user.
Mac Address	The MAC address of the user.
Slot	The slot associated with the user.
Port	The port associated with the user.
Vlan	The VLAN into which the user is authenticated.

Release History

Release 5.1; command was introduced.

Related Commands

aaa vlan no	Deletes a particular authenticated VLAN user from the configuration.

MIB Objects

```
aaaAuthenticatedUserTable
   aaaaMacAddress
   aaaaSlot
   aaaaPort
   aaaaVlan
```

show aaa avlan config

Displays the current global configuration parameters for authenticated VLANs.

show aaa avlan config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use this command to display DNS or DHCP information for authenticated VLANs.

Examples

```
-> show aaa avlan config
default DHCP relay address = 192.9.33.222
authentication DNS name    = authent.company.com
default traffic            = disabled
port bounding              = disabled
```

output definitions

default DHCP relay address	The gateway address of the DHCP server; configured through the **aaa avlan default dhcp** command.
authentication DNS name	The DNS host name, configured through the **aaa avlan dns** command.
default traffic	Whether or not the default VLAN is enabled for users to traffic in before authentication. Configured through the **avlan default-traffic** command.
port bounding	Whether or not port mobility rules are allowed on authenticated VLANs. Configured through the **avlan port-bound** command.

Release History

Release 5.1; command was introduced.

Related Commands

aaa avlan dns	Configures a host name.
aaa avlan default dhcp	Configures the gateway address for a DHCP server.
avlan default-traffic	Configures whether or not users are able to traffic in the default VLAN before they are actually authenticated.
avlan port-bound	Configures whether or not authenticated ports may use port mobility rules.

MIB Objects

```
aaaAvlanConfig
   aaaAvlanDnsName
   aaaAvlanDhcpDefGateway
   aaaAvlanDefaultTraffic
   aaaAvlanPortBound
```

show aaa avlan auth-ip

Displays the IP addresses for authenticated VLANs.

show aaa avlan auth-ip [vlan *vlan_id***]**

Syntax Definitions

vlan_id	The VLAN ID of the authenticated VLAN for which you want to display the authentication IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command displays all authenticated VLAN IP addresses unless a specific VLAN is requested with the **vlan** keyword and the relevant *vlan_id*.
- The IP addresses for authenticated VLANs is set automatically by the switch (based on the VLAN router port ID) or by the user through the **avlan auth-ip** command.

Examples

```
-> show aaa avlan auth-ip
Vlan number  Authenticated Ip Address
-------------+-----------------------
2     10.10.2.3
4     12.13.14.253

-> show aaa avlan auth-ip vlan 2
Vlan number  Authenticated Ip Address
-------------+-----------------------
2     10.10.2.3
```

output definitions

VLAN number	The VLAN ID.
Authenticated Ip Address	The IP address associated with the authenticated VLAN.

Release History

Release 5.1; command was introduced.

Related Commands

avlan auth-ip	Configures an IP address to be used for VLAN authentication.

MIB Objects

```
aaaAvlanConfigTable
   aaaAvlanAddress
```

debug command-info

Enables or disables the command information mode in the CLI. When this mode is enabled, any command entered on the command line will display information about the command rather than executing the command.

debug command-info {enable | disable}

Syntax Definitions

enable	Enables the debugging command information mode.
disable	Disables the debugging command information mode.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- When the mode is enabled, any command entered will result in output similar to the one shown in the Examples section below. Any commands entered when the mode is enabled are not executed. To return to normal operating mode, enter **debug command-info disable**.
- The command information mode is useful when setting privileges for users.

Examples

```
-> debug command-info enable
CLI command info mode on
-> vlan 2
PM family:  VLAN
R/W mode:   WRITE
-> ls
PM family:  SYSTEM
R/W mode:   READ
```

output definitions

PM family	The partitioned management (PM) command family to which the command belongs.
R/W mode	Whether the current command is a read-only or a write command.

Release History

Release 5.1; command was introduced.

Related Commands

user	Configures or modifies user entries in the local user database.

debug end-user profile

Use this command to display detailed information about profiles or a particular profile.

debug end-user profile *name*

Syntax Definitions

name	The name of the end-user profile, configured through the **end-user profile** command.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **show end-user profile** command to display basic information about end-user profiles.
- If a particular profile is specified, information will be displayed for the profile and for all indexes following that profile. (The index value is the way the switch internally tracks profiles and reflects the order in which profiles are created.)

Examples

```
-> debug end-user profile
End user profile : jentest, length : 7 for index : 1
  End user profile @0x5e781e8
  Read area rights : 3f
  Read and Write area rights : 0
  Physical area rights : 2
  vlan table area rights : 2
  Basic Ip routing area rights : 2
  Ip routes table area rights : 2
  Mac filtering table area rights : 2
  Spantree area rights : 2
  Slot 1, ports : 0 0 0 0
  Slot 2, ports : 0 0 0 0
  Slot 3, ports : 0 0 0 0
  Slot 4, ports : 0 0 0 0
  Slot 5, ports : 0 0 0 0
  Slot 6, ports : 0 0 0 0
  Slot 7, ports : 0 0 0 0
  Slot 8, ports : 0 0 0 0
  Slot 9, ports : 0 0 0 0
  Slot 10, ports : 0 0 0 0
  Slot 11, ports : 0 0 0 0
  Slot 12, ports : 0 0 0 0
  Slot 13, ports : 0 0 0 0
  Slot 14, ports : 0 0 0 0
  Slot 15, ports : 0 0 0 0
```

```
  Slot 16, ports : 0 0 0 0
  Vlan Id range number : 1
  Vlan range 1, start : 1, end : 3
End user profile not created for index : 2
End user profile not created for index : 3
End user profile not created for index : 4
End user profile not created for index : 5
End user profile not created for index : 6
End user profile not created for index : 7
End user profile not created for index : 8
End user profile not created for index : 9
End user profile not created for index : 10
.
.
.
.
```

Release History

Release 5.1; command was introduced.

Related Commands

end-user profile	Configures or modifies an end user profile, which specifies access to command areas on particular ports and VLANs.
show end-user profile	Displays information about end-user profiles or a particular end-user profile.

show end-user profile

Displays basic information about end-user profiles or a particular end-user profile.

show end-user profile *name*

Syntax Definitions

name	The name of the end-user profile (up to 32 alphanumeric characters).

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The **show end-user profile** command displays information about profiles configured on the switch. For information about users, use the **show user** command.
- If a particular profile is not specified, information about all profiles is displayed.

Examples

```
-> show end-user profile Prof1

End user profile : Prof1
  Area accessible with read and write rights :
    physical,
    vlan table,
    basic ip routing,
    ip routes table,
    mac filtering table,
    spantree
  Slot : 1, ports allowed : 1-2, 4-5, 7-8, 10-11, 13-14, 16-17, 19-20, 22-24
  Slot : 2, ports allowed : 1-2, 4-5, 7-8, 10-11, 13-14, 16-17, 19-20, 22-24
  Slot : 3, ports allowed : 1-2, 4-5, 7-8, 10-11, 13-14, 16-17, 19-20, 22-24
  Slot : 4, ports allowed : 1-2, 4-5, 7-8, 10-11, 13-14, 16-17, 19-20, 22-24
  Vlan Id :
   1-18,   23,   27-1001,   4073-4092
```

Release History

Release 5.1; command was introduced.

Related Commands

end-user profile	Configures or modifies an end user profile, which specifies access to command areas on particular ports and VLANs.
user	Configures or modifies user entries in the local user database.

MIB Objects

```
endUserProfileTable
   endUserProfileName
   endUserProfileAreaPhysical
   endUserProfileAreaVlanTable
   endUserProfileAreaBasicIPRouting
   endUserProfileAreaIpRoutesTable
   endUserProfileAreaMacFilteringTable
   endUserProfileAreaSpantree
endUserProfileSlotPortTable
   endUserProfileSlotNumber
   endUserProfilePortList
endUserProfileVlanIdTable
   endUserProfileVlanIdStart
   endUserProfileVlandIdEnd
```

show aaa priv hexa

Displays hexadecimal values for command domains/families. Useful for determining how to express command families in hexadecimal; hexadecimal values are used in configuring user privileges in attributes on an external LDAP or RADIUS authentication server.

show aaa priv hexa [*domain or family***]**

Syntax Definitions

domain or family	The CLI command domain or particular command family for which you want to display hexadecimal values. See table in Usage Guidelines.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Valid values for the family parameter are listed in the Corresponding Families column of the following table:

Domain	Corresponding Families
domain-admin	**file telnet dshell debug**
domain-system	**system aip snmp rmon webmgt config**
domain-physical	**chassis module interface pmm health**
domain-network	**ip rip ospf bgp vrrp ip-routing ipx ipmr ipms**
domain-layer2	**vlan bridge stp 802.1q linkagg ip-helper**
domain-service	**dns**
domain-policy	**qos policy slb**
domain-security	**session avlan aaa**

- Note that some command families may not be supported depending on the hardware platform you are running.
- If you do not specify a command family, hexadecimal values for all commands sets will display.

Examples

```
-> show aaa priv hexa
file            = 0x00000001 0x00000000,
telnet          = 0x00000008 0x00000000,
dshell          = 0x00000020 0x00000000,
debug           = 0x00000040 0x00000000,
domain-admin    = 0x00000069 0x00000000,
```

```
system          = 0x00000080 0x00000000,
aip             = 0x00000100 0x00000000,
snmp            = 0x00000200 0x00000000,
rmon            = 0x00000400 0x00000000,
webmgt          = 0x00000800 0x00000000,
config          = 0x00001000 0x00000000,
domain-system   = 0x00001F80 0x00000000,

chassis         = 0x00002000 0x00000000,
module          = 0x00004000 0x00000000,
interface       = 0x00008000 0x00000000,
pmm             = 0x00010000 0x00000000,
health          = 0x00040000 0x00000000,
domain-physical = 0x0005E000 0x00000000,

ip              = 0x00080000 0x00000000,
rip             = 0x00100000 0x00000000,
ospf            = 0x00200000 0x00000000,
bgp             = 0x00400000 0x00000000,
vrrp            = 0x00800000 0x00000000,
ip-routing      = 0x01000000 0x00000000,
ipx             = 0x02000000 0x00000000,
ipmr            = 0x04000000 0x00000000,
ipms            = 0x08000000 0x00000000,
domain-network  = 0x0FF80000 0x00000000,

vlan            = 0x10000000 0x00000000,
bridge          = 0x20000000 0x00000000,
stp             = 0x40000000 0x00000000,
802.1q          = 0x80000000 0x00000000,
linkagg         = 0x00000000 0x00000001,
ip-helper       = 0x00000000 0x00000002,
domain-layer2   = 0xF0000000 0x00000003,

dns             = 0x00000000 0x00000010,
domain-service  = 0x00000000 0x00000010,

qos             = 0x00000000 0x00000020,
policy          = 0x00000000 0x00000040,
slb             = 0x00000000 0x00000080,
domain-policy   = 0x00000000 0x000000E0,

session         = 0x00000000 0x00000100,
avlan           = 0x00000000 0x00000400,
aaa             = 0x00000000 0x00000800,
domain-security = 0x00000000 0x00000D00


-> show aaa priv hexa rip
0x00100000 0x00000000
```

Release History

Release 5.1; command was introduced.

Related Commands

user	Configures or modifies user entries in the local user database.

44 802.1X Commands

This chapter includes information about commands used for configuring and viewing port-specific 802.1X parameters. Included in this command set are specific commands used to configure Access Guardian policies (also referred to as device classification policies) for 802.1X ports.

Filename: AlcatelIND1Dot1x.mib
Module: ALCATEL-IND1-DOT1X-MIB

A summary of the available commands is listed here:

802.1X port commands	**802.1x** **802.1x initialize** **802.1x re-authenticate** **show 802.1x** **show 802.1x users** **show 802.1x statistics** **show 802.1x non-supp**
Access Guardian commands	**802.1x supplicant policy authentication** **802.1x non-supplicant policy authentication** **802.1x non-supplicant policy** **802.1x policy default** **show 802.1x device classification policies**

802.1x

Configures 802.1X parameters on a particular slot/port. Typically used for port access control on a dedicated 802.1X port.

802.1x *slot/port* **[direction {both | in}] [port-control {force-authorized | force-unauthorized | auto}] [quiet-period** *seconds***] [tx-period** *seconds***] [supp-timeout** *seconds***] [server-timeout** *seconds***] [max-req** *max_req***] [re-authperiod** *seconds***] [reauthentication | no reauthentication]**

Syntax Definitions

slot	The slot number of the 802.1X port.
port	The 802.1X port number.
both	Configures bidirectional control on the port.
in	Configures control over incoming traffic only.
force-authorized	Forces the port control to be authorized, which means that the port is open without restrictions and behaves as any other non-802.1X port. Devices do not need to authenticate to traffic through the port.
force-unauthorized	Forces the port control to be unauthorized, which means the port cannot accept any traffic.
auto	Configures the switch to dynamically control the port control status based on authentication exchanges between the 802.1X end station and the switch. Initially the port is in an unauthorized state; it becomes authorized if a device successfully completes an 802.1X authentication exchange with the switch.
quiet-period *seconds*	The time during which the port will not accept an 802.1X authentication attempt; the timer is activated after any authentication failure. During the time period specified, the switch will ignore and discard all Extensible Authentication Protocol over LAN (EAPOL) packets. The range is 0 to 65535 seconds.
tx-period *seconds*	The time before an EAP Request Identity will be re-transmitted. The range is 1 to 65535 seconds.
supp-timeout *seconds*	The number of seconds before the switch will time out an 802.1X user who is attempting to authenticate. The value should be modified to be a greater value if the authentication process will require additional steps by the user (for example, entering a challenge).
server-timeout *seconds*	The timeout for the authentication server for authentication attempts. This value is always superseded by the value configured for the RADIUS authentication server configured through the **aaa radius-server** command.
max_req	The maximum number of times the switch will retransmit a request for authentication information (request identity, password, challenge, etc.) to the 802.1X user before it times out the authentication session based on the **supp-timeout**. The range is 1 to 10.

re-authperiod *seconds*	The amount of time that must expire before the switch requires re-authentication of the Supplicant on this port. Only applicable when re-authentication is enabled.
reauthentication	Specifies that the port will be reauthenticated after the **re-authperiod** timer expires.
no reauthentication	Specifies that the port will not be reauthenticated unless the **802.1x re-authenticate** command is entered.

Defaults

parameter	default
both | in	both
force- authorized | force-unauthorized | auto	auto
quiet-period *seconds*	60
tx-period *seconds*	30
supp-timeout *seconds*	30
max_req	2
re-authperiod *seconds*	3600
reauthentication | no reauthentication	no reauthentication

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- To set the port to accept any traffic without requiring 802.1X authentication, use the **force-authorized** option.
- Use the **vlan port 802.1x** command with the **disable** option to disable 802.1X authentication on the port.
- Before any device is authenticated through an 802.1X port, the port will only process 802.1X frames (EAPoL frames) from an unknown source.
- Note that multiple devices can be authenticated on a given 802.1X port. Each device MAC address received on the port is authenticated and learned separately. Only those that authenticate successfully are allowed on the port, as described above. Those that fail authentication are blocked from accessing the 802.1X port.

Examples

```
-> 802.1x port 3/1 quiet-period 30
```

Release History

Release 5.1; command was introduced.

Related Commands

aaa authentication 802.1x	Specifies the RADIUS server to use for 802.1x authentication.
aaa authentication mac	Specifies the RADIUS server to use for MAC authentication.
vlan port 802.1x	Enables or disables 802.1X port-based access control on a mobile port.
show 802.1x	Displays information about ports configured for 802.1X.

MIB Objects

```
dot1xPaePortTable
   dot1xPaePortNumber
   dot1xPaePortInitialize
   dot1xPaePortReauthenticate
dot1xAuthConfigTable
   dot1xAuthAdminControlledDirections
   dot1xAuthOperControlledDirections
   dot1xAuthAuthControlledPortStatus
   dot1xAuthAuthControlledPortControl
   dot1xAuthQuitePeriod
   dot1xAuthTxPeriod
   dot1xAuthSuppTimeout
   dot1xAuthServerTimeout
   dot1xAuthMaxReq
   dot1xAuthReAuthPeriod
   dot1xAuthReAuthEnabled
```

802.1x initialize

Re-initializes a particular 802.1X port. Stops traffic on the port; then requires re-authentication of the port.

802.1x initialize *slot/port*

Syntax Definitions

slot	The slot number of the 802.1X port to be initialized.
port	The 802.1X port number.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command is typically only used for troubleshooting, to reset the port access control mechanism in the switch.
- When this command is entered, all traffic on the port is stopped; the port is then re-authenticated. Connectivity is restored with successful re-authentication.

Examples

```
-> 802.1x initialize 3/1
```

Release History

Release 5.1; command was introduced.

Related Commands

802.1x	Configures 802.1X parameters on a particular slot/port.

MIB Objects

```
dot1xPaePortTable
   dot1xPaePortInitialize
```

802.1x re-authenticate

Forces a particular 802.1X port to be re-authenticated.

802.1x reauthenticate *slot/port*

Syntax Definitions

slot	The slot number of the 802.1x port to be initialized.
port	The 802.1x port number.

Defaults

By default, 802.1X ports are not configured for periodic re-authentication. Use the **802.1x re-authenticate** command to force a re-authentication.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command forces a port to be re-authenticated, regardless of the re-authentication setting configured for the **802.1x** command.
- Re-authentication is transparent to the user. It does not affect traffic on the port unless there is a problem with the physical device connected to the port. The re-authentication mechanism verifies that there is a device connected to the port, and that the authentication exchange is still valid.

Examples

```
-> 802.1x reauthenticate 3/1
```

Release History

Release 5.1; command was introduced.

Related Commands

802.1x	Configures 802.1X parameters on a particular slot/port.

MIB Objects

```
dot1xPaePortTable
   dot1xPaePortReauthenticate
```

802.1x supp-polling retry

Configures the number of times to poll a device for EAP frames to determine whether or not the device is an 802.1x client.

802.1x *slot/port* **supp-polling retry** *retries*

Syntax Definitions

slot	The slot number of the 802.1x port.
port	The 802.1x port number.
retries	The number of times a device is polled for EAP frames (1–99).

Defaults

By default, the number of retries is set to 2.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guideline

- The polling interval is 0.5 seconds between each retry.
- If no EAP frames are received from a device connected to an 802.1x port, the device is considered a non-802.1x client (non-supplicant).
- If a guest VLAN is configured on the 802.1x port, the non-802.1x client is assigned to the guest VLAN. If a guest VLAN does not exist, the device is blocked from accessing the 802.1x port.

Examples

```
-> 802.1x 3/1 supp-polling retry 5
-> 802.1x 3/1 supp-polling retry 10
```

Release History

Release 5.1.6; command was introduced.

Related Commands

show 802.1x	Displays information about ports configured for 802.1X.
show 802.1x non-supp	Displays a list of all non-802.1x supplicants learned on all 802.1x ports.

MIB Objects

```
alaDot1xSuppPollingCnt
```

802.1x supplicant policy authentication

Configures a supplicant device classification policy for an 802.1x port. This type of policy uses 802.1x authentication via a remote RADIUS server. A supplicant is any device that uses the 802.1x protocol for authentication.

802.1x *slot/port* **supplicant policy authentication [[pass] {group-mobility | vlan** *vid* **| default-vlan | block}...] [[fail] {vlan** *vid* **| block}...]**

Syntax Definitions

slot/port	The slot and port number of the 802.1x port.
pass	Indicates which policies to apply if 802.1x authentication is successful but does not return a VLAN ID.
fail	Indicates which policies to apply if 802.1x authentication fails or if successful authentication returns a VLAN ID that does not exist.
group-mobility	Use Group Mobility rules for device classification.
vlan *vid*	Use this VLAN ID number for device classification.
default-vlan	Assign supplicant to the default VLAN for the 802.1x port.
block	Block supplicant access on the 802.1x port.

Defaults

parameter	default
pass	block
fail	block

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use this command to configure alternative device classification methods when successful 802.1x authentication *does not* return a VLAN ID, returns a VLAN ID that does not exist, or authentication fails.
- When authentication does return a VLAN ID that exists in the switch configuration, the supplicant is assigned to that VLAN and no further classification is performed.
- If this command is used without specifying any of the optional policy keywords or a **pass**/**fail** parameter (e.g. **802.1x 1/10 supplicant authentication**), the resulting policy will block supplicants if successful 802.1x authentication *does not* return a VLAN ID, returns a VLAN ID that does not exist, or authentication fails.

- When multiple parameters are configured, the policy is referred to as a compound supplicant policy. Such policies use the **pass** and **fail** parameters to specify which policies to use when 802.1x authentication is successful and which to use when it fails.
- The **pass** keyword is implied and therefore an optional keyword. If the **fail** keyword is not used, the default action is to block the device when authentication fails.
- The order in which parameters are specified determines the order in which they are applied. However, this type of policy must end with either the **default-vlan** or **block** parameters, referred to as terminal parameters (or policies).
- Configuring supplicant classification policies is only supported on 802.1x enabled mobile ports.
- Each 802.1x port can have one supplicant policy and one non-supplicant policy for handling 802.1x and non-802.1x devices, respectively. Configuring a new supplicant or non-supplicant policy overwrites any policies that may already exist for the port.
- If a user-defined supplicant policy does not exist for the 802.1x port, then by default 802.1x attempts to use Group Mobility to classify a supplicant when successful authentication does not return a VLAN ID. If classifying the supplicant with Group Mobility fails, then the supplicant is assigned to the default VLAN for the port. If successful authentication returns a VLAN ID that does not exist or authentication fails, the supplicant is blocked. All non-supplicants are automatically blocked.

Examples

```
-> 802.1x 3/1 supplicant policy authentication
-> 802.1x 4/1 supplicant policy authentication vlan 27 default-vlan
-> 802.1x 5/10 supplicant policy authentication pass group-mobility default-vlan
fail vlan 43 block
```

Release History

Release 5.4.1; command was introduced.

Related Commands

802.1x non-supplicant policy authentication	Configures MAC authentication device classification policies for non-supplicants.
802.1x non-supplicant policy	Configures device classification policies that do not perform 802.1x or MAC authentication for non-supplicants.
802.1x policy default	Resets the device classification policy to the default policy value for the 802.1x port.
show 802.1x device classification policies	Displays device classification policies configured for an 802.1x port.
show 802.1x non-supp	Displays a list of all non-supplicants learned on all 802.1x ports.

MIB Objects

```
alaDot1xAuthPolicyTable
   alaDot1xSuppPolicy
```

802.1x non-supplicant policy authentication

Configures a non-supplicant classification policy for an 802.1x port. This type of policy uses MAC authentication via a remote RADIUS server. A non-supplicant is a device that does not support using the 802.1x protocol for authentication.

802.1x *slot/port* **non-supplicant policy authentication [[pass] {group-mobility | vlan** *vid* **| default-vlan | block}] [[fail] {group-mobility | vlan** *vid* | **default-vlan | block}]**

Syntax Definitions

slot/port	The slot and port number of the 802.1x port.
pass	Indicates which policies to apply if MAC authentication is successful but does not return a VLAN ID or the VLAN ID returned does not exist.
fail	Indicates which policies to apply if MAC authentication fails.
group-mobility	Use Group Mobility rules for device classification.
vlan *vid*	Use this VLAN ID number for device classification.
default-vlan	Assign supplicant to the default VLAN for the 802.1x port.
block	Block supplicant traffic on the 802.1x port.

Defaults

By default no device classification policies are configured for an 802.1x port.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use this command to configure alternative device classification policies when a successful MAC authentication *does not* return a VLAN ID, returns a VLAN ID that does not exist, or when MAC authentication fails.
- When MAC authentication does return a VLAN ID that exists in the switch configuration, the supplicant is assigned to that VLAN and no further classification is performed.
- When multiple parameters are configured, the policy is referred to as a compound non-supplicant policy. Such policies use the **pass** and **fail** parameters to specify which policies to use when MAC authentication is successful and which to use when it fails.
- The **pass** keyword is implied and therefore an optional keyword. If the **fail** keyword is not used, the default action is to block the device when authentication fails.
- The order in which the parameters are specified with this command determines the order in which they are applied. However, this type of policy must end with either the **default-vlan** or **block** parameters, referred to as terminal parameters (or policies). This applies to both pass and fail policies.
- Configuring non-supplicant classification policies is only supported on 802.1x enabled mobile ports.

- Each 802.1x port can have one supplicant policy and one non-supplicant policy for handling 802.1x and non-802.1x devices, respectively. Configuring a new supplicant or non-supplicant policy over-writes any policies that may already exist for the port.
- Note that if there are no device classification policies configured for an 802.1x-enabled port, then non-supplicants are automatically blocked from accessing the port.

Examples

```
-> 802.1x 3/1 non-supplicant policy authentication
-> 802.1x 4/1 non-supplicant policy authentication pass group-mobility fail
default-vlan
-> 802.1x 5/10 non-supplicant policy authentication vlan 27 fail vlan 500 default-
vlan
-> 802.1x 2/1 non-supplicant policy authentication vlan 10 default-vlan
```

Release History

Release 5.4.1; command was introduced.

Related Commands

802.1x supplicant policy authentication	Configures 802.1x authentication device classification policies for supplicants.
802.1x non-supplicant policy	Configures device classification policies that do not perform 802.1x or MAC authentication for non-supplicants.
802.1x policy default	Resets the device classification policy to the default policy value for the 802.1x port.
show 802.1x device classification policies	Displays device classification policies configured for an 802.1x port.
show 802.1x non-supp	Displays a list of all non-supplicants learned on all 802.1x ports.

MIB Objects

```
alaDot1xAuthPolicyTable
   alaDot1xNonSuppPolicy
```

802.1x non-supplicant policy

Configures a non-supplicant device classification policy for an 802.1x port. This type of policy does not perform any authentication. A non-supplicant is a device that does not support using the 802.1x protocol for authentication.

802.1x *slot/port* **non-supplicant policy {group-mobility | vlan** *vid* **| default-vlan | block}**

Syntax Definitions

slot/port	The slot and port number of the 802.1x port.
group-mobility	Use Group Mobility rules for device classification.
vlan *vid*	Use this VLAN ID number for device classification.
default-vlan	Assign supplicant to the default VLAN for the 802.1x port.
block	Block supplicant traffic on the 802.1x port.

Defaults

By default no device classification policies are configured for an 802.1x port.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- When multiple parameters are configured, the policy is referred to as a compound non-supplicant policy. The order in which the parameters are specified determines the order in which they are applied. However, this type of policy must end with either the **default-vlan** or **block** parameters, referred to as terminal parameters (or policies).
- Because this policy does not use 802.1x or MAC authentication, non-supplicants are only classified for assignment to non-authenticated VLANs.
- Note that if a non-supplicant policy is not configured for an 802.1x port, then non-supplicants are automatically blocked from accessing the port.
- Configuring non-supplicant classification policies is only supported on 802.1x enabled mobile ports.
- Each 802.1x port can have one supplicant policy and one non-supplicant policy for handling 802.1x and non-802.1x devices, respectively. Configuring a new supplicant or non-supplicant policy overwrites any policies that may already exist for the port.

Examples

```
-> 802.1x 4/1 non-supplicant policy group-mobility default-vlan
-> 802.1x 5/10 non-supplicant policy vlan 500 block
-> 8022.1x 6/1 non-supplicant policy group-mobility vlan 247 block
```

Release History

Release 5.4.1; command was introduced.

Related Commands

802.1x supplicant policy authentication	Configures 802.1x authentication device classification policies for supplicants.
802.1x non-supplicant policy authentication	Configures MAC authentication device classification policies for non-supplicants.
802.1x policy default	Resets the device classification policy to the default policy value for the 802.1x port.
show 802.1x device classification policies	Displays device classification policies configured for an 802.1x port.
show 802.1x non-supp	Displays a list of all non-supplicants learned on all 802.1x ports.

MIB Objects

```
alaDot1xAuthPolicyTable
   alaDot1xNonSuppPolicy
```

802.1x policy default

Resets the device classification policy to the default value for the 802.1x port.

802.1x *slot/port* **{supplicant | non-supplicant} policy default**

Syntax Definitions

slot/port	The slot and port number of the 802.1x port.
supplicant	Reset the supplicant policy to the default policy value.
non-supplicant	Reset the non-supplicant policy to the default policy value.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- The default non-supplicant policy blocks all non-supplicants from accessing the 802.1x port.
- The default supplicant policy blocks supplicants that fail authentication. If authentication is successful but does not return a VLAN ID, then Group Mobility rules are examined. If no rules exist or match supplicant traffic, then the supplicant is assigned to the default VLAN for the 802.1x port.

Examples

```
-> 802.1x 3/1 supplicant policy default
-> 802.1x 4/1 non-supplicant policy default
```

Release History

Release 5.4.1; command was introduced.

Related Commands

802.1x supplicant policy authentication	Configures 802.1x authentication device classification policies for supplicants.
802.1x non-supplicant policy authentication	Configures MAC authentication device classification policies for non-supplicants.
802.1x non-supplicant policy	Configures device classification policies that do not perform 802.1x or MAC authentication for non-supplicants.
show 802.1x device classification policies	Displays device classification policies configured for an 802.1x port.
show 802.1x non-supp	Displays a list of all non-supplicants learned on all 802.1x ports.

MIB Objects

```
alaDot1xAuthPolicyTable
   alaDot1xSuppPolicy
```

show 802.1x

Displays information about ports configured for 802.1X.

show 802.1x [*slot/port***]**

Syntax Definitions

slot	The slot of the port for which you want to display information.
port	The port for which you want to display 802.1X information.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

If you do not specify a particular slot/port, information for all 802.1X ports is displayed.

Examples

```
-> show 802.1x 1/13

802.1x configuration for slot 1 port 13:

  direction                   = both,
  operational directions      = both,
  port-control                = auto,
  quiet-period (seconds)      = 60,
  tx-period (seconds)         = 30,
  supp-timeout (seconds)      = 30,
  server-timeout (seconds)    = 30,
  max-req                     = 2,
  re-authperiod (seconds)     = 3600,
  reauthentication            = no
  Supplicant polling retry count = 2
```

output definitions

`direction`	Whether the port is configured for control on bidirectional traffic or incoming traffic only. May be configured through the **802.1x** command. Possible values are **both** or **in**.
`operational directions`	The operational state of controlled direction on the port, which is set automatically by the switch. If the value of **direction** is **both**, the value of operational directions is **both**. If the value of **direction** is **in**, the operational state is set to **in** on initialization and when the port's MAC address becomes operable. If the port's MAC address becomes inoperable, the operational direction is set to **both**.

output definitions (continued)

`port-control`	The value of the port control parameter for the port (**auto**, **force-authorized**, or **force-unauthorized**), which is set through the **802.1x** command.
`quiet-period`	The time during which the port will not accept an 802.1X authentication attempt; the timer is activated after any authentication failure. The range is 0 to 65535 seconds.
`tx-period`	The time before an EAP Request Identity will be transmitted. The range is 1 to 65535 seconds.
`supp-timeout`	The number of seconds before the switch will time out an 802.1x user who is attempting to authenticate.
`server-timeout`	The timeout for the authentication server for authentication attempts. This value is always superseded by the value configured for the RADIUS authentication server configured through the **aaa radius-server** command.
`max-req`	The maximum number of times the switch will retransmit a request for authentication information (request identity, password, challenge, etc.) to the 802.1X user before it times out the authentication session based on the **supp-timeout**. The range is 1 to 10.
`re-authperiod`	The amount of time that must expire before the switch requires re-authentication of the Supplicant on this port. Only applicable when re-authentication is enabled.
`reauthentication`	Whether or not the port will be re-authenticated after the re-authperiod expires.
Supplicant polling retry count	The number of times a device is polled for EAP frames to determine whether or not the device is an 802.1x client. Configured through the **802.1x supp-polling retry** command.

Release History

Release 5.1; command was introduced.
Release 5.1.6 and 5.4.1; command output modified.

Related Commands

802.1x	Configures 802.1X parameters on a particular slot/port.
802.1x supp-polling retry	Configures the number of times to poll a device for EAP frames to determine whether or not the device is an 802.1x client.

MIB Objects

```
dot1xAuthConfigTable
   dot1xAuthAdminControlledDirections
   dot1xAuthOperControlledDirections
   dot1xAuthAuthControlledPortControl
   dot1xAuthQuietPeriod
   dot1xAuthTxPeriod
   dot1xAuthSuppTimeout
   dot1xAuthServerTimeout
   dot1xAuthMaxReq
   dot1xAuthReAuthPeriod
   dot1xAuthReAuthEnabled
   alaDot1xSuppPollingCnt
```

show 802.1x users

Displays a list of all users for one or more 802.1X ports.

show 802.1x users [*slot/port***]**

Syntax Definitions

slot	The slot of the port for which you want to display information.
port	The port for which you want to display 802.1X information.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

If you do not specify a particular slot/port, all users associated with 802.1X ports are displayed.

Examples

```
->show 802.1x users

Slot  MAC               Port                          User
Port  Address           State                Policy   Name
-----+-----------------+--------------------+---------+-----------------
3/1   00:60:4f:11:22:33  Authenticated        VLAN ID   user50
3/1   00:60:4f:44:55:66  Authenticated        VLAN ID   user51
3/1   00:60:4f:77:88:99  Authenticated        VLAN ID   user52
3/3   00:60:22:15:22:33  Force-authenticated  N/A
3/3   00:60:22:44:75:66  Force-authenticated  N/A
3/3   00:60:22:37:98:09  Force-authenticated  N/A

->show 802.1x users 3/1

Slot  MAC               Port                          User
Port  Address           State                Policy   Name
-----+-----------------+--------------------+---------+-----------------
3/1   00:60:4f:11:22:33  Connecting           VLAN ID   user50
3/1   00:60:4f:44:55:66  Held                 VLAN ID   user51
3/1   00:60:4f:77:88:99  Authenticated        VLAN ID   user52
```

output definitions

Slot/Port	The 802.1X slot and port number that provides access to the user.
MAC Address	The source MAC address of the 802.1X user.

output definitions (continued)

`Port State`	The current state of the 802.1X port for a specific user: • **Initialize** • **Disconnected** • **Connecting** • **Authenticating** • **Authenticated** • **Aborting** • **Held** • **Force-Authenticated** • **Force-Unauthenticated**
Policy	The 802.1x device classification policy that was applied to the device.
`User Name`	The user name that is used for authentication.

Release History

Release 5.1.6; command was introduced.
Release 5.4.1: **policy** field added.

Related Commands

802.1x	Configures 802.1X parameters on a particular slot/port.

MIB Objects

```
alaDot1xPortTable
   alaDot1xPortSlotNumber
   alaDot1xPortPortNumber
   alaDot1xPortMACAddress
   alaDot1xPortUserName
   alaDot1xPortState
alaDot1xAuthPolicyTable
   alaDot1xSuppPolicy
   alaDot1xNonSuppPolicy
```

show 802.1x statistics

Displays statistics about all 802.1X ports or for a particular 802.1X port.

show 802.1x statistics [*slot/port***]**

Syntax Definitions

slot	The slot of the port for which you want to display 802.1X statistics.
port	The port for which you want to display 802.1X statistics.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

If you do not specify a particular slot/port, information for each 802.1X port is displayed.

Examples

```
-> show 802.1x statistic 1/13
802.1x slot/port = 1/13
  Last EAPOL frame source          = 00:0d:0c:00:00:02
  Last EAPOL frame version         = 1,
  EAPOL frames received            = 3,
  EAPOL frames transmitted         = 3,
  EAPOL start frames received      = 1,
  EAPOL logoff frames received     = 0,
  EAP Resp/Id frames received      = 1,
  EAP Response frames received     = 1,
  EAP Req/Id frames transmitted    = 1,
  EAP Req frames transmitted       = 1,
  EAP length error frames received = 0,
  Invalid EAPOL frames received    = 0,
```

output definitions

Slot	The slot number of the 802.1X port.
Port	The 802.1X port number.
`Last EAPOL frame version`	The protocol version number carried in the most recently received EAPOL frame.
`Last EAPOL frame source`	The source MAC address carried in the most recently received EAPOL frame.
EAPOL frames received	The number of valid EAPOL frames of any type that have been received by the switch.

output definitions

EAPOL frames transmitted	The number of EAPOL frames of any type that have been transmitted by the switch.
EAPOL Start frames received	The number of EAPOL Start frames that have been received by the switch.
EAPOL Logoff frames received	The number of EAPOL Logoff frames that have been received by the switch.
EAP Resp/Id frames received	The number of EAP Resp/Id frames that have been received by the switch.
EAP Response frames received	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by the switch.
EAP Req/Id frames transmitted	The number of EAP Req/Id frames that have been transmitted by the switch.
`EAP Req frames transmitted`	The number of valid EAP Request frames (other than Req/Id frames) that have been transmitted by the switch.
`EAP length error frames received`	The number of EAPOL frames that have been received by the switch for which the Packet Body Length field is invalid.
`Invalid EAPOL frames received`	The number of EAPOL frames that have been received by the switch for which the frame type is not recognized by the switch.

Release History

Release 5.1; command was introduced.

Related Commands

show 802.1x	Displays information about ports configured for 802.1X.

MIB Objects

```
dot1xAuthStatsTable
   dot1xAuthEapolFramesRx
   dot1xAuthEapolFramesTx
   dot1xAuthEapolStartFramesRx
   dot1xAuthEapolLogoffFramesRx
   dot1xAuthEapolRespIdFramesRx
   dot1xAuthEapolRespFramesRx
   dot1xAuthEapolReqIdFramesTx
   dot1xAuthEapolReqFramesTx
   dot1xAuthInvalidEapolFramesRx
   dot1xAuthEapLengthErrorFramesRx
   dot1xAuthLastEapolFrameVersion
   dot1xAuthLastEapolFrameSource
```

show 802.1x device classification policies

Displays device classification policies configured for 802.1x ports.

show 802.1x device classification policies [*slot/port***]**

Syntax Definitions

slot/port	The slot and port number of the 802.1x port for which you want to display the policy configuration.

Defaults

All device classification policies for all 802.1x ports are displayed.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

Use the *slot/port* parameter to display device classification policies for a specific 802.1X port.

Examples

```
-> show 802.1x device classification policies
Device classification policies on 802.1x port 2/26
 Supplicant:
    authentication, block
 Non-Supplicant:
    block
Device classification policies on 802.1x port 2/47
 Supplicant:
    authentication, block
 Non-Supplicant:
    block
Device classification policies on 802.1x port 2/48
 Supplicant:
    authentication, vlan  247, default-vlan
 Non-Supplicant:
    authentication:
       pass: group-mobility, block
       fail: strict-vlan  347, default-vlan

-> show 802.1x device classification policies 2/48
Device classification policies on 802.1x port 2/48
 Supplicant:
    authentication, vlan  247, default-vlan
 Non-Supplicant:
    authentication:
       pass: group-mobility, block
       fail: strict-vlan  347, default-vlan
```

output definitions

Supplicant:	Displays the supplicant device classification policy configured for the 802.1x port.
Non-Supplicant:	Displays the non-supplicant device classification policy configured for the 802.1x port.

Release History

Release 5.4.1; command was introduced.

Related Commands

show 802.1x	Displays information about ports configured for 802.1X.
show 802.1x non-supp	Displays a list of all non-supplicants learned on all 802.1x ports.

MIB Objects

```
alaDot1xAuthPolicyTable
   alaDot1xSuppPolicy
   alaDot1xNonSuppPolicy
```

show 802.1x non-supp

Displays a list of all non-802.1x supplicants learned on all 802.1x ports.

show 802.1x non-supp [*slot/port***]**

Syntax Definitions

slot	The slot of the port for which you want to display information.
port	The port for which you want to display 802.1X information.

Defaults

N/A.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

If you do not specify a particular slot/port, all non-802.1x supplicants associated with all 802.1X ports are displayed.

Examples

```
->show 802.1x non-supp

Slot  MAC               Vlan
Port  Address           Learned
-----+-----------------+----------
3/1   00:61:4f:11:22:33     2
3/1   00:61:4f:44:55:66     2
3/1   00:61:4f:77:88:99     2
3/3   00:61:22:15:22:33     5
3/3   00:61:22:44:75:66     5

->show 802.1x non-supp 3/3

Slot  MAC               Vlan
Port  Address           Learned
-----+-----------------+----------
3/3   00:61:22:15:22:33     5
3/3   00:61:22:44:75:66     5
```

output definitions

`Slot/Port`	The 802.1X slot and port number that provides access to the non-802.1x device.
`MAC Address`	The source MAC address of the non-802.1x device connected to the 802.1x port.
`VLAN Learned`	The VLAN ID of the guest VLAN in which the source MAC address of the non-802.1x device was learned.

Release History

Release 5.1.6; command was introduced.

Related Commands

show 802.1x	Displays information about ports configured for 802.1X.

MIB Objects

```
alaDot1xPortTable
   alaDot1xNonSupplicantSlotNum
   alaDot1xNonSupplicantPortNum
   alaDot1xNonSupplicantMACAddress
   alaDot1xNonSupplicantVlanID
```

45 Memory Monitoring Commands

This chapter includes descriptions for System Debug and Memory Monitoring commands. These commands are used to configure parameters for kTrace and sysTrace Debug utilities and Memory Monitoring.

A summary of the available commands is listed here:

kTrace and sysTrace	**debug ktrace** **debug ktrace appid level** **debug ktrace show** **debug ktrace show log** **debug systrace** **debug systrace watch** **debug systrace appid level** **debug systrace show** **debug systrace show log** **show log pmd**
Memory monitoring	**debug memory monitor** **debug memory monitor show log** **debug memory monitor show log global** **debug memory monitor show log task** **debug memory monitor show log size**

debug ktrace

Enables or disables kTrace logging. The kernel trace, or *kTrace*, facility provides a consistent, low-level mechanism for capturing integer-based event records in a history buffer. This trace facility will generally be used by lower level functions to track information, such as which task is operating.

debug ktrace {enable | disable}

Syntax Definitions

enable	Enables kTrace logging.
disable	Disables kTrace logging.

Defaults

By default, kTrace logging is enabled.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> debug ktrace enable
-> debug ktrace disable
```

Release History

Release 5.1; command was introduced.

Related Commands

debug ktrace appid level	Adds or removes a kTrace capture level for a specified subsystem.
debug ktrace show	Displays current kTrace parameters.
debug ktrace show log	Displays kTrace log information.
debug systrace	Enables or disables sysTrace logging.
debug systrace watch	Enables or disables sysTrace log output to the console.
debug systrace appid level	Adds or removes a sysTrace capture level for a specified subsystem.
debug systrace show	Displays sysTrace debug log information.
debug systrace show log	Displays the sysTrace log.
show log pmd	Displays the contents of a stored Post Mortem Dump (PMD) file.

MIB Objects

N/A

debug ktrace appid level

Adds or removes a kTrace capture level for a specified application ID (i.e., subsystem).

debug ktrace appid {*app_id* **|** *integer***} level {***level* **|** *integer***}**

debug ktrace no appid *app_id*

Syntax Definitions

app_id	An application ID keyword value. Currently supported application IDs are listed below.
appid *integer*	A numerical equivalent value for the application ID. Currently supported numeric equivalent values are listed below.

Supported Application IDs and Numeric Equivalents

802.1q - 7	**ipc-diag - 1**	**psm - 81**
aaa - 20	**ip-helper - 22**	**qdispatcher - 3**
bridge - 10	**ipc-link - 4**	**qdriver - 2**
chassis - 64	**ipc-mon - 21**	**qos - 13**
cli - 67	**ipms - 17**	**rmon - 79**
config - 66	**ipx - 16**	**rsvp - 14**
dbggw - 89	**lanpower - 108**	**session - 71**
diag - 0	**ldap - 86**	**slb - 25**
distrib - 84	**linkagg - 12**	**smni - 83**
drc - 74	**mipgw - 70**	**snmp - 68**
eipc - 26	**module - 24**	**ssl - 88**
epilogue - 85	**nan-driver - 78**	**stp - 11**
ftp - 82	**ni-supervision - 5**	**system - 75**
health - 76	**nosnmp - 87**	**telnet - 80**
idle - 255	**pmm - 23**	**trap - 72**
interface - 6	**policy - 73**	**vlan - 8**
ip - 15	**port-mgr - 65**	**vrrp - 77**
		web - 69

level	The severity level keyword for the application ID (shown below). All kTrace events of the specified level and lower will be captured.
level *integer*	A numerical equivalent value for the severity level (shown below). Values may range from 1–9.

Supported Levels	Numeric Equivalents	Description
off	**1**	Off.
alarm	**2**	Highest severity. The system is about to crash and reboot.
error	**3**	System functionality is reduced.
alert	**4**	A violation has occurred.
warning	**5**	A unexpected, non-critical event has occurred.
info	**6**	Any other non-debug message (default).
debug1	**7**	A normal event debug message.
debug2	**8**	A debug-specific message.
debug3	**9**	Lowest severity. A maximum verbosity debug message.

Defaults

parameter	default
level	info (6)

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- You may enter more than one application ID in the command line. Separate each application ID with a space.
- Application IDs may be entered in any order.

Examples

```
-> debug ktrace appid 254 level off
-> debug ktrace appid policy level info
-> debug ktrace appid policy snmp web aaa vlan level alert
-> debug ktrace no appid debug2
```

Release History

Release 5.1; command was introduced.

Related Commands

debug ktrace	Enables or disables kTrace logging.
debug ktrace show	Displays current kTrace parameters.
debug ktrace show log	Displays kTrace log information.
debug systrace	Enables or disables sysTrace logging.
debug systrace watch	Enables or disables sysTrace log output to the console.
debug systrace appid level	Adds or removes a sysTrace capture level for a specified subsystem.
debug systrace show	Displays sysTrace debug log information.
debug systrace show log	Displays the sysTrace log.
show log pmd	Displays the contents of a stored Post Mortem Dump (PMD) file.

MIB Objects

N/A

debug ktrace show

Displays current kTrace parameters (e.g., kTrace status, Application IDs with non-default Severity Level settings).

debug ktrace show

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> debug ktrace show
kTrace is:
- INITIALIZED
- RUNNING
- configured to TRACE CALLERS

All applications have their trace level set to the level ‘info’ (6)
```

Output fields are described here:

output definitions

Application ID	If an Application ID (subsystem) keyword is displayed, such as SNMP (68), its Severity Level is not set to the info (6) default setting.
Level	The Severity Level of the above-referenced Application ID. Levels include off (1), alarm (2), error (3), alert (4), warning (5), info (6), debug1 (7), debug2 (8), and debug3 (9).

Release History

Release 5.1; command was introduced.

Related Commands

debug ktrace	Enables or disables kTrace logging.
debug ktrace appid level	Adds or removes a kTrace capture level for a specified subsystem.
debug ktrace show log	Displays kTrace log information.
debug systrace	Enables or disables sysTrace logging.
debug systrace watch	Enables or disables sysTrace log output to the console.
debug systrace appid level	Adds or removes a sysTrace capture level for a specified subsystem.
debug systrace show	Displays sysTrace debug log information.
debug systrace show log	Displays the sysTrace log.
show log pmd	Displays the contents of a stored Post Mortem Dump (PMD) file.

MIB Objects

N/A

debug ktrace show log

Displays kTrace log information.

debug ktrace show log [*file*]

Syntax Definitions

file	Specifies a particular file from which kTrace log information will be displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> debug ktrace show log
   Event     Timestamp AppID Level    Task ID  Caller (arg1, arg2, arg3, arg4)
   ----------+-------------+-------+------------+-------+---------------------------------------
   TSWITCH 0x4cad9a4  0x4b   info (6) SSAppKTL (0x00ca6370) 0x00066578 0x027b23b0
   0x00ca6370 0x00000000 0x00000000
   TSWITCH 0xd4cad98d 0x4b   info (6) ipcInteg (0x027b23b0) 0x00066578 0x00ca6370
   0x027b23b0 0x00000000 0x00000000
   TSWITCH 0xd4cad8ae 0x4b   info (6) SSAppKTL (0x00ca6370) 0x00066578 0x03186c10
   0x00ca6370 0x00000000 0x00000000
   TCREATE 0xd4cad810 0x4b   info (6) tssApp_2 (0x00cab440) 0x000665d0 0x00ca6370
   0x00000000 0x00000000 0x00000000
   TSWITCH 0xd4cad787 0x4b   info (6) tssApp_2 (0x00cab440) 0x00066578 0x03186c10
   0x00cab440 0x00000000 0x00000000
   TSWITCH 0xd4cad77c 0x4b   info (6) tMemMon (0x03186c10) 0x00066578 0x00cab440
   0x03186c10 0x00000000 0x00000000
   TSWITCH 0xd4cad771 0x4b   info (6) tssApp_2 (0x00cab440) 0x00066578 0x00cab440
   0x03186c10 0x00000000 0x00000000
   TSWITCH 0xd4cad751 0x4b   info (6) tMemMon (0x03186c10) 0x00066578 0x03186c10
   0x00cab440 0x00000000 0x00000000
   KICKDOG 0xd276db09 0x4b   info (6) tCsCSMta (0x022fb0d0) 0x00046760 0x0000001e
   0x0000001e 0x00000002 0x0000001e
   TSWITCH 0xd276d875 0x4b   info (6) SSApp (0x01d62350) 0x00066578 0x03186c10
   0x01d62350 0x00000000 0x00000000
```

Output fields are described here:

output definitions

Event	The event for which kTrace log information is displayed.
Timestamp	The timestamp for the kTrace log information being displayed. Values can range from 0x00000000 through 0xffffffff.
AppID	The Application ID (subsystem) for which kTrace log information is displayed. Values can range from 0x00 through 0xff.
Level	The Severity Level for which kTrace log information is displayed.Values include off (1), alarm (2), error (3), alert (4), warning (5), info (6) (default) debug1 (7), debug2 (8), and debug3 (9).
Task ID	The Task for which kTrace log information is displayed.
Caller	The address of the function containing the call that logged the event.

Release History

Release 5.1; command was introduced.

Related Commands

debug ktrace	Enables or disables kTrace logging.
debug ktrace appid level	Adds or removes a kTrace capture level for a specified subsystem.
debug ktrace show	Displays current kTrace parameters.
debug systrace	Enables or disables sysTrace logging.
debug systrace watch	Enables or disables sysTrace log output to the console.
debug systrace appid level	Adds or removes a sysTrace capture level for a specified subsystem.
debug systrace show	Displays sysTrace debug log information.
debug systrace show log	Displays the sysTrace log.
show log pmd	Displays the contents of a stored Post Mortem Dump (PMD) file.

MIB Objects

N/A

debug systrace

Enables or disables sysTrace logging. The system trace, or *sysTrace*, facility provides a consistent, high-level mechanism for capturing event records in a history buffer. Captured sysTrace information can be referenced for system debugging or following the unlikely event of a system crash. This trace facility will generally be used by higher level applications.

debug systrace {enable | disable}

Syntax Definitions

enable	Enables sysTrace logging.
disable	Disables sysTrace logging.

Defaults

By default, sysTrace logging is enabled.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> debug systrace enable
-> debug systrace disable
```

Release History

Release 5.1; command was introduced.

Related Commands

debug ktrace	Enables or disables kTrace logging.
debug ktrace appid level	Adds or removes a kTrace capture level for a specified subsystem.
debug ktrace show	Displays current kTrace parameters.
debug ktrace show log	Displays kTrace log information.
debug systrace watch	Enables or disables sysTrace log output to the console.
debug systrace appid level	Adds or removes a sysTrace capture level for a specified subsystem.
debug systrace show	Displays sysTrace debug log information.
debug systrace show log	Displays the sysTrace log.
show log pmd	Displays the contents of a stored Post Mortem Dump (PMD) file.

MIB Objects

N/A

debug systrace watch

Enables the sysTrace log on the console, or turns off (disables) the console display.

debug systrace watch {enable | disable}

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> debug systrace watch enable
-> debug systrace watch disable
```

Release History

Release 5.1; command was introduced.

Related Commands

debug ktrace	Enables or disables kTrace logging.
debug ktrace appid level	Adds or removes a kTrace capture level for a specified subsystem.
debug ktrace show	Displays current kTrace parameters.
debug ktrace show log	Displays kTrace log information.
debug systrace	Enables or disables sysTrace Logging
debug systrace appid level	Adds or removes a sysTrace capture level for a specified subsystem.
debug systrace show	Displays sysTrace debug log information.
debug systrace show log	Displays the sysTrace log.
show log pmd	Displays the contents of a stored Post Mortem Dump (PMD) file.

MIB Objects

N/A

debug systrace appid level

Adds or removes a sysTrace capture level for a specified application ID (i.e., subsystem).

debug systrace appid {*app_id* **|** *integer***} level {***level* **|** *integer***}**

debug systrace no appid *app_id*

Syntax Definitions

app_id	An application ID keyword value. Currently supported application IDs are listed below.
appid *integer*	A numerical equivalent value for the application ID. Currently supported numeric equivalent values are listed below.

Supported Application IDs and Numerical Equivalents

802.1q - 7	**interface - 6**	**psm - 81**
aaa - 20	**ip - 15**	**qdispatcher - 3**
amap - 18	**ipc-diag - 1**	**qdriver - 2**
bridge - 10	**ip-helper - 22**	**qos - 13**
chassis - 64	**ipc-link - 4**	**rmon - 79**
cli - 67	**ipc-mon - 21**	**rsvp - 14**
config - 66	**ipms - 17**	**session - 71**
dbggw - 89	**ipx - 16**	**slb - 25**
diag - 0	**lanpower - 108**	**smni - 83**
distrib - 84	**ldap - 86**	**snmp - 68**
drc - 74	**linkagg - 12**	**ssh - 109**
eipc - 26	**mipgw - 70**	**ssl - 88**
epilogue - 85	**module - 24**	**stp - 11**
ftp - 82	**nan-driver - 78**	**system - 75**
gmap - 19	**ni-supervision - 5**	**telnet - 80**
gm - 9	**nosnmp - 87**	**trap - 72**
health - 76	**pmm - 23**	**vlan - 8**
idle - 255	**policy - 73**	**vrrp - 77**
	port-mgr - 65	**web - 69**

level	The severity level keyword for the application ID (shown below). All sysTrace events of the specified level and lower will be captured.
level *integer*	A numerical equivalent value for the severity level (shown below). Values may range from 1–9.

Supported Levels	Numeric Equivalents	Description
off	**1**	Off.
alarm	**2**	Highest severity. The system is about to crash and reboot.
error	**3**	System functionality is reduced.
alert	**4**	A violation has occurred.
warning	**5**	A unexpected, non-critical event has occurred.
info	**6**	Any other non-debug message (default).
debug1	**7**	A normal event debug message.
debug2	**8**	A debug-specific message.
debug3	**9**	Lowest severity. A maximum verbosity debug message.

Defaults

parameter	default
level	info

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- You may enter more than one application ID in the command line. Separate each application ID with a space.
- Application IDs may be entered in any order.

Examples

```
-> debug systrace appid 254 level off
-> debug systrace appid policy level info
-> debug systrace appid policy snmp web aaa vlan level alert
-> debug systrace no appid debug2
```

Release History

Release 5.1; command was introduced.

Related Commands

debug ktrace	Enables or disables kTrace logging.
debug ktrace appid level	Adds or removes a kTrace capture level for a specified subsystem.
debug ktrace show	Displays current kTrace parameters.
debug ktrace show log	Displays kTrace log information.
debug systrace	Enables or disables sysTrace logging.
debug systrace watch	Enables or disables sysTrace log output to the console.
debug systrace show	Displays sysTrace debug log information.
debug systrace show log	Displays the sysTrace log.
show log pmd	Displays the contents of a stored Post Mortem Dump (PMD) file.

MIB Objects

N/A

debug systrace show

Displays sysTrace debug log information (e.g., sysTrace status, Application IDs with non-default Severity Level settings).

debug systrace show

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> debug systrace show
   sysTrace is:
   - INITIALIZED
   - RUNNING
   - configured to TRACE CALLERS
   - configured to NOT WATCH on stdout

   Only applications not at the level 'info' (6) are shown

   Application ID      Level
   ------------------------------------------------------
   SNMP         (68)   debug 1   (7)
   MIPGW        (70)   debug 1   (7)
   SYSTEM       (75)   debug 3   (9)
```

Output fields are described here:

output definitions

Application ID	The Application ID (subsystem) for which the Severity Level is not set to the info (6) default setting.
Level	The Severity Level of the above-referenced Application ID. Levels include off (1), alarm (2), error (3), alert (4), warning (5), info (6), debug1 (7), debug2 (8), and debug3 (9).

Release History

Release 5.1; command was introduced.

Related Commands

debug ktrace	Enables or disables kTrace logging.
debug ktrace appid level	Adds or removes a kTrace capture level for a specified subsystem.
debug ktrace show	Displays current kTrace parameters.
debug ktrace show log	Displays kTrace log information.
debug systrace	Enables or disables sysTrace logging.
debug systrace watch	Enables or disables sysTrace log output to the console.
debug systrace appid level	Adds or removes a sysTrace capture level for a specified subsystem.
debug systrace show log	Displays the sysTrace log.
show log pmd	Displays the contents of a stored Post Mortem Dump (PMD) file.

MIB Objects

N/A

debug systrace show log

Displays sysTrace log information.

debug systrace show log [*file*]

Syntax Definitions

file	Specifies a particular file from which sysTrace log information will be displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> debug systrace show log filename
   TimeStamp      AppID      Trace Level Task    Caller     Session ID Comment
   ---------------+----------+-----------------+----------+-------------+------------+--------------
   0xd3db513d  0x43 CLI     0x6   info 0x00ccd590 CliShell0 0x0305f608 0xffffffff
   [CLISHELL2] INIT socket nb : 175, local APP_ID: 67 and SNAP_ID: 66(TRUNCATED)
   0xd3db4ff1  0x43 CLI 0x6 info 0x00ccd590 CliShell0 0x0305f608 0xffffffff
   [CLISHELL2] INIT socket nb : 174, local APP_ID: 67 and SNAP_ID: 2(TRUNCATED)
   0xd3db4f47  0x43 CLI 0x6 info 0x00ccd590 CliShell0 0x030732bc 0xffffffff
   [CTRACE] CLI(ccd590) INITIALIZED address=3178b68/size=4096
   0xd3db4ed8  0x43 CLI 0x6 info 0x00ccd590 CliShell0 0x0305f914 0xffffffff
   [CLISHELL2] Task spawned, inactivity timer: 100000,file descriptor: 61
   0xc6d8b3e0  0x43 CLI 0x6 info 0x00cd1890 N/A 0x03073454 0xffffffff
   [CTRACE] CLI (cd1890) end by cd1890 address=16d1de0/size=4096
   0x0e0641fe  0x4b SYSTEM 0x5 warning 0x03186c10 tMemMon 0x000a7ad4 0xffffffff
   Task tShell has a memory leak at address 0x01527d68. Size is 52.
   0x0e0641e7  0x4b SYSTEM 0x5 warning 0x03186c10 tMemMon 0x000a7ad4 0xffffffff
   Task tShell has a memory leak at address 0x035ff510. Size is 129.
   0x0e0641d0  0x4b SYSTEM 0x5 warning 0x03186c10 tMemMon 0x000a7ad4 0xffffffff
   Task tShell has a memory leak at address 0x035ff478. Size is 140.
   0x0e0641b8  0x4b SYSTEM 0x5 warning 0x03186c10 tMemMon 0x000a7ad4 0xffffffff
   Task tShell has a memory leak at address 0x035ff3e0. Size is 140.
   0x0e0641a1  0x4b SYSTEM 0x5 warning 0x03186c10 tMemMon 0x000a7ad4 0xffffffff
   Task tShell has a memory leak at address 0x01096590. Size is 140.
   0x010fb724  0x4b SYSTEM 0x5 warning 0x03186c10 tMemMon 0x000a7ad4 0xffffffff
   Task has a memory leak at address 0x031773d0. Size is 32.
   0x010a5e85  0x4b SYSTEM 0x6 info0x035ffd60 N/A 0x000b2da4 0xffffffff ====>SYSTEM
   BOOT THU DEC 13 02:06:48 2001 <=====
   0x010a5e28  0x4b SYSTEM 0x6 info0x035ffd60 N/A 0x00067c9c 0xffffffff initializ-
   ing sysTrace, trace buffer at 0x31c0938, size=16384 entries.
```

Output fields are described here:

output definitions

Timestamp	The timestamp indicating when the sysTrace log entry occurred. Values can range from 0x00000000 through 0xffffffff.
AppID	The Application ID for which the stored sysTrace log information is displayed. Values can range from 0x00 through 0xff.
Trace Level	The Severity Level for which the stored sysTrace log information is displayed.
Task	The Task for which the stored sysTrace log information is displayed.
Caller	The function that called the sysTrace log.
Session ID	The Session ID for which the stored sysTrace log information is displayed. Values can range from 0x00000000 through 0xffffffff.
Comment	The condition that resulted in the sysTrace log entry.

Release History

Release 5.1; command was introduced.

Related Commands

debug ktrace	Enables or disables kTrace logging.
debug ktrace appid level	Adds or removes a kTrace capture level for a specified subsystem.
debug ktrace show	Displays current kTrace parameters.
debug ktrace show log	Displays kTrace log information.
debug systrace	Enables or disables sysTrace logging.
debug systrace watch	Enables or disables sysTrace log output to the console.
debug systrace appid level	Adds or removes a sysTrace capture level for a specified subsystem.
debug systrace show	Displays sysTrace debug log information.
show log pmd	Displays the contents of a stored Post Mortem Dump (PMD) file.

MIB Objects

N/A

show log pmd

Displays the contents of a stored Post Mortem Dump (PMD) file. The PMD file is a diagnostic aid that stores system information following some precipitating event (e.g., a system error).

show log pmd *file_name* [**type** *type_string* | **id** *registrationidentifier_int* | **subid** *subidentifier_int* | **taskname** *taskname_string* | **taskid** *tasknumber_int* | **record** *recordtype_string* | **address** *address_int*]

Syntax Definitions

file_name	Specifies a file containing the PMD dump information.
type_string	Specifies a registration type. Valid registration types include task, application, user-defined.
registrationidentifier_int	Specifies a registration identifier. Valid identifiers include **task number**, **unique value**, **snap/app id**.
subidentifier_int	Specifies a value that is unique when used with the registration type and registration identifier.
taskname_string	Specifies the name associated with the desired task.
tasknumber_int	Specifies the numeric value corresponding with the desired task.
recordtype_string	Specifies a record type. Valid record types include **userdefined**, **stackinfo**, **taskinfo**, **taskname**, **textstring**, **rawmemory**, **stacktrace**, **tasknumber**.
address_int	Specifies the address of the data buffer (specified in the original registration), to which memory list data will be sent.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

If no additional filter parameter is entered, all stored PMD file information will be displayed.

Examples

```
-> show log pmd filename
PMD Version -> 102
File Dump Type -> Mixed
Date Created - Coordinated universal time:  Wed Dec 19 09:22:27 2001

--------------------------------------------------------------------------------
Registration Type ->Application         Application Id. ->4b
```

```
Record Type -> MemoryData  Address -> 1b2b74  Size -> c4
 0  0  0  7  0 6e 31 3d  3 3e df  5  0  0 37 54  0  0 18 b6  0  0 11 87  0  0 7a 88
0 0 2c 4f
 0  0 c7 58  0  0 58 40  0  0 53 fc  0  0 b9 f0  0  0 d6 71  0  7 4c 54  0  6 a6 48
0 d c3 20
 0 4e 6f 24  0  0 9e c5  0 23 2a  2  0  5 77 c4  0  2 91 f1  0  1 63  8  0  7  d  8
0 4 2c  6
 0  9 3e d4  0  e dd 7e  0 24 2d  4  0 2a 43 e0  0 a1  4 89  0 80 1c d7  1 7e c1 dd
0 0  0  0
 0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0 2f
3 18 42 50
 3 43  8 d0  0  0  0  0  3 43  9 18  2 6a 7e 38  0  0  0  0  3 43  8 e8  2 21 42 b0
3 43  7 90
3 18 15  0
------------------------------------------------------------
Registration Type ->Task        Task No. ->3571290
Record Type -> TaskName Task Id  -> 3571290

tExcTask
------------------------------------------------------------
Registration Type ->Task        Task No. ->3571290
Record Type -> StackCheck       Task Id  -> 3571290

  NAME        ENTRY        TID     SIZE   CUR  HIGH  MARGIN
----------- ------------ -------- ----- ----- ----- ------
tExcTask     excTask      3571290  19984   976  3488  16496

------------------------------------------------------------
Registration Type ->Task        Task No. ->3571290
Record Type -> StackTrace       Task Id  -> 3571290

 e371c vxTaskEntry    +c  : excTask (0, 0, 0, 0, 0, 0)
 fb304 excTask        +24 : msgQReceive (1b8c00, 3571120, 1c, ffffffff, 0, 0)
130578 msgQReceive    +278: qJobGet (10000003, ffffffff, 7a000400, 1b8c00, 1ed400,
9e)

------------------------------------------------------------
Registration Type ->Task        Task No. ->3571290
Record Type -> TaskInfo Task Id  -> 3571290
  Address -> 0  Size -> 40

 task id= 3571290
 task priority= 0
 task status= 2
 task option bits= 7
 original entry point of task= fb2e0
 size of stack in bytes= 4e10
 current stack usage in bytes= 3d0
 maximum stack usage in bytes= da0
 current stack margin in bytes = 4070
 most recent task error status = 3d0001
 delay/timeout ticks = 0
 saved stack pointer= 3570ec0
 the bottom of the stack= 3571290
 the effective end of the stack= 356c480
 the actual end of the stack= 356c470

------------------------------------------------------------
```

```
Registration Type ->Task        Task No. ->3571290
Record Type -> UserDefined      Task Id  -> 3571290
  Address -> 1adcc38  Size -> 10
46 69 72 73 74 20 69 74 65 72 61 74 69 6f 6e  a
-------------------------------------------------------------
Registration Type ->Task        Task No. ->3571290
Record Type -> UserDefined      Task Id  -> 3571290
  Address -> 1adcc50  Size -> 11
53 65 63 6f 6e 64 20 69 74 65 72 61 74 69 6f 6e  a
-------------------------------------------------------------
Registration Type ->Task        Task No. ->356b990
Record Type -> TaskName Task Id  -> 356b990

tLogTask
-------------------------------------------------------------
Registration Type ->Task        Task No. ->356b990
Record Type -> StackCheck       Task Id  -> 356b990

  NAME        ENTRY        TID     SIZE   CUR  HIGH  MARGIN
------------ ------------ -------- ----- ----- ----- ------
tLogTask     logTask      356b990   8176   976  1168   7008

-------------------------------------------------------------
Registration Type ->Task        Task No. ->356b990
Record Type -> StackTrace       Task Id  -> 356b990

 e371c vxTaskEntry    +c  : logTask (0, 0, 0, 0, 0, 0)
100cac logTask        +2c : msgQReceive (1b8c00, 356b820, 20, ffffffff,
&fppTaskRegsCFmt, 9e)
130578 msgQReceive    +278: qJobGet (10000003, ffffffff, 7a000400, 1b8c00, 1ed400,
0)

-------------------------------------------------------------
Registration Type ->Task        Task No. ->356b990
Record Type -> TaskInfo Task Id  -> 356b990
  Address -> 0  Size -> 40

 task id= 356b990
 task priority= 0
 task status= 2
 task option bits= 6
 original entry point of task= 100c80
 size of stack in bytes= 1ff0
 current stack usage in bytes= 3d0
 maximum stack usage in bytes= 490
 current stack margin in bytes = 1b60
 most recent task error status = 0
 delay/timeout ticks = 0
 saved stack pointer= 356b5c0
 the bottom of the stack= 356b990
 the effective end of the stack= 35699a0
 the actual end of the stack= 3569990
-------------------------------------------------------------
```

Output fields are described here:

output definitions

PMD Version	The Post Mortem Dump (PMD) version ID.
File Dump Type	The file dump type.
Date Created	The date when the log was created.
Registration Type	The type of data being registered with PMD.
Application ID	The ID of the Application registering with PMD.
Record Type	The type of data registered with PMD.
Address	The address of the data being registered.
Size	The size (number of bytes) being registered.
Task Number	The number of the task registering with PMD.
Task ID	The vxWorks Task ID of the task registering with PMD.
Task Priority	The priority of the task registering with PMD.
Task Status	The status of the task registering with PMD.
Task Option Bits	The option bits of the task registering with PMD.
Original Entry Point of Task	The starting function of the task registering with PMD.
Size of Stack (bytes)	The size of the stack of the task registering with PMD.
Current Stack Usage (bytes)	The amount of the stack currently being used by the task registered with PMD.
Maximum Stack Usage (bytes)	The maximum amount of the stack used by the task registered with PMD.
Task Error Status	The current error status of the task registering with PMD.
Delay/Timeout Ticks	The number of ticks that the task will delay before becoming active.
Saved Stack Pointer	The stack pointer of the task registered with PMD.
Bottom of Stack	The base of the task's stack of the task registered with PMD.
Effective End of Stack	The end of the task's stack based upon the size shown previously.
Actual End of Stack	The actual end of the task's stack.

Release History

Release 5.1; command was introduced.

Related Commands

N/A

MIB Objects

N/A

debug memory monitor

Enables or disables memory monitoring functions.

debug memory monitor {enable | disable}

Syntax Definitions

enable	Enables memory monitoring.
disable	Disables memory monitoring.

Defaults

By default, memory monitoring functions are disabled.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> debug memory monitor enable
-> debug memory monitor disable
```

Release History

Release 5.1; command was introduced.

Related Commands

debug memory monitor show log	Displays memory monitoring log information.
debug memory monitor show log global	Displays memory monitoring global statistics.
debug memory monitor show log task	Displays memory monitoring task statistics.
debug memory monitor show log size	Displays memory monitoring size statistics.

MIB Objects

N/A

debug memory monitor show log

Displays memory monitoring log information.

debug memory monitor show log

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> debug memory monitor show log
   Task             Memory   Memory  Addr of  OSfunc   Calling Previous
   Name   Comments   Addr       Size OS call Called Function Caller
   ---------+---------+-------------+----------+--------+--------+------------+----------------------
   tssApp_2* TCB Stac 00ca1550 20680 0013a180 objAllocEx taskSpawn  ssAppChild
   tssApp_2* Vx B Sem 02317ca8   28 001374d0 objAlloc   pipe       ssAppChild
   tssApp_2* Vx B Sem 02317f78   28 001374d0 objAlloc   pipe       ssAppChild
   tssApp_2*          0107be78 5121 0012cfc8 malloc     pipe       ssAppChild
   tssApp_2*          023182b0   16 0012cfa8 malloc     pipe       ssAppChild
   tssApp_2*          024fdc90    9 00105fb0 malloc     pipe       ssAppChild
   tssApp_2*          016d6548   288 000af228 malloc    ssAppChild mip_msg_qu
   CliShell0 Vx C Sem 035fe590    28 0011f038 semCCreate zcSelect   mip_msg_do
   SsApp     Vx C Sem 035fe4b8   28 0011f038 semCCreate zcSelect   tssAppMain
   CliShell0          02318250    2 02b33a3c malloc     SSLexLexem SSYaccStac
   CliShell0          02317538   56 02b33a3c malloc     SSLexLexem SSYaccStac
   CliShell0          016d6670  272 02b33a3c malloc     SSYaccStac SSYaccPars
   CliShell0          02318260    1 02b33a3c malloc    SSLexLexem SSYaccStac
   CliShell0          02317718   56 02b33a3c malloc     SSLexLexem SSYaccStac
   CliShell0          016d68b0  272 02b33a3c malloc     SSYaccStac PropagateP
   CliShell0          023182c8    4 02b33a3c malloc     SSLexLexem SSYaccStac
   CliShell0          027b0060   56 02b33a3c malloc     SSLexLexem SSYaccStac
   CliShell0          01896b28  272 02b33a3c malloc     SSYaccStac SSYaccPars
   CliShell0          023182d8    4 02b33a3c malloc     SSLexLexem SSYaccStac
   CliShell0          035fe4e0   56 02b33a3c malloc     SSLexLexem SSYaccStac
   CliShell0          01e3d928  272 02b33a3c malloc     SSYaccStac SSYaccPars
   CliShell0          024fdca8    4 02b33a3c malloc     SSLexLexem SSYaccStac
   CliShell0          035fe3e0   56 02b33a3c malloc     SSLexLexem SSYaccStac
   CliShell0          022b3ab0  272 02b33a3c malloc     SSYaccStac SSYaccPars
   CliShell0          024fdcb8    3 02b33a3c malloc     SSLexLexem SSYaccStac
   CliShell0          01e37e40   56 02b33a3c malloc     SSLexLexem SSYaccStac
   CliShell0          022b3bc8  272 02b33a3c malloc     SSYaccStac SSYaccPars
```

```
CliShell0          02314da8  272 02b33a3c malloc     SSYaccStac SSYaccInit
CliShell0          023183d8  512 02b33a3c malloc     CliParse   clishell_m
CliShell0          027b0100  576 02b33a3c malloc     CliParse   clishell_m
CliShell0          0107a128 2404 02b33a3c malloc     CliParse   clishell_m
CliShell0          0107aa98  1280 02b33a3c malloc     CliParse   clishell_m
Stp       Vx C Sem024fdcc8 28 0011f038 semCCreate zcSelect   stpSock_st
LnkAgg Vx C Sem 023182e8  28 0011f038 semCCreate zcSelect   lagg_Sock_
AmapMgr Vx C Sem 02318270      28 0011f038 semCCreate zcSelect   xmap_main_
GrpMob Vx C Sem 035fe5b8 28 0011f038 semCCreate zcSelect   gmcWaitFor
GmapMgr Vx C Sem 02317fa0      28 0011f038 semCCreate zcRecvfrom gmap_main_
VlanMgr   Vx C Sem 02317cd0    28 0011f038 semCCreate zcSelect   vmcWaitFor
NanDrvr   Vx C Sem 02318158    28 0011f038 semCCreate zcRecvfrom nanDriver
```

Output fields are described here:

output definitions

Task Name	The task that "owns" the memory block.
Comments	The type of memory block that has been allocated. Comments include: • TCB Stack—this block belongs to the task whose name is listed • PX Msg Q—Posix Message Queue • Vx Msg Q—vxWorks Message Queue • P Sem—Posix Semaphore • Vx B Sem—vxWorks binary semaphore • Vx C Sem—vxWorks counting semaphore • Vx M Sem—vxWorks mutual exclusion semaphore • Leak—Memory leak.
Memory Address	The address of the memory block.
Memory Size	The size of the memory block.
Address of OS Call	The address of the call that allocated the block.
OS Function Called	The function that contained the call that allocated the block.
Calling Function	The function that called the above-mentioned function.
Previous Caller	The function that called the above-mentioned function.

Release History

Release 5.1; command was introduced.

Related Commands

debug memory monitor	Enables or disables memory monitoring functions.
debug memory monitor show log global	Displays memory monitoring global statistics.
debug memory monitor show log task	Displays memory monitoring task statistics.
debug memory monitor show log size	Displays memory monitoring size statistics.

MIB Objects

N/A

debug memory monitor show log global

Displays memory monitoring global statistics.

debug memory monitor show log global

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> debug memory monitor show log global
Current    = 33741
Cumulative = 687952
```

Output fields are described here:

output definitions

Current	The amount of dynamic memory allocated (currently) since the last enable.
Cumulative	The amount of dynamic memory allocated (cumulative) since the last enable.

Release History

Release 5.1; command was introduced.

Related Commands

debug memory monitor	Enables or disables memory monitoring functions.
debug memory monitor show log	Displays memory monitoring log information.
debug memory monitor show log task	Displays memory monitoring task statistics.
debug memory monitor show log size	Displays memory monitoring size statistics.

MIB Objects

N/A

debug memory monitor show log task

Displays memory monitoring task statistics.

debug memory monitor show log task

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> debug memory monitor show log task
Task Name           Current     Cumulative
----------------+-------------+-------------
       tssApp0_4         26369          52594
      cliConsole         16169          20186
      tIpxGapper           242            242
       tIpxTimer           214            214
        tDrcIprm       1801287        1801315
           DrcTm        479453         675448
         WebView         53690         340083
            Rmon        285084         334616
         SlbCtrl           578            578
          PolMgr           808          15704
             Qos         47096         938852
          UdpRly          8320           8348
            Vrrp           622           1198
             Ipx         29634          29634
           ipmpm        231152         231152
           ipmfm        480422         480450
           Ipmem        423686         423686
         GmapMgr          9128         263872
         AmapMgr           284         891188
          LnkAgg         86988        1867592
           8021q           128            184
         stpTick          1024           1024
             Stp         70782        1555454
          GrpMob           128         669300
          SrcLrn         12516          12572
          EsmDrv           356          74752
           PsMgr           168            308
           L3Hre           528            528
```

```
          Health            249          127649
             AAA         221312          222236
           Ipedr          31500          105868
          NanDrvr             56           74396
             Ftpd             56              56
          Telnetd           9552            9552
          tCS_CVM             28              28
  tssApp65535_3            228             228
           SsApp          49088          198284
          SesMgr          69200          202029
         SNMPagt          26347          210129
         TrapMgr           4548           63976
            EIpc           2336            2392
         VlanMgr            208          149672
         PortMgr            804           75424
         Gateway             84             140
          CfgMgr            228          897491
         tCS_HSM           1240            2500
         tCS_CMS            188             328
         tCS_PRB            312             340
         tCS_CCM            612           12555
      tCsCSMtask         586128        15256874
      tSwLogTask                          13519+
```

Output fields are described here:

output definitions

Task Name	The task that “owns” the memory block.
Current	The amount of dynamic memory allocated (currently) since log was enabled.
Cumulative	The amount of dynamic memory allocated (cumulative) since log was enabled.

Release History

Release 5.1; command was introduced.

Related Commands

debug memory monitor	Enables or disables memory monitoring functions.
debug memory monitor show log	Displays memory monitoring log information.
debug memory monitor show log global	Displays memory monitoring global statistics.
debug memory monitor show log size	Displays memory monitoring size statistics.

MIB Objects

N/A

debug memory monitor show log size

Displays memory monitoring size statistics.

debug memory monitor show log size

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> debug memory monitor show log size
Lower Upper   Currently   Cummulatively
Limit Limit   Allocated     Allocated
-----+-----+-------------+-------------+
    0    16         14439         31689
   16    32          6299       7704923
   32    64          4833        373109
   64   128         44248        145775
  128   256         12367        122315
  256   512         52096        228673
  512  1024         26778        365552
 1024  2048         24572        358630
 2048  4096         49648        274071
 4096  8192         50793       1534291
 8192 16384        478292        673610
16384 32768        431784       1075783
32768 65536        850216       1588017
65536             5130020       25675316
```

Output fields are described here:

output definitions

Lower Limit	The lower limit of the memory size range being measured.
Upper Limit	The upper limit of the memory size range being measured.
Currently Allocated	The amount of memory currently allocated (in bytes).
Cummulatively Allocated	The amount of memory cumulatively allocated (in bytes).

Release History

Release 5.1; command was introduced.

Related Commands

debug memory monitor	Enables or disables memory monitoring functions.
debug memory monitor show log	Displays memory monitoring log information.
debug memory monitor show log global	Displays memory monitoring global statistics.
debug memory monitor show log task	Displays memory monitoring task statistics.

MIB Objects

N/A

46 Switch Logging Commands

This chapter includes descriptions for Switch Logging commands. These commands are used to configure parameters for the Switch Logging utility.

MIB information for the system commands is as follows:

Filename: AlcatelIND1System.MIB
Module: ALCATEL-IND1-SYSTEM-MIB

A summary of the available commands is listed here.

swlog
swlog appid level
swlog output
swlog output flash file-size
swlog clear
show log swlog
show swlog

swlog

Enables or disables switch logging. Switch logging allows you to view a history of various switch activities in a text format.

swlog

no swlog

Syntax Definitions

N/A

Defaults

By default, switch logging is enabled.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

N/A

Examples

```
-> swlog
-> no swlog
```

Release History

Release 5.1; command was introduced.

Related Commands

swlog appid level	Defines the level at which switch logging information will be filtered for the specified application.
swlog output	Enables or disables switch logging output to the console, file, or data socket.
show log swlog	Displays stored switch logging information from flash.
show swlog	Displays switch logging information.

MIB Objects

```
systemSwitchLoggingGroup
   systemSwitchLoggingEnable
```

swlog appid level

Defines the level at which switch logging information will be filtered for the specified application. All application events of the defined level and lower are captured. Applications can be specified by their application ID (i.e., subsystem) or by their numeric equivalent.

swlog appid {*app_id* **|** *integer***} level {***level* **|** *integer***}**

no swlog appid *app_id*

Syntax Definitions

app_id	An application identification keyword. Current application IDs are listed in the table below.
integer	A numerical equivalent value for the application ID. Current numeric equivalent values are listed in the table below.

Supported Application IDs and their Numeric Equivalents

802.1q - 7	**ip - 15**	**psm - 81**
aaa - 20	**ipc-diag - 1**	**qdispatcher - 3**
amap - 18	**ip-helper - 22**	**qdriver - 2**
bridge - 10	**ipc-link - 4**	**qos - 13**
chassis - 64	**ipc-mon - 21**	**rmon - 79**
cli - 67	**ipms - 17**	**rsvp - 14**
config - 66	**ipx - 16**	**session - 71**
dbggw - 89	**lanpower - 108**	**slb - 25**
diag - 0	**ldap - 86**	**smni - 83**
distrib - 84	**linkagg - 12**	**snmp - 68**
drc - 74	**mipgw - 70**	**ssl - 88**
eipc - 26	**module - 24**	**stp - 11**
epilogue - 85	**nan-driver - 78**	**system - 75**
ftp - 82	**ni-supervision - 5**	**telnet - 80**
gmap - 19	**nosnmp - 87**	**trap - 72**
health - 76	**pmm - 23**	**vlan - 8**
idle - 255	**policy - 73**	**vrrp - 77**
interface - 6	**port-mgr - 64**	**web - 69**

level	The severity level filter keyword value for the application ID *(see table on the following page)*. All switch logging messages of the specified level and lower will be captured. The severity level is a value assigned to the relative severity of the switch logging message. A lower value indicates messages that are more severe, a higher value indicates messages that are less severe.
integer	A numerical equivalent value for the severity level *(see table on the following page)*. All switch logging messages of the specified level and lower will be captured. The severity level is a value assigned to the relative severity of the switch logging message. A lower value indicates messages that are more severe, a higher value indicates messages that are less severe. Values range from 2–9.

Supported Levels	Numeric Equivalents	Description
alarm	**2**	Highest severity. The system is about to crash and reboot.
error	**3**	System functionality is reduced.
alert	**4**	A violation has occurred.
warning	**5**	A unexpected, non-critical event has occurred.
info	**6**	Any other non-debug message (default).
debug1	**7**	A normal event debug message.
debug2	**8**	A debug-specific message.
debug3	**9**	Lowest severity. A maximum verbosity debug message.

Defaults

Default severity level is **info**. The numeric equivalent for info is 6.

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- You may enter multiple application IDs in the command line. Separate each application ID with a space but no comma.
- Application IDs may be entered in any order.
- This command can also be used on the secondary CMM.

Examples

```
-> swlog appid 254 level alarm
-> swlog appid policy level info
-> swlog appid policy snmp web aaa vlan level alert
-> no swlog appid debug2
```

Release History

Release 5.1; command was introduced.

Related Commands

swlog	Enables or disables switch logging.
swlog output	Enables or disables switch logging output to the console, file, or data socket.
show log swlog	Displays stored switch logging information from flash.
show swlog	Displays switch logging information.

MIB Objects

```
systemSwitchLoggingGroup
   systemSwitchLoggingLevelAppId
   systemSwitchLoggingLevel
```

swlog output

Enables or disables switch logging output to the console, file, or data socket (remote session).

swlog output {console | flash | socket *[ip_address]***}**

no swlog output {console | flash | socket *[ip_address]***}**

Syntax Definitions

console	Specifies console output. When enabled, switch logging output is printed to the user console.
flash	Specifies /flash file output. When enabled, switch logging output is printed to a file in the switch's /flash file system.
socket	Specifies data socket output. When enabled, switch logging output is printed to a remote session.
ip_address	The IP address for the remote session host.

Defaults

parameter	default
console | **flash** | **socket**	**flash** and **console**

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- This command can also be used on the secondary CMM.
- You can send syslog files to multiple hosts (maximum of four) using the **socket** keyword, followed by the IP address of the remote host.

Examples

```
-> swlog output console
-> no swlog output flash
-> swlog output socket 14.1.1.1
-> swlog output socket 15.1.1.1
-> swlog output socket 16.1.1.1
-> swlog output socket 17.1.1.1
```

Release History

Release 5.1; command was introduced.

Related Commands

swlog	Enables or disables switch logging.
swlog appid level	Defines the level at which switch logging information will be filtered for the specified application.
show log swlog	Displays stored switch logging information from flash.
show swlog	Displays switch logging information.

MIB Objects

```
systemSwitchLoggingGroup
   systemSwitchLoggingFlash
   systemSwitchLoggingSocket
   systemSwitchLoggingSocketIpAddr
   systemSwitchLoggingConsole
systemSwitchLoggingHostTable
   systemSwitchLoggingHostIpAddr
   systemSwitchLoggingHostPort
   systemSwitchLoggingHostStatus
```

swlog output flash file-size

Configures the size of the switch logging file.

swlog output flash file-size *bytes*

Syntax Definitions

bytes	The size of the switch logging file. The minimum value is 32000 while the maximum value is the total amount of free space in flash memory.

Defaults

parameter	default
bytes	128000

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use the **ls** command to determine the amount of available flash memory.
- This command can also be used on the secondary CMM.

Examples

```
-> swlog output flash file size 400000
```

Release History

Release 5.1; command was introduced.

Related Commands

swlog clear	Clears the files that store switch logging data.
show log swlog	Displays stored switch logging information from flash.
show swlog	Displays switch logging information.

MIB Objects

```
systemSwitchLoggingGroup
   systemSwitchLoggingFileSize
```

swlog clear

Clears the files that store switch logging data.

swlog clear

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- Use this command when the switch logging display is too long due to some of the data being old or out dated.
- This command can also be used on the secondary CMM.

Examples

```
-> swlog clear
```

Release History

Release 5.1; command was introduced.

Related Commands

swlog output	Enables or disables switch logging output to the console, file, or data socket.
show log swlog	Displays stored switch logging information from flash.
show swlog	Displays switch logging information.

MIB Objects

```
systemSwitchLoggingGroup
   systemSwitchLoggingClear
```

show log swlog

Displays stored switch logging information.

show log swlog

show log swlog [session *session_id***] [timestamp** *start_time* **[***end_time***]] [appid** *appid***] [level** *level***]**

Syntax Definitions

session_id	Identification number of the session for which switch logging information is displayed.
start_time	Specify the starting time for the switch logging information to be displayed. Use the format mm/dd/yyyy hh:mm where mm represents the month, dd is the day, yyyy is the year, hh is the hour, and mm is the minutes. Use four digits to specify the year.
end_time	Specify the ending time for the switch logging information to be displayed. Use the format mm/dd/yyyy hh:mm where mm represents the month, dd is the day, yyyy is the year, hh is the hour, mm is the minutes. Use four digits to specify the year.
appid	A digit that represents the application ID for the switch logging information to be displayed. Values are listed in the following table.

Supported Application IDs and their Numeric Equivalents

802.1q - 7	**ip - 15**	**qdispatcher - 3**
aaa - 20	**ipc-diag - 1**	**qdriver - 2**
amap - 18	**ip-helper - 22**	**qos - 13**
bridge - 10	**ipc-link - 4**	**rmon - 79**
chassis - 64	**ipc-mon - 21**	**rsvp - 14**
cli - 67	**ipms - 17**	**session - 71**
config - 66	**ipx - 16**	**slb - 25**
dbggw - 89	**ldap - 86**	**smni - 83**
diag - 0	**linkagg - 12**	**snmp - 68**
distrib - 84	**mipgw - 70**	**ssl - 88**
drc - 74	**module - 24**	**stp - 11**
eipc - 26	**nan-driver - 78**	**system - 75**
epilogue - 85	**ni-supervision - 5**	**telnet - 80**
ftp - 82	**nosnmp - 87**	**trap - 72**
gmap - 19	**pmm - 23**	**vlan - 8**
health - 76	**policy - 73**	**vrrp - 77**
idle - 255	**port-mgr - 64**	**web - 69**
interface - 6	**psm - 81**	

level A numerical equivalent value for the severity level *(see table below)*. All switch logging messages of the specified level and lower will be shown. The severity level is a value assigned to the relative severity of the switch logging message. A lower value indicates messages that are more severe, a higher value indicates messages that are less severe. Values range from 2–9.

Supported Levels	Numeric Equivalents	Description
alarm	**2**	Highest severity. The system is about to crash and reboot.
error	**3**	System functionality is reduced.
alert	**4**	A violation has occurred.
warning	**5**	A unexpected, non-critical event has occurred.
info	**6**	Any other non-debug message (default).
debug1	**7**	A normal event debug message.
debug2	**8**	A debug-specific message.
debug3	**9**	Lowest severity. A maximum verbosity debug message.

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

- When the switch logging display is too long, you may use the **show log swlog** command to clear all of the switch logging information.
- This command can also be used on the secondary CMM.

Examples

(The example display shown on the next page is from an OmniSwitch 6600 Family switch. The display is similar for OmniSwitch 7700/7800/8800.)

```
-> show log swlog
Displaying file contents for 'swlog2.log'
FILEID: fileName[swlog2.log], endPtr[32]
         configSize[64000], currentSize[64000], mode[2]
Displaying file contents for 'swlog1.log'
FILEID: fileName[swlog1.log], endPtr[395]
         configSize[64000], currentSize[64000], mode[1]

Time Stamp               Application    Level   Log Message

-----------------------+-------------+-------+------------------------------

MON NOV 11 12:42:11 2002         SYSTEM    info Switch Logging files cleared by
command
MON NOV 11 13:07:26 2002            WEB    info The HTTP session login successfu
l!
MON NOV 11 13:18:24 2002            WEB    info The HTTP session login successfu
l!
MON NOV 11 13:24:03 2002         TELNET    info New telnet connection, Address ,
128.251.30.88
MON NOV 11 13:24:03 2002         TELNET    info Session 4, Created
MON NOV 11 13:59:04 2002            WEB    info The HTTP session user logout suc
cessful!
```

output definitions

Time Stamp	The day, date, and time for which Switch Logging log information is displayed.
Application	The Application ID (Subsystem) for which Switch Logging log information is displayed.
Level	The corresponding Severity Level for which Switch Logging information was stored. Levels include alarm, error, alert, warning, info, debug1, debug2, and debug3.
Log Message	The condition that resulted in the logging information being stored.

Release History

Release 5.1; command was introduced.

Related Commands

swlog	Enables or disables switch logging.
swlog appid level	Adds or removes a filter level for a specified subsystem.
swlog output	Enables or disables switch logging output to the console, file, or data socket.
swlog clear	Clears the files that store switch logging data.
show swlog	Displays switch logging information.

show swlog

Displays switch logging information (e.g., switch logging status, log devices, application IDs with non-default severity level settings).

show swlog

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6600, 7700, 7800, 8800

Usage Guidelines

This command can also be used on the secondary CMM.

Examples

```
-> show swlog
Switch Logging is :
        - INITIALIZED.
        - RUNNING.

Log Device(s)
-------------
flash
console
socket ipaddr 11.1.1.1
socket ipaddr 12.1.1.1
socket ipaddr 13.1.1.1
socket ipaddr 14.1.1.1

All Applications have their trace level set to the level 'info' (6)
```

output definitions

Application ID	The Application ID (subsystem) for which the Severity Level is not set to the info (6) default setting.
Level	The Severity Level of the above-referenced Application ID. Levels include (2), error (3), alert (4), warning (5), info (6), debug1 (7), debug2 (8), and debug3 (9).

Release History

Release 5.1; command was introduced.

Related Commands

swlog	Enables or disables switch logging.
swlog appid level	Defines the level at which switch logging information will be filtered for the specified application.
swlog output	Enables or disables switch logging output to the console, file, or data socket.
show log swlog	Displays stored switch logging information from flash.

A Software License and Copyright Statements

This appendix contains Alcatel and third-party software vendor license and copyright statements.

Alcatel License Agreement

ALCATEL INTERNETWORKING, INC. ("AII") SOFTWARE LICENSE AGREEMENT

IMPORTANT. Please read the terms and conditions of this license agreement carefully before opening this package.

By opening this package, you accept and agree to the terms of this license agreement. If you are not willing to be bound by the terms of this license agreement, do not open this package. Please promptly return the product and any materials in unopened form to the place where you obtained it for a full refund.

1. **License Grant.** This is a license, not a sales agreement, between you (the "Licensee") and AII. AII hereby grants to Licensee, and Licensee accepts, a non-exclusive license to use program media and computer software contained therein (the "Licensed Files") and the accompanying user documentation (collectively the "Licensed Materials"), only as authorized in this License Agreement. Licensee, subject to the terms of this License Agreement, may use one copy of the Licensed Files on the Licensee's system. Licensee agrees not to assign, sublicense, transfer, pledge, lease, rent, or share their rights under this License Agreement. Licensee may retain the program media for backup purposes with retention of the copyright and other proprietary notices. Except as authorized under this paragraph, no copies of the Licensed Materials or any portions thereof may be made by Licensee and Licensee shall not modify, decompile, disassemble, reverse engineer, or otherwise attempt to derive the Source Code. Licensee is also advised that AII products contain embedded software known as firmware which resides in silicon. Licensee may not copy the firmware or transfer the firmware to another medium.

2. **AII's Rights.** Licensee acknowledges and agrees that the Licensed Materials are the sole property of AII and its licensors (herein "its licensors"), protected by U.S. copyright law, trademark law, and are licensed on a right to use basis. Licensee further acknowledges and agrees that all rights, title, and interest in and to the Licensed Materials are and shall remain with AII and its licensors and that no such right, license, or interest shall be asserted with respect to such copyrights and trademarks. This License Agreement does not convey to Licensee an interest in or to the Licensed Materials, but only a limited right to use revocable in accordance with the terms of this License Agreement.

3. **Confidentiality.** AII considers the Licensed Files to contain valuable trade secrets of AII, the unauthorized disclosure of which could cause irreparable harm to AII. Except as expressly set forth herein, Licensee agrees to use reasonable efforts not to disclose the Licensed Files to any third party and not to use the Licensed Files other than for the purpose authorized by this License Agreement. This confidentiality obligation shall continue after any termination of this License Agreement.

4. **Indemnity.** Licensee agrees to indemnify, defend and hold AII harmless from any claim, lawsuit, legal proceeding, settlement or judgment (including without limitation AII's reasonable United States and local attorneys' and expert witnesses' fees and costs) arising out of or in connection with the unauthorized copying, marketing, performance or distribution of the Licensed Files.

5. **Limited Warranty.** AII warrants, for Licensee's benefit alone, that the program media shall, for a period of ninety (90) days from the date of commencement of this License Agreement (referred to as the Warranty Period), be free from defects in material and workmanship. AII further warrants, for Licensee benefit alone, that during the Warranty Period the Licensed Files shall operate substantially in accordance with the functional specifications in the User Guide. If during the Warranty Period, a defect in the Licensed Files appears, Licensee may return the Licensed Files to AII for either replacement or, if so elected by AII, refund of amounts paid by Licensee under this License Agreement. EXCEPT FOR THE WARRANTIES SET FORTH ABOVE, THE LICENSED MATERIALS ARE LICENSED "AS IS" AND AII AND ITS LICENSORS DISCLAIM ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING (WITHOUT LIMITATION) ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES SO THE ABOVE EXCLUSIONS MAY NOT APPLY TO LICENSEE. THIS WARRANTY GIVES THE LICENSEE SPECIFIC LEGAL RIGHTS. LICENSEE MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM STATE TO STATE.

6. **Limitation of Liability.** AII's cumulative liability to Licensee or any other party for any loss or damages resulting from any claims, demands, or actions arising out of or relating to this License Agreement shall not exceed the license fee paid to AII for the Licensed Materials. IN NO EVENT SHALL AII BE LIABLE FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, OR EXEMPLARY DAMAGES OR LOST PROFITS, EVEN IF AII HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION TO INCIDENTAL OR CONSEQUENTIAL DAMAGES MAY NOT APPLY TO LICENSEE.

7. **Export Control.** This product is subject to the jurisdiction of the United States. Licensee may not export or reexport the Licensed Files, without complying with all United States export laws and regulations, including but not limited to (i) obtaining prior authorization from the U.S. Department of Commerce if a validated export license is required, and (ii) obtaining "written assurances" from licensees, if required.

8. **Support and Maintenance.** Except as may be provided in a separate agreement between AII and Licensee, if any, AII is under no obligation to maintain or support the copies of the Licensed Files made and distributed hereunder and AII has no obligation to furnish Licensee with any further assistance, documentation or information of any nature or kind.

9. **Term.** This License Agreement is effective upon Licensee opening this package and shall continue until terminated. Licensee may terminate this License Agreement at any time by returning the Licensed Materials and all copies thereof and extracts therefrom to AII and certifying to AII in writing that all Licensed Materials and all copies thereof and extracts therefrom have been returned or erased by the memory of Licensee's computer or made non-readable. AII may terminate this License Agreement upon the breach by Licensee of any term hereof. Upon such termination by AII, Licensee agrees to return to AII or destroy the Licensed Materials and all copies and portions thereof.

10. **Governing Law.** This License Agreement shall be construed and governed in accordance with the laws of the State of California.

11. **Severability.** Should any term of this License Agreement be declared void or unenforceable by any court of competent jurisdiction, such declaration shall have no effect on the remaining terms herein.

12. **No Waiver.** The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent actions in the event of future breaches.

13. **Notes to United States Government Users.** Software and documentation are provided with restricted rights. Use, duplication or disclosure by the government is subject to (i) restrictions set forth in GSA ADP Schedule Contract with AII's reseller(s), or (ii) restrictions set forth in subparagraph (c) (1) and (2) of 48 CFR 52.227-19, as applicable.

14.**Third Party Materials.** Licensee is notified that the Licensed Files contain third party software and materials licensed to AII by certain third party licensors. Some third party licensors (e.g., Wind River and their licensors with respect to the Run-Time Module) are third part beneficiaries to this License Agreement with full rights of enforcement. Please refer to the section entitled "Third Party Licenses and Notices" on page A-4 for the third party license and notice terms.

Third Party Licenses and Notices

The licenses and notices related only to such third party software are set forth below:

A. Booting and Debugging Non-Proprietary Software

A small, separate software portion aggregated with the core software in this product and primarily used for initial booting and debugging constitutes non-proprietary software, some of which may be obtained in source code format from AII for a limited period of time. AII will provide a machine-readable copy of the applicable non-proprietary software to any requester for a cost of copying, shipping and handling. This offer will expire 3 years from the date of the first shipment of this product.

B. The OpenLDAP Public License: Version 2.4, 8 December 2000

Redistribution and use of this software and associated documentation (“Software”), with or without modification, are permitted provided that the following conditions are met:

1 Redistributions of source code must retain copyright statements and notices.

2 Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

3 Redistributions must contain a verbatim copy of this document.

4 The names and trademarks of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission.

5 Due credit should be given to the OpenLDAP Project.

6 The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use the Software under terms of this license revision or under the terms of any subsequent revision of the license.

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

OpenLDAP is a trademark of the OpenLDAP Foundation.

C. Linux

Linux is written and distributed under the GNU General Public License which means that its source code is freely-distributed and available to the general public.

D. GNU GENERAL PUBLIC LICENSE: Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 675 Mass Ave, Cambridge, MA 02139, USA
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0 This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either

verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term “modification”.) Each licensee is addressed as “you”.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1 You may copy and distribute verbatim copies of the Program’s source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2 You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3 You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4 You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5 You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6 Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7 If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on

consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8 If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9 The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10 If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11 BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12 IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Appendix: How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

> <one line to give the program's name and a brief idea of what it does.> Copyright (C) 19yy <name of author>
>
> This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.
>
> This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.
>
> You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

> Gnomovision version 69, Copyright (C) 19yy name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type 'show w'. This is free software, and you are welcome to redistribute it under certain conditions; type 'show c' for details.

The hypothetical commands 'show w' and 'show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than 'show w' and 'show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

> Yoyodyne, Inc., hereby disclaims all copyright interest in the program 'Gnomovision' (which makes passes at compilers) written by James Hacker.
>
> <signature of Ty Coon>, 1 April 1989
> Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

> URLWatch:
>
> For notice when this page changes, fill in your email address.

Maintained by: Webmaster, Linux Online Inc.
Last modified: 09-Aug-2000 02:03AM.
Views since 16-Aug-2000: 177203.

Material copyright Linux Online Inc.
Design and compilation copyright (c)1994-2002 Linux Online Inc.
Linux is a registered trademark of Linus Torvalds
Tux the Penguin, featured in our logo, was created by Larry Ewing
Consult our privacy statement

URLWatch provided by URLWatch Services.
All rights reserved.

E. University of California

Provided with this product is certain TCP input and Telnet client software developed by the University of California, Berkeley.

F. Carnegie-Mellon University

Provided with this product is certain BOOTP Relay software developed by Carnegie-Mellon University.

G. Random.c

PR 30872 B Kesner created May 5 2000
PR 30872 B Kesner June 16 2000 moved batch_entropy_process to own task iWhirlpool to make code more efficient

random.c -- A strong random number generator

Version 1.89, last modified 19-Sep-99

Copyright Theodore Ts'o, 1994, 1995, 1996, 1997, 1998, 1999. All rights reserved.

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

1. Redistributions of source code must retain the above copyright notice, and the entire permission notice in its entirety, including the disclaimer of warranties.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission. ALTERNATIVELY, this product may be distributed under the terms of the GNU Public License, in which case the provisions of the GPL are required INSTEAD OF the above restrictions. (This clause is necessary due to a potential bad interaction between the GPL and the restrictions contained in a BSD-style copyright.)

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

H. Apptitude, Inc.

Provided with this product is certain network monitoring software ("MeterWorks/RMON") licensed from Apptitude, Inc., whose copyright notice is as follows: Copyright (C) 1997-1999 by Apptitude, Inc. All Rights Reserved. Licensee is notified that Apptitude, Inc. (formerly, Technically Elite, Inc.), a California corporation with principal offices at 6330 San Ignacio Avenue, San Jose, California, is a third party beneficiary to the Software License Agreement. The provisions of the Software License Agreement as applied to MeterWorks/RMON are made expressly for the benefit of Apptitude, Inc., and are enforceable by Apptitude, Inc. in addition to AII. IN NO EVENT SHALL APPTITUDE, INC. OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES, INCLUDING COSTS OF PROCUREMENT OF SUBSTITUTE PRODUCTS OR SERVICES, LOST PROFITS, OR ANY SPECIAL, INDIRECT, CONSEQUENTIAL OR INCIDENTAL DAMAGES, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, ARISING IN ANY WAY OUT OF THIS AGREEMENT.

I. Agranat

Provided with this product is certain web server software ("EMWEB PRODUCT") licensed from Agranat Systems, Inc. ("Agranat"). Agranat has granted to AII certain warranties of performance, which warranties [or portion thereof] AII now extends to Licensee. IN NO EVENT, HOWEVER, SHALL AGRANAT BE LIABLE TO LICENSEE FOR ANY INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES OF LICENSEE OR A THIRD PARTY AGAINST LICENSEE ARISING OUT OF, OR IN CONNECTION WITH, THIS DISTRIBUTION OF EMWEB PRODUCT TO LICENSEE. In case of any termination of the Software License Agreement between AII and Licensee, Licensee shall immediately return the EMWEB Product and any back-up copy to AII, and will certify to AII in writing that all EMWEB Product components and any copies of the software have been returned or erased by the memory of Licensee's computer or made non-readable.

J. RSA Security Inc.

Provided with this product is certain security software ("RSA Software") licensed from RSA Security Inc. RSA SECURITY INC. PROVIDES RSA SOFTWARE "AS IS" WITHOUT ANY WARRANTY WHATSOEVER. RSA SECURITY INC. DISCLAIMS ALL WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO ANY MATTER WHATSOEVER INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS.

K. Sun Microsystems, Inc.

This product contains Coronado ASIC, which includes a component derived from designs licensed from Sun Microsystems, Inc.

L. Wind River Systems, Inc.

Provided with this product is certain software (“Run-Time Module”) licensed from Wind River Systems, Inc. Licensee is prohibited from: (i) copying the Run-Time Module, except for archive purposes consistent with Licensee’s archive procedures; (ii) transferring the Run-Time Module to a third party apart from the product; (iii) modifying, decompiling, disassembling, reverse engineering or otherwise attempting to derive the source code of the Run-Time Module; (iv) exporting the Run-Time Module or underlying technology in contravention of applicable U.S. and foreign export laws and regulations; and (v) using the Run-Time Module other than in connection with operation of the product. In addition, please be advised that: (i) the Run-Time Module is licensed, not sold and that AII and its licensors retain ownership of all copies of the Run-Time Module; (ii) WIND RIVER DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, (iii) The SOFTWARE LICENSE AGREEMENT EXCLUDES LIABILITY FOR ANY SPECIAL, INDIRECT, PUNITIVE, INCIDENTAL AND CONSEQUENTIAL DAMAGES; and (iv) any further distribution of the Run-Time Module shall be subject to the same restrictions set forth herein. With respect to the Run-Time Module, Wind River and its licensors are third party beneficiaries of the License Agreement and the provisions related to the Run-Time Module are made expressly for the benefit of, and are enforceable by, Wind River and its licensors.

M.Network Time Protocol Version 4

The following copyright notice applies to all files collectively called the Network Time Protocol Version 4 Distribution. Unless specifically declared otherwise in an individual file, this notice applies as if the text was explicitly included in the file.

```
***********************************************************************
*                                                                     *
* Copyright (c) David L. Mills 1992-2003                              *
*                                                                     *
* Permission to use, copy, modify, and distribute this software and   *
* its documentation for any purpose and without fee is hereby         *
* granted, provided that the above copyright notice appears in all    *
* copies and that both the copyright notice and this permission       *
* notice appear in supporting documentation, and that the name        *
* University of Delaware not be used in advertising or publicity      *
* pertaining to distribution of the software without specific,        *
* written prior permission. The University of Delaware makes no       *
* representations about the suitability this software for any         *
* purpose. It is provided "as is" without express or implied          *
* warranty.                                                           *
*                                                                     *
***********************************************************************
```

CLI Quick Reference

CMM Commands

reload [primary | secondary] [in [*hours*:] *minutes* | at *hour*:*minute* [*month day* | *day month*]]
reload [primary | secondary] cancel
reload working {rollback-timeout minutes | no rollback-timeout} [in [*hours*:] *minutes* | at *hour*:*minute*]
[configure] copy running-config working
[configure] write memory
[configure] copy certified working
[configure] copy working certified [flash-synchro]
[configure] copy flash-synchro
takeover
debug chassis auto-reboot {enable | disable}
show running-directory
show reload [status]
show microcode [working | certified | loaded]
show microcode history [working | certified]

Chassis Management and Monitoring Commands

system contact *text_string*
system name *text_string*
system location *text_string*
system date [*mm/dd/yyyy*]
system time [*hh:mm:ss*]
system time-and-date synchro
system timezone [*timezone_abbrev* | *offset_value* | *time_notation*]
system daylight savings time [{enable | disable} | start {*week*} {*day*} in {*month*} at {*hh:mm*} end {*week*} {*day*} in {*month*} at {*hh:mm*} [by *min*]]
reload ni [slot] *number*
reload all [in [*hours*:] *minutes* | at *hour*:*minute* [*month day* | *day month*]]
reload all cancel
power ni [slot] *slot-number*
no power ni [slot] *slot-number*
temp-threshold *temp*
fabric standby *number*
power fabric *number*
no power fabric *number*
show system
show hardware info
show chassis [*number*]
show cmm [*number*]
show ni [*number*]
show module [*number*]
show module long [*number*]
show module status [*number*]
show power [supply] [*number*]
show fan [*number*]
show temperature [*number*]
show stack topology [*slot-number*]
show fabric [*number*]

Chassis MAC Server (CMS) Commands

mac-range eeprom *start_mac_address count*
show mac-range [*index*]
show mac-range [*index*] alloc

Power over Ethernet (PoE) Commands

lanpower start {*slot/port* | *slot*}
lanpower stop {*slot/port* | *slot*}
lanpower {*slot/port* | *slot*} power *milliwatts*
lanpower {*slot/port* | *slot*} maxpower *watts*
lanpower *slot/port* priority {critical | high | low}
lanpower *slot* priority-disconnect {enable | disable}
lanpower redundant-power {enable | disable}
lanpower *slot* capacitor-detection {enable | disable}
show lanpower *slot*
show lanpower capacitor-detection *slot*
show lanpower priority-disconnect *slot*
show lanpower slot-priority *slot*

Network Time Protocol Commands

ntp server {*ip_address* | *domain_name*} [key *key* | version *version* | minpoll *exponent* | prefer]
no ntp server {*ip_address* | *domain_name*}
ntp client {enable | disable}
ntp broadcast {enable | disable}
ntp broadcast delay *microseconds*
ntp key *key* [trusted | untrusted]
ntp key load
show ntp client
show ntp client server-list
show ntp server status [*ip_address* | *domain_name*]

show ntp keys

Session Management Commands

session login-attempt integer
session login-timeout *seconds*
session banner {cli | ftp} file_name
session banner no {cli | ftp}
session timeout {cli | http | ftp} *minutes*
session prompt default [*string*]
session xon-xoff {**enable** | **disable**}
prompt [user] [time] [date] [string *string*] [prefix]
no prompt
show prefix
alias *alias command_name*
show alias
user profile save
user profile reset
history size *number*
show history [*parameters*]
!{! | *n*}
command-log {enable | disable}
kill *session_number*
exit
whoami
who
show session config
show session xon-xoff
more size *lines*
more
no more
show more
telnet {*host_name* | *ip_address***}**
ssh {*host_name* | *ip_address***}**
show command-log
show command-log status

File Management Commands

cd [*path*]
pwd
mkdir [*path/*]*dir*
rmdir [*path/*]*dir*
ls [-r] [[*path/*]*dir*]
dir [[*path/*]*dir*]
rename [*path/*]*old_name* [*path/*]*new_name*
rm [-r] [*path/*]*filename*
delete [*path/*]*filename*
cp [-r] [*path/*]*orig_filename* [*dest_path/*]*dupl_filename*
mv {[*path/*]*filename dest_path*[*/new_filename*] | [*path/*]*dir dest_path*[*/new_dir*]}
move {[*path/*]*filename dest_path*[*/new_filename*] | [*path/*]*dir dest_path*[*/new_dir*]}
chmod { +w | -w } [*path/*]*file*
attrib { +w | -w } [*path/*]*file*
freespace [*/flash*]
fsck */flash*
newfs */flash*
rcp *slot source_filepath destination_file*
rrm *slot filepath*
rls *slot directory* [*file_name*]
rdf {*slot*}
vi [*path/*]*filename*
view [*path/*]*filename*
tty *lines columns*
show tty
more [*path/*]*file*
ftp {*host_name* | *ip_address***}**
rz
install *file* [*argument*]

Web Management Commands

{[ip] http | https} server
no {[ip] http | https} server
{[ip] http | https} ssl
no {[ip] http | https} ssl
debug http sessiondb
show [ip] http

Configuration File Manager Commands

configuration apply *filename* [at *hh:mm month dd* [*year*]] | [in *hh*[*:mm*]] [verbose]
configuration error-file limit *number*
show configuration status
configuration cancel
configuration syntax check *path/filename* [verbose]
configuration snapshot *feature_list* [*path/filename*]
show configuration snapshot [*feature_list*]

write terminal

SNMP Commands

snmp station *ip_address* {[*udp_port*] [*username*] [v1 | v2 | v3] [enable | disable]}
no snmp station *ip_address*
show snmp station
snmp community map *community_string* {[user *useraccount_name*] | {enable | disable}}
no snmp community map *community_string*
snmp community map mode {enable | disable}
show snmp community map
snmp security {no security | authentication set | authentication all | privacy set | privacy all | trap only}
show snmp security
show snmp statistics
show snmp mib family [*table_name*]
snmp trap absorption {enable | disable}
snmp trap to webview {enable | disable}
snmp trap replay *ip_address* {*seq_id*}
snmp trap filter *ip_address trap_id_list*
no snmp trap filter *ip_address trap_id_list*
snmp authentication trap {enable | disable}
show snmp trap replay
show snmp trap filter
show snmp authentication trap
show snmp trap config

Hardware Routing Engine (HRE) Commands

hre mode configuration *slot/slice mode* [*number hash_function*]
hre clear changes {all | *slot/slice mode*}
hre apply changes
show hre changes *slot/slice*
show hre configuration *slot/slice*
show hre pcam utilization *slot/slice*
show hre statistics *slot/slice*
show hre cache utilization *slot/slice*

DNS Commands

ip domain-lookup
no ip domain-lookup
ip name-server *server-address1* [*server-address2* [*server-address3*]]
ip domain-name *name*
no ip domain-name
show dns

Link Aggregation Commands

static linkagg *agg_num* size *size* [name *name*] [admin state {enable | disable}]
no static linkagg *agg_num*
static linkagg *agg_num* name *name*
static linkagg *agg_num* no name
static linkagg *agg_num* admin state {enable | disable}
static agg [ethernet | fastethernet | gigaethernet] *slot*/*port* agg num *agg_num*
static agg no [ethernet | fastethernet | gigaethernet] *slot*/*port*
lacp linkagg *agg_num* size *size*
no lacp linkagg *agg_num*
lacp linkagg *agg_num* name *name*
lacp linkagg *agg_num* no name
lacp linkagg *agg_num* admin state {enable | disable}
lacp linkagg *agg_num* actor admin key *actor_admin_key*
lacp linkagg *agg_num* no actor admin key
lacp linkagg *agg_num* actor system priority *actor_system_priority*
lacp linkagg *agg_num* no actor system priority
lacp linkagg *agg_num* actor system id *actor_system_id*
lacp linkagg *agg_num* no actor system id
lacp linkagg *agg_num* partner system id *partner_system_id*
lacp linkagg *agg_num* no partner system id
lacp linkagg *agg_num* partner system priority *partner_system_priority*
lacp linkagg *agg_num* no partner system priority
lacp linkagg *agg_num* partner admin key *partner_admin_key*
lacp linkagg *agg_num* no partner admin key
lacp agg [ethernet | fastethernet | gigaethernet] *slot*/*port* actor admin key *actor_admin_key*
lacp agg no [ethernet | fastethernet | gigaethernet] *slot*/*port*
lacp agg [ethernet | fastethernet | gigaethernet] *slot*/*port* actor admin state {[active] [timeout] [aggregate] [synchronize] [collect] [distribute] [default] [expire] | none}
lacp agg [ethernet | fastethernet | gigaethernet] *slot*/*port* actor admin state {[[no] active] [[no] timeout] [[no] aggregate] [[no] synchronize] [[no] collect] [[no] distribute] [[no] default] [[no] expire] | none}
lacp agg [ethernet | fastethernet | gigaethernet] *slot*/*port* actor system id *actor_system_id*
lacp agg [ethernet | fastethernet | gigaethernet] *slot*/*port* no actor system id
lacp agg [ethernet | fastethernet | gigaethernet] *slot*/*port* actor system priority *actor_system_priority*
lacp agg [ethernet | fastethernet | gigaethernet] *slot*/*port* no actor system priority

lacp agg [ethernet | fastethernet | gigaethernet] *slot*/*port* partner admin state {[active] [timeout] [aggregate] [synchronize] [collect] [distribute] [default] [expire] | none}
lacp agg [ethernet | fastethernet | gigaethernet] *slot*/*port* partner admin state {[[no] active] [[no] timeout] [[no] aggregate] [[no] synchronize] [[no] collect] [[no] distribute] [[no] default] [[no] expire] | none}
lacp agg [ethernet | fastethernet | gigaethernet] *slot*/*port* partner admin system id *partner_admin_system_id*
lacp agg [ethernet | fastethernet | gigaethernet] *slot*/*port* no partner admin system id
lacp agg [ethernet | fastethernet | gigaethernet] *slot*/*port* partner admin key *partner_admin_key*
lacp agg [ethernet | fastethernet | gigaethernet] *slot*/*port* no partner admin key
lacp agg [ethernet | fastethernet | gigaethernet] *slot*/*port* partner admin system priority *partner_admin_system_priority*
lacp agg [ethernet | fastethernet | gigaethernet] *slot*/*port* no partner admin system priority
lacp agg [ethernet | fastethernet | gigaethernet] *slot*/*port* actor port priority *actor_port_priority*
lacp agg [ethernet | fastethernet | gigaethernet] *slot*/*port* no actor port priority
lacp agg [ethernet | fastethernet | gigaethernet] *slot*/*port* partner admin port *partner_admin_port*
lacp agg [ethernet | fastethernet | gigaethernet] *slot*/*port* no partner admin port
lacp agg [ethernet | fastethernet | gigaethernet] *slot*/*port* partner admin port priority *partner_admin_port_priority*
lacp agg [ethernet | fastethernet | gigaethernet] *slot*/*port* no partner admin port priority
linkagg slot *slot* optimization {enable | disable}
linkagg slot *slot* single
linkagg slot *slot* multiple
show linkagg [*agg_num*]
show linkagg port [*slot*/*port*]
show linkagg slot *slot* optimization

Interswitch Protocol Commands

amap {enable | disable}
amap discovery [time] *seconds*
amap common [time] *seconds*
show amap

802.1Q Commands

vlan *vid* 802.1q {slot/port | aggregate_id} [*description*]
vlan *vid* no 802.1q {slot/port | aggregate_id}
vlan 802.1q *slot/port* frame type {all | tagged}
vlan 802.1q *slot/port* force tag internal {on | off}
debug 802.1q {slot/port | aggregate_id}
show 802.1q {slot/port | aggregate_id}

Distributed Spanning Tree Commands

bridge mode {flat | 1x1}
bridge [*instance*] protocol {stp | rstp | mstp}
bridge cist protocol {stp | rstp | mstp}
bridge 1x1 *vid* protocol {stp | rstp}
bridge mst region name *name*
bridge mst region no name
bridge mst region revision level *rev_level*
bridge mst region max hops *max_hops*
bridge msti *msti_id* [name *name*]
bridge no msti *msti_id*
bridge msti *msti_id* no name
bridge msti *msti_id* vlan *vid_range*
bridge msti *msti_id* no vlan *vid_range*
bridge [*instance*] priority *priority*
bridge cist priority *priority*
bridge mist *msti_id* priority *priority*
bridge 1x1 *vid* priority *priority*
bridge [*instance*] hello time *seconds*
bridge cist hello time *seconds*
bridge 1x1 *vid* hello time *seconds*
bridge [*instance*] max age *seconds*
bridge cist max age *seconds*
bridge 1x1 *vid* max age *seconds*
bridge [*instance*] forward delay *seconds*
bridge cist forward delay *seconds*
bridge 1x1 *vid* forward delay *seconds*
bridge *instance* bpdu-switching {enable | disable}
bridge path cost mode {auto | 32bit}
bridge *instance* {*slot/port* | *logical_port*} {enable | disable}
bridge cist {*slot/port* | *logical_port*} port {enable | disable}
bridge 1x1 *vid* {*slot/port* | *logical_port*} port {enable | disable}
bridge *instance* {*slot/port* | *logical_port*} priority *priority*

bridge **cist** {*slot/port* | *logical_port*} priority *priority*
bridge **msti** *msti_id* {*slot/port* | *logical_port*} priority *priority*
bridge **1x1** *vid* {*slot/port* | *logical_port*} priority *priority*
bridge *instance* {*slot/port* | *logical_port*} path cost *path_cost*
bridge **cist** {*slot/port* | *logical_port*} path cost *path_cost*
bridge **mist** *msti_id* {*slot/port* | *logical_port*} path cost *path_cost*
bridge **1x1** *vid* {*slot/port* | *logical_port*} path cost *path_cost*
bridge *instance* {*slot/port* | *logical_port*} mode {forwarding | blocking | dynamic}
bridge cist {*slot/port* | *logical_port*} mode {dynamic | blocking | forwarding}
bridge 1x1 *vid* {*slot/port* | *logical_port*} mode {dynamic | blocking | forwarding}
bridge *instance* {*slot/port* | *logical_port*} connection {noptp | ptp | autoptp | edgeport}
bridge cist {*slot/port* | *logical_port*} connection {noptp | ptp | autoptp | edgeport}
bridge 1x1 *vid* {*slot/port* | *logical_port*} connection {noptp | ptp | autoptp | edgeport}
show spantree [*instance*]
show spantree cist
show spantree msti [*msti_id*]
show spantree 1x1 [*vid*]
show spantree [*instance*] ports [forwarding | blocking | active | configured]
show spantree cist ports [forwarding | blocking | active | configured]
show spantree msti [*msti_id*] ports [forwarding | blocking | active | configured]
show spantree 1x1 [*vid*] ports [forwarding | blocking | active | configured]
show spantree mst region
show spantree mst [*msti_id*] vlan-map
show spantree cist vlan-map
show spantree mst *vid* vlan-map
show spantree mst port {*slot/port* | *logical_port*}

Source Learning Commands

mac-address-table [permanent | reset | timeout] *mac_address* {*slot/port* | linkagg *link_agg*} *vid* [bridging | filtering]
no mac-address-table [permanent | reset | timeout | learned] *mac_address* {*slot/port* | **linkagg** *link_agg*} *vid*
mac-address-table static-multicast *multicast_address* {*slot1*/*port1*[-*port1a*] [*slot2/port2*[-*port2a*]...] | **linkagg** *link_agg*} *vid*
no mac-address-table static-multicast [*multicast_address* {*slot1*/*port1*[-*port1a*] [*slot2/port2*[-*port2a*]...] | **linkagg** *link_agg*} *vid*]
mac-address-table aging-time *seconds* [vlan *vid*]
no mac-address-table aging-time [vlan *vid*]
show mac-address-table [permanent | reset | timeout | learned] [*mac_address*] [slot *slot* | *slot/port*] [linkagg *link_agg*] [*vid*]
show mac-address-table static-multicast [*multicast_address*] [slot *slot* | *slot/port*] [linkagg *link_agg*] [*vid*]
show mac-address-table count [*mac_address*] [slot *slot* | *slot/port*] [linkagg *link_agg*] [*vid*]
show mac-address-table aging-time [vlan *vid*]

Learned Port Security Commands

port-security *slot/port* [enable | disable]
no port security *slot/port*
port-security shutdown *minutes*
port-security *slot/port* maximum *number*
port-security *slot/port* mac *mac_address*
port-security *slot/port* no mac *mac_address*
port-security *slot/port* mac-range [low *mac_address* | high *mac_address* | low *mac_address* high *mac_address*]
port-security *slot/port* violation {restrict | shutdown}
port-security *slot/port* release
show port-security [*slot/port* | *slot* | config-mac-range]
show port-security shutdown

Ethernet Port Commands

trap *slot*[/*port*[-*port2*]] port link {enable | disable | on | off}
flow [ethernet | fastethernet | gigaethernet] *slot*[/*port*[-*port2*]]
no flow [ethernet | fastethernet | gigaethernet] *slot*[/*port*[-*port2*]]
flow [ethernet | fastethernet | gigaethernet] *slot*[/*port*[-*port2*]] wait [time] *microseconds*
flow [ethernet | fastethernet | gigaethernet] *slot*[/*port*[-*port2*]] no wait [time]
interfaces [ethernet | fastethernet | gigaethernet] *slot*[/*port*[-*port2*]] speed {auto | 10 | 100 | 1000 | 10000 | max {100 | 1000}}
interfaces [ethernet | fastethernet | gigaethernet] *slot*[/*port*[-*port2*]] autoneg {enable | disable | on | off}
interfaces [ethernet | fastethernet | gigaethernet] *slot*[/*port*[-*port2*]] crossover {auto | mdix | mdi | disable}
interfaces [ethernet | fastethernet | gigaethernet] *slot*[/*port*[-*port2*]] flow {enable | disable | on | off}
interfaces [ethernet | fastethernet | gigaethernet] *slot*[/*port*[-*port2*]] duplex {full | half | auto}
interfaces [ethernet | fastethernet | gigaethernet] *slot*[/*port*[-*port2*]] admin {up | down}
interfaces [ethernet | fastethernet | gigaethernet] *slot*/*port* alias *description*
interfaces [ethernet | fastethernet | gigaethernet] *slot*[/*port*[-*port2*]] ifg *bytes*
interfaces [ethernet | fastethernet | gigaethernet] *slot*[/*port*[-*port2*]] no l2 statistics
interfaces [ethernet | fastethernet | gigaethernet] *slot*[/*port*[-*port2*]] long {enable | disable}
interfaces [gigaethernet] *slot*[/*port*[-*port2*]] max frame *bytes*
interfaces [ethernet | fastethernet | gigaethernet] *slot*[/*port*[-*port2*]] runt {enable | disable}
interfaces [ethernet | fastethernet | gigaethernet] *slot*[/*port*[-*port2*]] runtsize *framesize*
interfaces [ethernet | fastethernet | gigaethernet] *slot* flood

interfaces [ethernet | fastethernet | gigaethernet] *slot* flood multicast
interfaces [ethernet | fastethernet | gigaethernet] *slot*[/*port*[-*port2*]] flood rate *Mbps*
10gig slot *slot* {phy-a | phy-b}
show interfaces [ethernet | fastethernet | gigaethernet] [*slot*[/*port*[-*port2*]]] flow [control]
show interfaces [ethernet | fastethernet | gigaethernet] [*slot*[/*port*[-*port2*]]]
show interfaces [ethernet | fastethernet | gigaethernet] [*slot*[/*port*[-*port2*]]] capability
show interfaces [ethernet | fastethernet | gigaethernet] [*slot*[/*port*[-*port2*]]] accounting
show interfaces [ethernet | fastethernet | gigaethernet] [*slot*[/*port*[-*port2*]]] counters
show interfaces [ethernet | fastethernet | gigaethernet] [*slot*[/*port*[-*port2*]]] counters errors
show interfaces [ethernet | fastethernet | gigaethernet] [*slot*[/*port*[-*port2*]]] collisions
show interfaces [ethernet | fastethernet | gigaethernet] [*slot*[/*port*[-*port2*]]] status
show interfaces [ethernet | fastethernet | gigaethernet] [*slot*[/*port*[-*port2*]]] port
show interfaces [ethernet | fastethernet | gigaethernet] [*slot*[/*port*[-*port2*]]] ifg
show interfaces [ethernet | fastethernet | gigaethernet] [*slot*[/*port*[-*port2*]]] flood rate
show interfaces [ethernet | fastethernet | gigaethernet] [*slot*[/*port*[-*port2*]]] traffic
show 10gig [slot *slot*]
debug interfaces set [*slot*] backpressure {enable | disable}
debug interfaces [*slot*] backpressure

Port Mobility Commands

vlan *vid* dhcp mac *mac_address*
vlan *vid* no dhcp mac *mac_address*
vlan *vid* dhcp mac range *low_mac_address high_mac_address*
vlan *vid* no dhcp mac range *low_mac_address*
vlan *vid* dhcp port *slot/port*
vlan *vid* no dhcp port *slot/port*
vlan *vid* dhcp generic
vlan *vid* no dhcp generic
vlan *vid* binding mac-ip-port *mac_address ip_address slot/port*
vlan *vid* no binding mac-ip-port *mac_address*
vlan *vid* binding mac-port-protocol *mac_address slot/port* {ip-e2 | ip-snap | ipx-e2 | ipx-novell | ipx-llc | ipx-snap | decnet | appletalk | ethertype *type* | dsapssap *dsap/ssap* | snap *snaptype*}
vlan *vid* no binding mac-port-protocol *mac_address* {ip-e2 | ip-snap | ipx-e2 | ipx-novell | ipx-llc | ipx-snap | decnet | appletalk | ethertype *type* | dsapssap *dsap/ssap* | snap *snaptype*}
vlan *vid* binding mac-port *mac_address slot/port*
vlan *vid* no binding mac-port *mac_address*
vlan *vid* binding mac-ip *mac_address ip_address*
vlan *vid* no binding mac-ip *mac_address*
vlan *vid* binding ip-port *ip_address slot/port*
vlan *vid* no binding ip-port *ip_address*
vlan *vid* binding port-protocol *slot/port* {ip-e2 | ip-snap | ipv6 | ipx-e2 | ipx-novell | ipx-llc | ipx-snap | decnet | appletalk | ethertype *type* | dsapssap *dsap/ssap* | snap *snaptype*}
vlan *vid* no binding port-protocol *slot/port* {ip-e2 | ip-snap | ipx-e2 | ipx-novell | ipx-llc | ipx-snap | decnet | appletalk | ethertype *type* | dsapssap *dsap/ssap* | snap *snaptype*}
vlan *vid* mac *mac_address*
vlan *vid* no mac *mac_address*
vlan *vid* mac range *low_mac_address high_mac_address*
vlan *vid* no mac range *low_mac_address*
vlan *vid* ip *ip_address* [*subnet_mask*]
vlan *vid* no ip *ip_address* [*subnet_mask*]
vlan *vid* ipx *ipx_net* [e2 | llc | snap | novell]
vlan *vid* no ipx *ipx_net*
vlan *vid* protocol {ip-e2 | ip-snap | ipv6 | ipx-e2 | ipx-novell | ipx-llc | ipx-snap | decnet | appletalk |
ethertype *type* | dsapssap *dsap/ssap* | snap *snaptype*}
vlan *vid* no protocol {ip-e2 | ip-snap | ipx-e2 | ipx-nov | ipx-llc | ipx-snap | decnet | appletalk | ethertype *type* | dsapssap *dsap/ssap* | snap *snaptype*}
vlan *vid* user *offset value mask*
vlan *vid* no user *offset value*
vlan *vid* port *slot/port*
vlan *vid* no port *slot/port*
vlan port mobile *slot/port* [bpdu ignore {enable | disable}]
vlan no port mobile *slot/port*
vlan port *slot/port* default vlan restore {enable | disable}
vlan port *slot/port* default vlan {enable | disable}
vlan port *slot/port* authenticate {enable | disable}
vlan port *slot/port* 802.1x {enable | disable}
show vlan [*vid*] rules
show vlan port mobile [*slot/port*]

VLAN Management Commands

vlan *vid* [enable | disable] [name *description*]
no vlan *vid*
vlan *vid* [1x1 | flat] stp {enable | disable}
vlan *vid* mobile-tag {enable | disable}
vlan *vid* authentication {enable | disable}
vlan *vid* router ipx *ipx_net* [rip | active | inactive | triggered] [e2 | llc | snap | novell] [timeticks *ticks*]
vlan *vid* no router ipx
vlan router mac multiple {enable | disable}
vlan *vid* port default {*slot/port* | *link_agg*}
vlan *vid* no port default {*slot/port* | *link_agg*}
show vlan [*vid*]

show vlan [*vid*] port {*slot/port* | *link_agg*}
show vlan router mac status

Port Mapping Commands

port mapping *port_mapping_sessionid* {enable | disable}
no port mapping *port_mapping_sessionid*
show port mapping [*port_mapping_sessionid*]

IP Commands

ip interface *name* [address *ip_address*] [mask *subnet_mask*] [admin [enable | disable]] [vlan *vid*] [forward | no forward] [local-proxy-arp | no local-proxy-arp] [e2 | snap] [mtu *size*] [primary | no primary][firewall-vlan *vid*]
no ip interface *name*
ip router primary-address *ip_address*
ip router router-id *ip_address*
ip static-route *ip_address* [mask *mask*] gateway *gateway* [metric *metric*]
no ip static-route *ip_address* [mask *mask*] gateway *ip_address* [metric *metric*]
ip route-pref {static | ospf | rip | bgp} *value*
ip default-ttl *hops*
ping {*ip_address* | *hostname*} [count *count*] [size *packet_size*] [interval *seconds*] [timeout *seconds*]
traceroute {*ip_address* | *hostname*} [max-hop *max_hop_count*]
ip directed-broadcast {on | off}
ip service { all | ftp | ssh | telnet | http | secure-http | avlan-http | avlan-secure-http | avlan-telnet | udp-relay | network-time | snmp | port *service_port* }
no ip service { all | ftp | ssh | telnet | http | secure-http | avlan-http | avlan-secure-http | avlan-telnet | udp-relay | network-time | snmp | port *service_port*}
arp *ip_address mac_address* [alias]
no arp *ip_address* [alias]
clear arp-cache
arp filter *ip_address* [mask *ip_mask*] [*vid*] [sender | target] [allow | block]
no arp filter *ip_address*
clear arp-cache
icmp type *type* code *code* {{enable | disable} | min-pkt-gap *gap*}
icmp unreachable [net-unreachable | host-unreachable | protocol-unreachable | port-unreachable] {{enable | disable} | min-pkt-gap *gap*}
icmp echo [request | reply] {{enable | disable} | min-pkt-gap *gap*}
icmp timestamp [request | reply] {{enable | disable} | min-pkt-gap *gap*}
icmp add-mask [request | reply] {{enable | disable} | min-pkt-gap *gap*}
icmp messages {enable | disable}
ip dos scan close-port-penalty *penalty_value*
ip dos scan tcp open-port-penalty *penalty_value*
ip dos scan udp open-port-penalty *penalty_value*
ip dos scan threshold *threshold_value*
ip dos trap {enable | disable}
ip dos scan decay *decay_value*
show ip traffic
show ip interface [*name* | emp | vlan *vlan id*]
show ip route [summary]
Show ip route-pref [static | ospf | rip | bgp]
show ip router database [protocol *type* | gateway *ip_address* | dest *ip_address mask*]
show ip emp-route
show ip config
show ip protocols
show ip service
show arp [*ip_address* | *hardware_address*]
show arp filter [*ip_address*]
show icmp control
show icmp [statistics]
show tcp statistics
show tcp ports
show udp statistics
show udp ports
show ip dos config
show ip dos statistics
debug ip packet [start] [timeout *seconds*] [stop] [direction {in | out | all}] [format {header | text | all}] [output {console | file *filename*}] [board {cmm | ni [1-16] | all | none} [ether-type {arp | ip | hex [*hex_number*] | all}] [ip-address *ip_address*] [ip-address *ip_address*] [ip-pair [*ip1*] [*ip2*]] [protocol {tcp | udp | icmp | igmp | num [*integer*] | all}] [show-broadcast {on | off}] show-multicast {on | off}]
debug ip level *level*
debug ip packet default
debug ip packet

IPv6 Commands

ipv6 interface if_name [vlan vid | tunnel {tid | 6to4}] [enable | disable]
[mtu size]
[ra-send {yes | no}]
[ra-max-interval interval]
[ra-managed-config-flag {true | false}]
[ra-other-config-flag {true | false}]
[ra-reachable-time time]
[ra-retrans-timer time]
[ra-default-lifetime time | no ra-default-lifetime]
[ra-send-mtu] {yes | no}

no ipv6 interface if_name
ipv6 address *ipv6_address /prefix_length* [anycast] *{if_name | loopback}*
no ipv6 address *ipv6_address /prefix_length* [anycast] *{if_name | loopback}*
ipv6 address *ipv6_prefix/prefix_length* eui-64 *{if_name | loopback}*
no ipv6 address *ipv6_prefix/prefix_length* eui-64 *{if_name | loopback}*
ipv6 interface *if_name tunnel {[source ipv4_source] [destination ipv4_destination]}*
ipv6 dad-check *ipv6_address if_name*
ipv6 hop-limit *value*
no ipv6 hop-limit
ipv6 pmtu-lifetime *time*
ipv6 host *name ipv6_address*
no ipv6 host *name ipv6_address*
ipv6 neighbor *ipv6_address hardware_address {if_name} slot/port*
no ipv6 neighbor *ipv6_address {if_name}*
ipv6 prefix *ipv6_address /prefix_length if_name*
[valid-lifetime time]
[preferred-lifetime time]
[on-link-flag {true | false}
[autonomous-flag {true | false}] if_name
no ipv6 prefix *ipv6_address /prefix_length if_name*
ipv6 route *ipv6_prefix/prefix_length ipv6_address [if_name]*
no ipv6 route *ipv6_prefix/prefix_length ipv6_address [if_name]*
ping6 {*ipv6_address* | *hostname*} *[if_name]* [count *count*] [size *data_size*] [interval *seconds*]
traceroute6 {ipv6_address | hostname} [if_name] [max-hop *hop_count*] [wait-time time]
[port port_number] [probe-count probe]
debug ipv6 packet
[defaults]
[v6header {concise | verbose}]
[extheader {none | payload | concise | verbose}]
[etherheader {yes | no}]
[raw bytes]
[board {all | cmm | ni [slot_number] | none}]
[ether-filter mac_address | either-filter-pair mac_address mac_address | no ether-filter]
[ipv6-filter ipv6_address [/prefix_length] | ipv6-filter-pair ipv6_address [/prefix_length]
| no ipv6-filter]
[direction {all | in | out | from-cmm | from-ipv4 | to-cmm | to-ipv4}]
[output {console | file filename}]
no debug ipv6 packet
debug ipv6 trace-category [all | default | general | cmm-control | ni-data | ni-control | vlan |
tunnel | neighbor | route | mip | ipc | cd | pm | sm | monitor | rtadv]
no debug ipv6 trace-category [all | default | general | cmmcontrol | nidata | nicontrol | vlan |
tunnel | neigh | route | mip | ipc | cd | pm | sm | monitor | rtadv]
show ipv6 hosts [substring]
show ipv6 icmp statistics [if_name]
show ipv6 interface [if_name | loopback]
show ipv6 pmtu table
clear ipv6 pmtu table
show ipv6 neighbors [ipv6_prefix/prefix_length | if_name | hw hardware_address | static]
clear ipv6 neighbors
show ipv6 prefixes
show ipv6 routes [ipv6_prefix/prefix_length | static]
show ipv6 tcp ports
show ipv6 traffic [if_name]
clear ipv6 traffic
show ipv6 tunnel
show ipv6 udp ports
ipv6 load rip
ipv6 rip status {enable | disable}
ipv6 rip invalid-timer seconds
ipv6 rip garbage-timer seconds
ipv6 rip holddown-timer seconds
ipv6 rip jitter value
ipv6 rip route-tag value
ipv6 rip update-interval seconds
ipv6 rip triggered-sends {all | updated-only | none}
ipv6 rip interface if_name
[no] ipv6 rip interface if_name
ipv6 rip interface if_name metric value
ipv6 rip interface if_name recv-status {enable | disable}
ipv6 rip interface if_name send-status {enable | disable}
ipv6 rip interface if_name horizon {none | split-only | poison}
ipv6 rip debug-level level
ipv6 rip debug-type [error] [warning] [recv] [send] [rdb] [age] [mip] [info] [setup] [time] [tm]
[all]
show ipv6 rip
show ipv6 rip interface [if_name]
show ipv6 rip peer [ipv6_addresss]
show ipv6 rip routes [dest <ipv6_prefix/prefix_length>] | [gateway <ipv6_addr>] | [detail
<ipv6 prefix/prefix_length>]
show ipv6 rip debug

RDP Commands

ip router-discovery {enable | disable}
ip router-discovery interface {*name* | *ip_address*} [enable | disable]
no router-discovery interface {*name* | *ip_address*}
ip router-discovery interface {*name* | *ip_address*} advertisement-address {all-systems-
multicast | broadcast}

ip router-discovery interface {*name* | *ip_address*} max-advertisement-interval *seconds*
ip router-discovery interface {*name* | *ip_address*} min-advertisement-interval *seconds*
ip router-discovery interface {*name* | *ip_address*} advertisement-lifetime *seconds*
ip router-discovery interface {*name* | *ip_address*} preference-level *level*
show ip router-discovery
show ip router-discovery interface [*name* | *ip_address*]

DHCP Relay Commands

ip helper address *ip_address*
ip helper no address [*ip_address*]
ip helper address *ip_address* vlan *vlan_id*
ip helper no address *ip_address* vlan *vlan_id*
ip helper standard
ip helper avlan only
ip helper per-vlan only
ip helper forward delay *seconds*
ip helper maximum hops *hops*
ip helper agent-information {enable | disable}
ip helper agent-information policy {drop | keep | replace}
ip helper dhcp-snooping {enable | disable}
ip helper dhcp-snooping mac-address verification {enable | disable}
ip helper dhcp-snooping option-82 data-insertion {enable | disable}
ip helper dhcp-snooping vlan *vlan_id* [mac-address verification {enable | disable}] [option-82 data-insertion {enable | disable}]
no ip helper dhcp-snooping vlan *vlan_id*
ip helper dhcp-snooping port *slot1*/*port1*[-*port1a*] {block | client-only | trust}
ip helper dhcp-snooping port binding {[enable | disable] | [*mac_address* **port** *slot/port* **address** *ip_address* **lease-time** *time* **vlan** *vlan_id*]}
no ip helper dhcp-snooping port binding *mac_address* **port** *slot/port* **address** *ip_address* **lease-time** *time* **vlan** *vlan_id*
ip helper dhcp-snooping port binding timeout *seconds*
ip helper dhcp-snooping port binding action {purge | renew}
ip helper boot-up {enable | disable}
ip helper boot-up enable {BOOTP | DHCP}
ip udp relay {BOOTP | NBDD | NBNSNBDD | DNS | TACACS | TFTP | NTP | *port* [*name*]}
no ip udp relay {BOOTP | NBDD | NBNSNBDD | DNS | TACACS | TFTP | NTP | *port*}
ip udp relay {BOOTP | NBDD | NBNSNBDD | DNS | TACACS | TFTP | NTP | *port*} vlan *vlan_id*
no ip udp relay {BOOTP | NBDD | NBNSNBDD | DNS | TACACS | TFTP | NTP | *port*} vlan *vlan_id*
show ip helper
show ip helper stats
ip helper no stats
show ip helper dhcp-snooping vlan
show ip helper dhcp-snooping port
show ip helper dhcp-snooping binding
show ip udp relay service [BOOTP | NBDD | NBNSNBDD | DNS | TACACS | TFTP | NTP | *port*]
show ip udp relay [BOOTP | NBDD | NBNSNBDD | DNS | TACACS | TFTP | NTP | *port*]
show ip udp relay destination [BOOTP | NBDD | NBNSNBDD | DNS | TACACS | TFTP | NTP | *port*]

RIP Commands

ip load rip
ip rip status {enable | disable}
ip rip interface {*ip_address* | *interface_name*}
no ip rip interface {*ip_address* | *interface_name*}
ip rip interface *ip_address* status {enable | disable}
ip rip interface *ip_address* metric *value*
ip rip interface *ip_address* send-version {none | v1 | v1compatible | v2}
ip rip interface *ip_address* recv-version {v1 | v2 | both | none}
ip rip force-holddowntimer *seconds*
ip rip host-route
no ip rip host-route
ip rip route-tag *value*
ip rip redist status {enable | disable}
ip rip redist {local | static | ospf | bgp}
no ip rip redist {local | static | ospf | bgp}
ip rip redist {local | static | ospf | bgp} metric *value*
ip rip redist-filter {local | static | ospf | bgp} *ip_address ip_mask*
no ip rip redist-filter {local | static | ospf | bgp} *ip_address ip_mask*
ip rip redist-filter {local | static | ospf | bgp} *ip_address ip_mask* effect {permit | deny}
ip rip redist-filter {local | static | ospf | bgp} *ip_address ip_mask* metric *value*
ip rip redist-filter {local | static | osplf | bgp} *ip_address ip_mask* route-tag *value*
ip rip redist-filter {local | static | ospf | bgp} *ip_address ip_mask* redist-control {all-subnets | aggregate | no-subnets}
ip rip interface *ip_address* auth-type {none | simple | md5}
ip rip interface *ip_address* auth-key *string*
ip rip debug-type [error] [warning] [recv] [send] [rdb] [age] [redist] [info] [setup] [time] [tm] [all]
no ip rip debug-type [error] [warning] [recv] [send] [rdb] [age] [redist] [info] [setup] [time] [tm] [all]
ip rip debug-level *level*
show ip rip
show ip rip routes [*ip_address ip_mask*]
show ip rip interface [*ip_address*]

show ip rip peer [*ip_address*]
show ip rip redist [local] [static] [ospf] [bgp]
show ip rip redist-filter [local] [static] [ospf] [bgp]
show ip rip debug

IPX Commands

ipx routing
no ipx routing
ipx default-route *[vlan] network_number* [*network_node*]
no ipx default-route *[vlan]*
ipx route *network_number next_hop_network next_hop_node* [*hop_count*] [*delay*]
no ipx route *network_number*
clear ipx route {rip | sap | all}
ping ipx *network_number network_node [*count *packets] [*size *bytes] [*timeout *seconds] [*type *packet_type]*
ipx filter *[vlan]* rip {in | out} {allow | block} *[network_number [*mask *network_mask*]]
no ipx filter *[vlan]* rip {in | out} {allow | block} *[network_number [*mask *network_mask*]]
ipx filter *[vlan]* sap {all | *sap_type*} {in | out} {allow | block} *[network_number* [mask *network_mask*] *[network_node [*mask *node_mask]]]*
no ipx filter *[vlan]* sap {all | *sap_type*} {in | out} {allow | block} *[network_number* [mask *network_mask*] *[network_node [*mask *node_mask]]]*
ipx filter *[vlan]* gns {all | *gns_type*} out {allow | block} *[network_number* [mask *network_mask*] *[network_node [*mask *node_mask]]]*
no ipx filter *[vlan]* gns {all | *gns_type*} out {allow | block} *[network_number* [mask *network_mask*] *[network_node [*mask *node_mask]]]*
ipx type-20-propagation [*vlan*] {enable | disable}
no ipx type-20-propagation [*vlan]*
ipx packet-extension [*vlan*] {enable | disable}
no ipx packet-extension [*vlan]*
ipx timers [*vlan] rip_timer sap_timer*
no ipx timers [*vlan]*
show ipx interface [*vlan]*
show ipx traffic [*vlan]*
show ipx default-route
show ipx route {*network_number* | vlan *vlan*}
show ipx servers {vlan *vlan* | *server_name* | *server_type*}
show ipx filter {*vlan* | rip in | rip out | sap in | sap out | gns out | global}
show ipx type-20-propagation
show ipx packet-extension
show ipx timers

VRRP Commands

vrrp *vrid vlan_id* [enable | disable | on | off] [priority *priority*] [preempt | no preempt] [[advertising] interval *seconds*] [authenticate *password* | no authenticate]
no vrrp *vrid vlan_id*
vrrp *vrid vlan_id* ip *ip_address*
vrrp *vrid vlan_id* no ip *ip_address*
vrrp trap
no vrrp trap
vrrp delay *seconds*
vrrp track *track_id* [enable | disable] [priority *value*] {interface *name*} {vlan *vlan_id* | port *slot*/*port* | ip *ip_address*}
no vrrp track *track_id*
vrrp *vrid vlan_id* track-association *track_id*
vrrp *vrid vlan_id* no track-association *track_id*
show vrrp [*vrid*]
show vrrp [*vrid*] statistics
show vrrp track [*track_id*]
show vrrp [*vrid*] track-association [*track_id*]

OSPF Commands

ip ospf status {enable | disable}
ip load ospf
ip ospf asbr
no ip ospf asbr
ip ospf exit-overflow-interval *seconds*
ip ospf extlsdb-limit *limit*
ip ospf host *ip_address* tos *tos* [metric *metric*]
no ip ospf host *ip_address* tos *tos*
ip ospf mtu-checking
no ip ospf mtu-checking
ip ospf redist-filter {local | static | rip | bgp} *ip_address subnet_mask* [{[effect {permit | deny}] | [metric *value*] | [route-tag *tag*] | [redist-control {all-subnets | aggregate | no-subnets}]}]
no ip ospf redist-filter {local | static | rip | bgp} *ip_address subnet_mask*
ip ospf redist status {enable | disable}
ip ospf redist {local | static | rip | bgp} [metric *metric*] [metric-type {type1 | type2}] [subnets {enable | disable}]
no ip ospf redist {local | static | rip | bgp}
ip ospf route-tag *tag*
ip ospf spf-timer [delay *delay_seconds*] [hold *hold_seconds*]

ip ospf virtual-link *area_id router_id* [auth-type {none | simple | md5}] [auth-key *key_string*] [dead-interval *seconds*] [hello-interval *seconds*] [retrans-interval *seconds*] [transit-delay *seconds*]
no ip ospf virtual-link *area_id router_id*
ip ospf neighbor *neighbor_id* {eligible | non-eligible}
no ip ospf neighbor *neighbor_id*
ip ospf debug-level *level*
ip ospf debug-type [error] [warning] [state] [recv] [send] [flood] [spf] [lsdb] [rdb] [age] [vlink] [redist] [summary] [dbexch] [hello] [auth] [area] [intf] [mip] [info] [setup] [time] [tm] [restart] [helper] [all]
no ip ospf debug-type [error] [warning] [state] [recv] [send] [flood] [spf] [lsdb] [rdb] [age] [vlink] [redist] [summary] [dbexch] [hello] [auth] [area] [intf] [mip] [info] [setup] [time] [tm] [restart] [helper] [all]
ip ospf area *area_id* [summary {enable | disable}] | [type {normal | stub | nssa}]
no ip ospf area *area_id*
ip ospf area *area_id* status {enable | disable}
ip ospf area *area_id* default-metric *tos* [[cost *cost*] | [type {ospf | type 1 | type 2}]
no ip ospf area *area_id* default-metric *tos*
ip ospf area *area_id* range {summary | nssa} *ip_address subnet_mask* [effect {admatching | noMatching}]
no ip ospf area *area_id* range {summary | nssa} *ip_address subnet_mask*
ip ospf interface {*ip_address* | *interface_name*}
no ip ospf interface {*ip_address* | *interface_name*}
ip ospf interface {*ip_address* | *interface_name*} status {enable | disable}
no ip ospf interface {*ip_address* | *interface_name*} status {enable | disable}
ip ospf interface {*ip_address* | *interface_name*} area *area_id*
ip ospf interface {*ip_address* | *interface_name*} auth-key *key_string*
ip ospf interface {*ip_address* | *interface_name*} auth-type [none | simple | md5]
ip ospf interface {*ip_address* | *interface_name*} dead-interval *seconds*
ip ospf interface {*ip_address* | *interface_name*} hello-interval *seconds*
ip ospf interface {*ip_address* | *interface_name*} md5 *key_id* [enable | disable]
ip ospf interface {*ip_address* | *interface_name*} md5 *key_id* key *key_string*
ip ospf interface {*ip_address* | *interface_name*} type {point-to-point | point-to-multipoint | broadcast | non-broadcast}
ip ospf interface {*ip_address* | *interface_name*} cost *cost*
ip ospf interface {*ip_address* | *interface_name*} poll-interval *seconds*
ip ospf interface {*ip_address* | *interface_name*} priority *priority*
ip ospf interface {*ip_address* | *interface_name*} retrans-interval *seconds*
ip ospf interface {*ip_address* | *interface_name*} transit-delay *seconds*
ip ospf restart-support {planned-unplanned | planned-only}
no ip ospf restart-support
ip ospf restart-interval [*seconds*]
ip ospf restart-helper [status {enable | disable}]
ip ospf restart-helper strict-lsa-checking-status {enable | disable}
ip ospf restart initiate
show ip ospf
show ip ospf border-routers [*area_id*] [*router_id*] [*tos*] [*gateway*]
show ip ospf ext-lsdb [linkstate-id *ls_id*] [router-id *router_id*]
show ip ospf host [*ip_address*]
show ip ospf lsdb [*area_id*] [rtr | net | netsum | asbrsum] [linkstate-id *ls_id*] [router-id *router_id*]
show ip ospf neighbor [*ip_address*]
show ip redist-filter [local | static | rip | bgp] [*ip_address*] [*subnet_mask*]
show ip ospf redist [local | static | rip | bgp]
show ip ospf routes [*ip_addr mask tos gateway*]
show ip ospf virtual-link [*router_id*]
show ip ospf virtual-neighbor *area_id router_id*
show ip ospf area [*area_id*]
show ip ospf area *area_id* range [{summary | nssa} *ip_address ip_mask*]
show ip ospf area *area_id* stub
show ip ospf interface [*ip_address* | *interface_name*]
show ip ospf restart
show ip ospf debug

BGP Commands

ip load bgp
ip bgp status {enable | disable}
ip bgp autonomous-system *value*
ip bgp bestpath as-path ignore
no ip bgp bestpath as-path ignore
ip bgp cluster-id *ip_address*
ip bgp default local-preference *value*
ip bgp fast-external-failover
no ip bgp fast-external-failover
ip bgp always-compare-med
no ip bgp always-compare-med
ip bgp bestpath med missing-as-worst
no ip bgp bestpath med missing-as-worst
ip bgp client-to-client reflection
no ip bgp client-to-client reflection
ip bgp as-origin-interval *seconds*
no ip bgp as-origin-interval
ip bgp synchronization
no ip bgp synchronization
ip bgp confederation identifier *value*
ip bgp maximum-paths
no ip bgp maximum-paths

ip bgp log-neighbor-changes
no ip bgp log-neighbor-changes
ip bgp dampening [half-life *half_life* reuse *reuse* suppress *suppress* max-suppress-time *max_suppress_time*]
no ip bgp dampening
ip bgp dampening clear
ip bgp debug-type [warnings | tm | tcp | sync | sendudp | peer | redist | recvudp | policy | peer | open | notify | mip | local | keepalive | info | fsm | errors | damp | aggr | all]
ip bgp debug-level *level*
ip bgp aggregate-address *ip_address ip_mask*
no ip bgp aggregate-address *ip_address ip_mask*
ip bgp aggregate-address *ip_address ip_mask* status {enable | disable}
ip bgp aggregate-address *ip_address ip_mask* as-set
no ip bgp aggregate-address *ip_address ip_mask* as-set
ip bgp aggregate-address *ip_address ip_mask* community *string*
ip bgp aggregate-address *ip_address ip_mask* local-preference *value*
no ip bgp aggregate-address *ip_address ip_mask* local-preference *value*
ip bgp aggregate-address *ip_address ip_mask* metric *value*
no ip bgp aggregate-address *ip_address ip_mask* metric *value*
ip bgp aggregate-address *ip_address ip_mask* summary-only
no ip bgp aggregate-address *ip_address ip_mask* summary-only
ip bgp network *network_address ip_mask*
no ip bgp network network_address ip_mask
ip bgp network *network_address ip_mask* status {enable | disable}
ip bgp network *network_address ip_mask* community *string*
ip bgp network *network_address ip_mask* local-preference *value*
no ip bgp network *network_address ip_mask* local-preference *value*
ip bgp network *network_address ip_mask* metric *value*
no ip bgp network *network_address ip_mask* metric *value*
ip bgp neighbor *ip_address*
no ip bgp neighbor *ip_address*
ip bgp neighbor *ip_address* status {enable | disable}
ip bgp neighbor *ip_address* advertisement-interval *value*
ip bgp neighbor *ip_address* clear
ip bgp neighbor *ip_address* route-reflector-client
no ip bgp neighbor *ip_address* route-reflector-client
ip bgp neighbor *ip_address* default-originate
no ip bgp neighbor *ip_address* default-originate
ip bgp neighbor *ip_address* timers *keepalive holdtime*
ip bgp neighbor *ip_address* conn-retry-interval *seconds*
ip bgp neighbor *ip_address* auto-restart
ip bgp neighbor *ip_address* maximum-prefix *maximum* [warning-only]
ip bgp neighbor *ip_address* md5 key {*string* | none}
ip bgp neighbor *ip_address* md5 key-encrypt *encrypted_string*
ip bgp neighbor *ip_address* ebgp-multihop [*ttl*]
no ip bgp neighbor *ip_address* ebgp-multihop
ip bgp neighbor *ip_address* description *string*
ip bgp neighbor *ip_address* next-hop-self
no ip bgp neighbor *ip_address* next-hop-self
ip bgp neighbor *ip_address* passive
no ip bgp neighbor *ip_address* passive
ip bgp neighbor *ip_address* remote-as *value*
ip bgp neighbor *ip_address* remove-private-as
no ip bgp neighbor *ip_address* remove-private-as
ip bgp neighbor *ip_address* soft-reconfiguration
no ip bgp neighbor *ip_address* soft-reconfiguration
ip bgp neighbor *ip_address* stats-clear
ip bgp confederation neighbor *ip_address*
no ip bgp confederation neighbor *ip_address*
ip bgp neighbor *ip_address* update-source [*interface_address* | *interface_name*]
ip bgp neighbor *ip_address* in-aspathlist {*string* | none}
ip bgp neighbor *ip_address* in-communitylist {*string* | none}
ip bgp neighbor *ip_address* in-prefixlist {*string* | none}
ip bgp neighbor *ip_address* out-aspathlist {*string* | none}
ip bgp neighbor *ip_address* out-communitylist {*string* | none}
ip bgp neighbor *ip_address* out-prefixlist {*string* | none}
ip bgp neighbor *ip_address* route-map {*string* | none} {in | out}
no ip bgp neighbor *ip_address* route-map {in | out}
ip bgp neighbor *ip_address* clear soft {in | out}
ip bgp policy aspath-list *name* "*regular_expression*"
no ip bgp policy aspath-list *name* "*regular_expression*"
ip bgp policy aspath-list *name* **"***regular_expression***"** action {permit | deny}
ip bgp policy aspath-list *name* "*regular_expression*" priority *value*
ip bgp policy community-list *name* {none | no-export | no-advertise | no-export-subconfed | *num:num*}
no ip bgp policy community-list *name* {none | no-export | no-advertise | no-export-subconfed | *num:num*}
ip bgp policy community-list *name* {none | no-export | no-advertise | no-export-subconfed | *num:num*}
action {permit | deny}
ip bgp policy community-list *name* {none | no-export | no-advertise | no-export-subconfed | *num:num*}
match-type {exact | occur}
ip bgp policy community-list *name* {none | no-export | no-advertise | no-export-subconfed | *num:num*}
priority *value*
ip bgp policy prefix-list *name ip_address ip_mask*
no ip bgp policy prefix-list *name ip_address ip_mask*

ip bgp policy prefix-list *name ip_address ip_mask* action {permit | deny}
ip bgp policy prefix-list *name ip_address ip_mask* ge *value*
ip bgp policy prefix-list *name ip_address ip_mask* le *value*
ip bgp policy route-map *name sequence_number*
ip bgp policy route-map *name sequence_number* action {permit | deny}
ip bgp policy route-map *name sequence_number* aspath-list *as_name*
ip bgp policy route-map *name sequence_number* asprepend *path*
ip bgp policy route-map *name sequence_number* community [none | no-export | no-advertise | no-export-subconfed | *num*:*num*]
ip bgp policy route-map *name sequence_number* community-list *name*
ip bgp policy route-map *name sequence_number* community-mode {add | replace}
ip bgp policy route-map *name sequence_number* lpref *value*
ip bgp policy route-map *name sequence_number* lpref-mode {none | inc | dec | rep}
ip bgp policy route-map *name sequence_number* match-community [none | no-export | no-advertise | no-export-subconfed | *num:num*]
ip bgp policy route-map *name sequence_number* match-mask *ip_address*
ip bgp policy route-map *name sequence_number* match-prefix *ip_address*
ip bgp policy route-map *name sequence_number* match-regexp "*regular_expression*"
ip bgp policy route-map *name sequence_number* med *value*
ip bgp policy route-map *name sequence_number* med-mode {none | inc | dec | rep}
ip bgp policy route-map *name sequence_number* origin {igp | egp| incomplete | none}
ip bgp policy route-map *name sequence_number* prefix-list *prefix_name*
ip bgp policy route-map *name sequence_number* weight *value*
ip bgp policy route-map *name sequence_number* community-strip *community_list*
ip bgp redist-filter {local | static | rip | ospf} *ip_address ip_mask*
no ip bgp redist-filter {local | static | rip | ospf} *ip_address ip_mask*
ip bgp redist-filter {local | static | rip | ospf} *ip_address ip_mask* community *community_string*
ip bgp redist-filter {local | static | rip | ospf} *ip_address ip_mask* effect {permit | deny}
ip bgp redist-filter {local | static | rip | ospf} *ip_address ip_mask* local-preference *value*
ip bgp redist-filter {local | static | rip | ospf} *ip_address ip_mask* metric *value*
ip bgp redist-filter {local | static | rip | ospf} *ip_address ip_mask* subnets
no ip bgp redist-filter {local | static | rip | ospf} *ip_address ip_mask* subnets
show ip bgp
show ip bgp statistics
show ip bgp dampening
show ip bgp dampening-stats [*ip_address ip_mask] [peer_address*]
show ip bgp path
show ip bgp routes [*network_address ip_mask*]
show ip bgp debug
show ip bgp aggregate-address [*ip_address ip mask*]
show ip bgp network [*network_address ip_mask*]
show ip bgp neighbors [*ip_address*]
show ip bgp neighbors policy [*ip_address*]
show ip bgp neighbors timer [*ip_address*]
show ip bgp neighbors statistics [*ip_address*]
show ip bgp policy aspath-list [*name*] [*"regular_expression"*]
show ip bgp policy community-list [*name*] [*string*]
show ip bgp policy prefix-list [*name*] [*ip_address ip_mask*]
show ip bgp policy route-map [*name*] [*sequence_number*]
show ip bgp redist-filter [local] [static] [rip] [ospf]

PIM-SM Commands

ip load pimsm
ip pimsm status {enable | disable}
ip pimsm cbsr-masklength *bits*
ip pimsm static-rp status {enable | disable}
ip pimsm static-rp *group_address mask rp_address*
no ip pimsm static-rp *group_address mask rp_address*
ip pimsm rp-candidate *group_address mask rp_address*
no ip pimsm rp-candidate *group_address mask rp_address*
ip pimsm rp-threshold *bps*
ip pimsm crp-address *ip_address*
no ip pimsm crp-address
ip pimsm crp-expirytime *seconds*
ip pimsm crp-holdtime *seconds*
ip pimsm crp-interval *seconds*
ip pimsm crp-priority *priority*
ip pimsm data-timeout *seconds*
ip pimsm joinprune-interval *seconds*
ip pimsm max-rps *number*
ip pimsm probe-time *seconds*
ip pimsm register checksum {header | full}
ip pimsm registersuppress-timeout *seconds*
ip pimsm spt status {enable | disable}
ip pimsm interface *ip_address*
no ip pimsm interface *ip_address*
ip pimsm interface *ip_address* hello-interval *seconds*
ip pimsm interface *ip_address* joinprune-interval *seconds*
ip pimsm interface *ip_address* cbsr-preference *value*
ip pimsm interface *ip_address* dr-priority *priority*
ip pimsm interface *ip_address* prune-delay status {enable | disable}
ip pimsm interface *ip_address* prune-delay *milliseconds*
ip pimsm interface *ip_address* override-interval *milliseconds*
ip pimsm interface *ip_address* triggered-hello *seconds*
ip pimsm interface *ip_address* hello-holdtime *seconds*
ip pimsm interface *ip_address* genid {enable | disable}

ip pimsm interface *ip_address* joinprune-holdtime *seconds*
ip pimsm debug-level *level*
ip pimsm debug-type *message_list*
no ip pimsm debug-type *message_list*
show ip pimsm
show ip pimsm neighbor [*ip_address*]
show ip pimsm rp-candidate
show ip pimsm rp-set
show ip pimsm interface [*ip_address*]
show ip pimsm nexthop [*group_address source_address mask nexthop_address*]
show ip pimsm mroute [*group_address source_address mask*]
show ip pimsm static-rp
show ip pimsm debug

DVMRP Commands

ip load dvmrp
ip dvmrp status {enable | **safe-enable| unrestricted-enable |** disable}
ip dvmrp flash-interval *seconds*
ip dvmrp graft-timeout *seconds*
ip dvmrp interface {*ip_address* | *interface_name*}
no ip dvmrp interface {*ip_address* | *interface_name*}
ip dvmrp interface {*ip_address* | *interface_name*} metric *value*
ip dvmrp neighbor-interval *seconds*
ip dvmrp neighbor-timeout *seconds*
ip dvmrp prune-lifetime *seconds*
ip dvmrp prune-timeout *seconds*
ip dvmrp report-interval *seconds*
ip dvmrp route-holddown *seconds*
ip dvmrp route-timeout *seconds*
ip dvmrp subord-default {true | false}
ip dvmrp tunnel {*local_address* | *local_name*} {*remote_address* | *remote_name*}
no ip dvmrp tunnel {*local_address* | *local_name*} {*remote_address* | *remote_name*}
ip dvmrp tunnel {*local_address remote_address* | *interface_name*} ttl *value*
ip dvmrp debug-level *level*
ip dvmrp debug-type *message_type*
no ip dvmrp debug-type *message_type*
show ip dvmrp
show ip dvmrp interface [{*ip_address* | *interface_name* } | enabled | disabled]
show ip dvmrp neighbor [*ip_address*]
show ip dvmrp nexthop [*ip_address ip_mask*]
show ip dvmrp prune [*group_address source_address source_mask*]
show ip dvmrp route [*ip_address ip_mask*]
show ip dvmrp tunnel [*local_address remote_address*]
show ip dvmrp debug

Multicast Routing Commands

ip mroute-boundary *ip_address scoped_address mask*
no ip mroute-boundary *ip_address scoped_address mask*
ip mroute interface *ip_address* ttl *threshold*
show ip mroute-boundary
show ip mroute
show ip mroute interface
show ip mroute-nexthop
ip mroute debug-level *level*
ip mroute debug-type *message_list*
no ip mroute debug-type *message_list*
show ip mroute debug

Port Mirroring and Monitoring Commands

port mirroring *port_mirror_sessionid* [no] source *slot/port*[-*port2*] [*slot/port*[-*port2*]...]
destination *slot/port* [bidirectional |inport |outport] [unblocked *vlan_id*] [enable | disable]
port mirroring *port_mirror_sessionid* {enable | disable}
no port mirroring *port_mirror_sessionid* {enable | disable}
port monitoring *port_monitor_sessionid* source *slot/port*
[{no file | file *filename* [size *filesize*] | [overwrite {on | off}]}]
[inport | outport | bidirectional] [timeout *seconds*] [enable | disable]
port monitoring *port_monitor_sessionid* {disable | pause | resume}
no port monitoring *port_monitor_sessionid*
show port mirroring status [*port_mirror_sessionid*]
show port monitoring status [*port_monitor_sessionid*]
show port monitoring file [*port_monitor_sessionid*]

RMON Commands

rmon probes {stats | history | alarm} [*entry-number*] {enable | disable}
show rmon probes [stats | history | alarm] [*entry-number*]
show rmon events [*event-number*]

Health Monitoring Commands

health threshold {rx *percent* | txrx *percent* | memory *percent* | cpu *percent* | temperature *degrees*}
health interval *seconds*
health statistics reset

show health threshold [rx | txrx | memory | cpu | temperature]
show health interval
show health [*slot/port*] [statistics]
show health all {memory | cpu | rx | txrx}
show health slice *slot*

QoS Commands

qos {enable | disable}
qos trust ports
qos no trust ports
qos default queues {2 | 4}
qos forward log
qos no forward log
qos log console
qos no log console
qos log lines *lines*
qos log level *level*
qos no log level
qos classifyl3 bridged
qos no classifyl3 bridged
qos classify fragments
qos no classify fragments
qos flow timeout *seconds*
qos fragment timeout *seconds*
qos reflexive timeout *seconds*
qos no reflexive timeout
qos nat timeout *seconds*
qos default bridged disposition {accept | deny | drop}
qos default routed disposition {accept | deny | drop}
qos default multicast disposition {accept | deny | drop}
qos stats interval *seconds*
debug qos [info] [config] [rule] [main] [route] [hre] [port] [msg] [sl] [ioctl] [mem] [cam] [mapper] [flows] [queue] [slot] [l2] [l3] [classifier] [nat] [sem] [pm] [ingress] [egress] [rsvp] [balance] [nimsg]
debug no qos
debug no qos [info] [config] [rule] [main] [route] [hre] [port] [msg] [sl] [ioctl] [mem] [cam] [mapper] [flows] [queue] [slot] [l2] [l3] [classifier] [nat] [sem] [pm] [ingress] [egress] [rsvp] [balance] [nimsg]
debug qos internal [slice *slot/slice*] [flow] [queue] [port] [l2tree] [l3tree] [vector] [pending] [verbose] [mapper] [pool] [log] [pingonly | nopingonly]
qos clear log
qos apply
qos revert
qos flush
qos reset
qos stats reset
policy rule *rule_name* [enable | disable] [precedence *precedence*] [condition *condition*] [action *action*] [reflexive] [save] [log]
no policy rule *rule_name*
policy rule *rule_name* [no reflexive] [no save] [no log]
policy network group *net_group ip_address* [mask *net_mask*] [*ip_address2* [mask *net_mask2*]...]
no policy network group *net_group*
policy network group *net_group* no *ip_address* [mask *netmask*] [*ip_address2* [mask *net_mask2*]...]
policy service group *service_group service_name1* [*service_name2*...]
no policy service group *service_group*
policy service group *service_group* no *service_name1* [*service_name2*...]
policy mac group *mac_group mac_address* [mask *mac_mask*] [*mac_address2* [mask *mac_mask2*]...]
no policy mac group *mac_group*
policy mac group *mac_group* no *mac_address* [mask *mac_mask*] [*mac_address2* [mask *mac_mask2*]...]
policy port group *group_name slot*/*port*[-*port*] [*slot/port*[-*port*]...]
no policy port group *group_name*
policy port group *group_name* no *slot/port*[-*port*] [*slot/port*[-*port*]...]
policy service *service_name*
no policy service *service_name*
policy service *service_name* protocol *protocol* {[source ip port *port*[-*port*]] [destination ip port *port*[-*port*]]}
no policy service *service_name*
policy service *service_name* [no source ip port] [no destination ip port]
policy service *service_name* source tcp port *port*[-*port*]
no policy service *service_name*
policy service *service_name* no source tcp port
policy service *service_name* destination tcp port *port*[-*port*]
no policy service *service_name*
policy service *service_name* no destination tcp port
policy service *service_name* source udp port *port*[-*port*]
no policy service *service_name*
policy service *service_name* no source udp port
policy service *service_name* destination udp port *port*[-*port*]
no policy service *service_name*
policy service *service_name* no destination udp port
policy map group *map_group* {*value1*:*value2*...}
no policy map group *map_group*
policy map group no {*value1*:*value2*...}

policy condition *condition_name*
no policy condition *condition_name*
policy condition *condition_name* source ip *ip_address* [mask *netmask*]
policy condition *condition_name* no source ip
policy condition *condition_name* destination ip *ip_address* [mask *netmask*]
policy condition *condition_name* no destination ip
policy condition *condition_name* multicast ip *ip_address* [mask *netmask*]
policy condition *condition_name* no multicast ip
policy condition *condition_name* source network group *network_group*
policy condition *condition_name* no source network group
policy condition *condition_name* destination network group *network_group*
policy condition *condition_name* no destination network group
policy condition *condition_name* multicast network group *multicast_group*
policy condition *condition_name* no multicast network group
policy condition *condition_name* source ip port *port*[*-port*]
policy condition *condition_name* no source ip port
policy condition *condition_name* destination ip port *port*[*-port*]
policy condition *condition_name* no destination ip port
policy condition *condition_name* source tcp port *port*[*-port*]
policy condition *condition_name* no source tcp port
policy condition *condition_name* destination tcp port *port*[*-port*]
policy condition *condition_name* no destination tcp port
policy condition *condition_name* source udp port *port*[*-port*]
policy condition *condition_name* no source udp port
policy condition *condition_name* destination udp port *port*[*-port*]
policy condition *condition_name* no destination udp port
policy condition *condition_name* ethertype *etype*
policy condition *condition_name* no ethertype
policy condition *condition_name* service *service_name*
policy condition *condition_name* no service
policy condition *condition_name* service group *service_group*
policy condition *condition_name* no service group
policy condition *condition_name* ip protocol *protocol*
policy condition *condition_name* no ip protocol
policy condition *condition_name* source mac *mac_address* [mask *mac_mask*]
policy condition *condition_name* no source mac
policy condition *condition_name* destination mac *mac_address* [mask *mac_mask*]
policy condition *condition_name* no destination mac
policy condition *condition_name* source mac group *group_name*
policy condition *condition_name* no source mac group
policy condition *condition_name* destination mac group *mac_group*
policy condition *condition_name* no destination
policy condition *condition_name* source vlan *vlan_id*
policy condition *condition_name* no source vlan
policy condition *condition_name* destination vlan *vlan_id*
policy condition *condition_name* no destination vlan
policy condition *condition_name* source port *slot/port*[*-port*]
policy condition *condition_name* no source port
policy condition *condition_name* destination port *slot/port*[*-port*]
policy condition *condition_name* no destination port
policy condition *condition_name* source port group *group_name*
policy condition *condition_name* no source port group
policy condition *condition_name* destination port group *group_name*
policy condition *condition_name* no destination port
policy condition *condition_name* source interface type {ethernet | wan | ethernet-10 | ethernet-100 | ethernet-1G | ethernet-10G}
policy condition *condition_name* no source interface type
policy condition *condition_name* destination interface type {ethernet | wan | ethernet-10 | ethernet-100 | ethernet-1G | ethernet-10G}
policy condition *condition_name* no destination interface type
policy action *action_name*
policy no action *action_name*
policy action *action_name* disposition {accept | drop | deny}
policy action *action_name* no disposition
policy action *action_name* shared
policy action *action_name* no shared
policy action *action_name* priority *priority_value*
policy action *action_name* no priority
policy action *action_name* maximum bandwidth *bps*
policy action *action_name* no maximum bandwidth
policy action *action_name* maximum buffers *max_buffers*
policy action *action_name* no maximum buffers
policy action *action_name* minimum depth *bytes*
policy action *action_name* no minimum depth
policy action *action_name* maximum depth *bytes*
policy action *action_name* no maximum depth
policy action *action_name* tos *tos_value*
policy action *action_name* no tos
policy action *action_name* 802.1p *802.1p_value*
policy action *action_name* no 802.1p
policy action *action_name* dscp *dscp_value*
policy action *action_name* no dscp
policy action map {802.1p | tos | dscp} to {802.1p | tos| dscp} using *map_group*
policy action no map
policy action *action_name* source rewrite ip *ip_address* [mask *netmask*]
policy action *action_name* no source rewrite ip
policy action *action_name* source rewrite network group *network_group*
policy action *action_name* no source rewrite network group

policy action *action_name* destination rewrite ip *ip_address* [mask *netmask*]
policy action *action_name* no destination rewrite ip
policy action *action_name* destination rewrite network group *network_group*
policy action *action_name* no destination rewrite network group
policy action *action_name* load balance group *slb_cluster*
policy action *action_name* no load balance group
policy action *action_name* alternate gateway ip *ip_address*
policy action *action_name* no alternate gateway ip
policy action *action_name* permanent gateway ip *ip_address*
policy action *action_name* no permanent gateway ip
qos port *slot/port* reset
qos port *slot/port*
qos port *slot/port* default queues [2 | 4]
qos port *slot/port* trusted
qos port *slot/port* no trusted
qos port *slot/port* maximum reserve bandwidth *bps*
qos port *slot/port* no maximum reserve bandwidth
qos port *slot/port* maximum signal bandwidth *bps*
qos port *slot/port* no maximum signal bandwidth
qos port *slot/port* maximum default depth *bytes*
qos port *slot/port* no maximum default depth
qos port *slot/port* maximum default buffers *max_default_buffers*
qos port *slot/port* no maximum default buffers
qos port *slot/port* default 802.1p *value*
qos port *slot/port* default dscp *value*
qos port *slot/port* default classification {802.1p | tos | dscp}
qos port *slot/port* enqueuing thresholds *up0-low0 up1-low1 up2-low2 up3-low3*
qos port *slot/port* no enqueuing thresholds
qos port *slot/port* protocol *id* [priority {*p0 p1 p2 p3 p4 p5 p6 p7*}] [classification {tos | 802.1p | dscp}]
qos port *slot/port* no protocol *id*
qos slice *slot/slice* protocol *id* ethertype *etype* [dsapssap *dsap/ssap*] [802.3 {enable | disable}] [priority | fallback]
qos slice *slot/slice* no protocol *id*
qos slice *slot/slice* dscp *index value*
qos slice *slot/slice* servicing mode {strict-priority | wrr | priority-wrr [*p1 p2 p3*]}
qos slice *slot/slice* wred thresholds *up0-low0 up1-low1 up2-low2 up3-low3* [weight *weight_value*]
qos slice *slot/slice* no wred thresholds
show policy classify {l2 | l3 | multicast} [applied]
show policy classify {l2 | l3 | multicast} [applied] source port *slot/port*
show policy classify {l2 | l3 | multicast} [applied] source mac *mac_address*
show policy classify {l2 | l3 multicast} [applied] destination mac *mac_address*
show policy classify {l2 | l3 | multicast} [applied] source vlan *vlan_id*
show policy classify {l2 | l3 | multicast} [applied] destination vlan *vlan_id*
show policy classify {l2 | l3 | multicast} [applied] source interface type {ethernet | wan | ethernet-10 | ethernet-100 | ethernet-1G | ethernet-10G}
show policy classify {l2 | l3 | multicast} [applied] source ip *ip_address*
show policy classify {l2 | l3 | multicast} [applied] destination ip *ip_address*
show policy classify {l2 | l3 | multicast} [applied] multicast ip *ip_address*
show policy classify {l2 | l3 | multicast} [applied] tos *tos_value*
show policy classify {l2 | l3 | multicast} [applied] dscp *dscp_value*
show policy classify {l2 | l3 | multicast} [applied] ip protocol *protocol*
show policy classify {l2 | l3 | multicast} [applied] source ip port *port*
show policy classify {l2 | l3 | multicast} [applied] destination ip port *port*
show [applied] policy network group [*network_group*]
show [applied] policy service [*service_name*]
show [applied] policy service group [*service_group*]
show [applied] policy mac group [*mac_group*]
show [applied] policy port group [*group_name*]
show [applied] policy map group [*group_name*]
show [applied] policy action [*action_name*]
show [applied] policy condition [*condition_name*]
show active [bridged | routed | multicast] policy rule [*rule_name*]
show [applied] [bridged | routed | multicast] policy rule [*rule_name*]
show qos port [*slot/port*] [statistics]
show qos port [*slot/port*] [statistics]
show qos port [*slot/port*] [statistics] high-density-module
show qos port [*slot/port*] pdis
show qos queue
show qos slice [*slot/slice*]
show qos slice [*slot/slice*] high-density-module
show qos slice [*slot/slice*] pcams
show qos log
show qos config
show qos statistics

Policy Server Commands

policy server load
policy server flush
policy server *ip_address* [port *port_number*] [admin {up | down}] [preference *preference*] [user *user_name* password *password*] [searchbase *search_string*] [ssl | no ssl]
no policy server *ip_address* [port *port_number*]
show policy server
show policy server long
show policy server statistics

show policy server rules
show policy server events

IP Multicast Switching Commands

ip multicast switching
no ip multicast switching
ip multicast igmp-proxy-version {v2 | v3}
ip multicast no igmp-proxy-version
ip multicast leave-timeout *seconds*
ip multicast no leave-timeout
ip multicast query-interval *seconds*
ip multicast no query-interval
ip multicast membership-timeout *seconds*
ip multicast no membership-timeout
ip multicast neighbor-timeout *seconds*
ip multicast no neighbor-timeout
ip multicast querier-timeout *seconds*
ip multicast no querier-timeout
ip multicast other-querier-timeout *seconds*
ip multicast no other-querier-timeout
ip multicast flow-timeout seconds
ip multicast priority {urgent | high | medium | low}
ip multicast no priority
ip multicast max-ingress-bandwidth *megabits*
ip multicast no max-ingress bandwidth
ip multicast static-neighbor *vlan_id* {*slot*/*port* | linkagg *agg_num*} [v2 | v3]
ip multicast no static-neighbor *vlan_id* {*slot*/*port* | linkagg *agg_num*} [v2 | v3]
ip multicast static-querier *vlan_id* {*slot*/*port* | linkagg *agg_num*} [v2 | v3]
ip multicast no static-querier *vlan_id* {*slot*/*port* | linkagg *agg_num*} [v2 | v3]
ip multicast static-member *ip_address vlan_id* {*slot*/*port* | linkagg *agg_num*}
ip multicast no static-member *ip_address vlan_id* {*slot*/*port* | linkagg *agg_num*}
ip multicast hardware-routing
ip multicast no hardware-routing
show ip multicast switching
show ip multicast groups [*ip_address*]
show ip multicast neighbors
show ip multicast queriers
show ip multicast forwarding [*ip_address*]
show ip multicast policy-cache

Server Load Balancing Commands

ip slb admin {enable | disable}
ip slb cluster name vip ip_address
no ip slb cluster name
ip slb cluster cluster_name admin status {enable | disable}
ip slb cluster cluster_name ping period seconds
ip slb cluster *cluster_name* ping timeout *milliseconds*
ip slb cluster *cluster_name* ping retries *count*
ip slb cluster *cluster_name* distribution {round robin | server failover}
ip slb cluster *cluster_name* sticky time *seconds*
ip slb cluster cluster_name probe *probe_name*
ip slb server ip *ip_address* cluster *cluster_name* [admin status {enable | disable}]
[weight *admin_weight*]
no ip slb server ip *ip_address* cluster *cluster_name*
ip slb server ip *ip_address* cluster *cluster_name* probe *probe_name*
ip slb probe *probe_name* {ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp}
no ip slb probe *probe_name*
ip slb probe *probe_name* {ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp}
timeout *seconds*
ip slb probe *probe_name* {ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp}
period *seconds*
ip slb probe *probe_name* {ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp}
port *port_number*
ip slb probe *probe_name* {ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp}
retries *retries*
ip slb probe *probe_name* {http | https} username user_name
ip slb probe *probe_name* {http | https} password *password*
ip slb probe *probe_name* {http | https} url *url*
ip slb probe *probe_name* {http | https} status *status_value*
ip slb probe *probe_name* {http | https | tcp | udp} send *send_string*
ip slb probe *probe_name* {http | https | tcp | udp} expect *expect_string*
show ip slb
show ip slb clusters
show ip slb cluster *name*
show ip slb cluster *name* server *ip_address*
show ip slb servers
show ip slb probes *probe_name*

High Availability VLAN Commands

vlan *vid* port-mac ingress-port *slot1*/*port1*[-*port1a*] [*slot2*/*port2*[-*port2a*]...]

vlan *vid* port-mac no ingress-port *slot1*/*port1*[-*port1a*] [*slot2/port2*[-*port2a*]...]
vlan *vid* port-mac egress-port *slot1*/*port1*[-*port1a*] [*slot2/port2*[-*port2a*]...]
vlan *vid* port-mac no egress-port *slot1*/*port1*[-*port1a*] [*slot2/port2*[-*port2a*]...]
mac-address-table port-mac vlan *vid* **mac** *mac_address1* [*mac_address2*...]
mac-address-table port-mac vlan *vid* no mac *mac_address1* [*mac_address2*...]
vlan *vid* **port-mac bandwidth** *mbps*
show mac-address-table port-mac [vlan *vid*]

AAA Commands

aaa radius-server *server* [host {*hostname* | *ip_address*} [*hostname2* | *ip_address2*]] [key *secret*] [retransmit *retries*] [timeout *seconds*] [auth-port *auth_port*] [acct-port *acct_port*]
no aaa radius server *server*
aaa ldap-server *server_name* [host {*hostname* | *ip_address*} [{*hostname2* | *ip_address2*}]] [dn *dn_name*] [password *super_password*] [base *search_base*] [retransmit *retries*] [timeout *seconds*] [ssl | no ssl] [port *port*]
no aaa ldap-server *server-name*
aaa ace-server clear
aaa authentication vlan single-mode *server1* [*server2*] [*server3*] [*server4*]
no aaa authentication vlan
aaa authentication vlan multiple-mode *vlan_id server1* [*server2*] [*server3*] [*server4*]
no aaa authentication vlan *vlan_id*
aaa avlan no [mac-address] *mac_address*
aaa avlan dns [name] *dns_name*
no aaa avlan dns [name]
aaa avlan default dhcp [gateway] *ip_address*
no aaa avlan default dhcp [gateway]
aaa authentication {console | telnet | ftp | http | snmp | ssh | default} *server1* [*server2*...] [local]
no aaa authentication [console | telnet | ftp | http | snmp | ssh | default]
aaa authentication {console | telnet | ftp | http | snmp | ssh } default
aaa authentication 802.1x *server1* [*server2*] [*server3*] [*server4*]
no aaa authentication 802.1x
aaa authentication MAC *server1* [*server2*] [*server3*] [*server4*]
no aaa authentication MAC
aaa accounting 802.1x *server1* [*server2*...] [local]
no aaa accounting 802.1x
aaa accounting vlan [*vlan_id*] *server1* [*server2*...] [local]
no accounting vlan [*vlan_id*]
aaa accounting session *server1* [*server2*...] [local]
no accounting session
avlan default-traffic {enable | disable}
avlan port-bound {enable | disable}
avlan *vlan_id* auth-ip *ip_address*
aaa avlan http language
user *username* [password *password*] [expiration {*day* | *date*}] [read-only | read-write [*families...* | *domains...*| all | none]] [no snmp | no auth | sha | md5 | sha+des | md5+des] [end-user profile *name*]
no user *username*
password
user password-size min *size*
user password-expiration {*day* | disable}
end-user profile *name* [read-only [*area* | all]] [read-write [*area* | all]] [disable [*area* | all]]
no end-user profile *name*
end-user profile *name* vlan-range *vlan_range* [*vlan_range2*...]
end-user profile *name* no vlan-range *vlan1* [*vlan2*..]
show aaa server [*server_name*]
show aaa authentication vlan
show aaa authentication
show aaa authentication 802.1x
show aaa authentication mac
show aaa authentication 802.1x
show aaa accounting vlan
show aaa accounting
show user [*username*]
show user password-size
show user password-expiration
show avlan user [vlan *vlan_id* | slot *slot*]
show aaa avlan config
show aaa avlan auth-ip [vlan *vlan_id*]
debug command-info {enable | disable}
debug end-user profile *name*
show end-user profile *name*
show aaa priv hexa [*domain or family*]

802.1X Commands

802.1x *slot/port* [direction {both | in}] [port-control {force-authorized | force-unauthorized | auto}] [quiet-period *seconds*] [tx-period *seconds*] [supp-timeout *seconds*] [server-timeout *seconds*] [max-req *max_req*] [re-authperiod *seconds*] [reauthentication | no reauthentication]
802.1x initialize *slot/port*
802.1x reauthenticate *slot/port*
802.1x *slot/port* **supp-polling retry** *retries*
802.1x *slot/port* **supplicant policy authentication [[pass] {group-mobility | vlan** *vid* | default-vlan | block}...] [[fail] {vlan *vid* | block}...]
802.1x *slot/port* **non-supplicant policy authentication [[pass] {group-mobility | vlan** *vid* | default-vlan | block}] [[fail] {group-mobility | vlan *vid* | default-vlan | block}]
802.1x *slot/port* **non-supplicant policy {**group-mobility | vlan *vid* | default-vlan | block}

802.1x *slot/port* **{supplicant | non-supplicant} policy default**
show 802.1x [*slot/port*]
show 802.1x users [*slot/port*]
show 802.1x statistics [*slot/port*]
show 802.1x device classification policies [*slot/port*]
show 802.1x non-supp [*slot/port*]

Memory Monitoring Commands

debug ktrace {enable | disable}
debug ktrace appid {*app_id* | *integer*} level {*level* | *integer*}
debug ktrace no appid *app_id*
debug ktrace show
debug ktrace show log [*file*]
debug systrace {enable | disable}
debug systrace watch {enable | disable}
debug systrace appid {*app_id* | *integer*} level {*level* | *integer*}
debug systrace no appid *app_id*
debug systrace show
debug systrace show log [*file*]
show log pmd *file_name* [type *type_string* | id *registrationidentifier_int* | subid *subidentifier_int* | taskname *taskname_string* | taskid *tasknumber_int* | record *recordtype_string* | address *address_int*]
debug memory monitor {enable | disable}
debug memory monitor show log
debug memory monitor show log global
debug memory monitor show log task
debug memory monitor show log size

Switch Logging Commands

swlog
no swlog
swlog appid {*app_id* | *integer*} level {*level* | *integer*}
no swlog appid *app_id*
swlog output {console | flash | socket *[ip_address]*}
no swlog output {console | flash | socket *[ip_address]*}
swlog output flash file-size *bytes*
swlog clear
show log swlog
show log swlog [session *session_id*] [timestamp *start_time* [*end_time*]] [appid *appid*] [level *level*]
show swlog

Index

Numerics

802.1p
  default queues 38-165
  mapped to ToS or DSCP 38-146
  QoS port default 38-177
  trusted ports 38-167
802.1Q
  untrusted ports 38-7
802.1q
  debug 15-8
  vlan 15-2

A

accounting 19-49
actions
  address translation 38-148, 38-150, 38-152, 38-154
  Server Load Balancing groups 38-156
  supported by hardware 38-124
active login sessions 6-30
Alcatel Mapping Adjacency Protocol
  adjacent switches 14-2
  common transmission state 14-5
  discovery transmission state 14-3
alerts 46-4, 46-11
alias 6-14
assigning ports to VLANs 21-13
attributes 7-25
authenticated mobile ports 20-37, 20-39, 20-41, 20-42, 20-43
authenticated VLANs 21-8
  DHCP Relay 26-7

B

BGP 31-1
  aggregate 31-31
  dampening 31-24
  debug 31-28
  global 31-4
  neighbor 31-54
  network 31-45
  policy 31-95
  route import and export 31-143
binding VLAN rules 20-10, 20-12, 20-14, 20-16, 20-18, 20-20
boot.cfg file
  QoS log lines 38-12
BPDU
  see Bridge Protocol Data Units
Bridge Protocol Data Units 16-4, 16-87, 16-89, 16-91

C

chmod 7-24
CLI
  logging commands 6-24
CMM
  automatic reboot 1-16
  copying 1-6
  reload 1-2
  takeover 1-14
CMS
  mac-range 3-2
commands
  domains and families 43-38
conditions
  multiple conditions defined 38-67
copy 7-18
counters 19-52
current user session 6-27
custom (user) VLAN rule 20-32

D

Daylight Savings Time (DST)
  enabling or disabling 2-12
debug messages 46-4, 46-11
default route
  IP 23-9
DHCP Relay 26-1
  AVLAN only forwarding option 26-7
  DHCP server IP address 26-2
  elapsed boot time 26-11
  forward delay time 26-11
  Global DHCP 26-2
  maximum number of hops 26-13
  per-VLAN forwarding option 26-9
  standard forwarding option 26-6
  statistics 26-40, 26-42
DHCP VLAN rules 20-2, 20-4, 20-6, 20-8
DNS
  domain name 12-2
  enabling resolver 12-2
  name servers 12-3
  resolver 12-1
DSCP
  mapped to 802.1p or ToS 38-146
  QoS port default 38-178
duplex data transfer 19-18
dvmrp
  interface 33-7
  tunnel 33-18
dynamic link aggregation
  adding ports 13-22
  creating 13-9
  deleting 13-9
  deleting ports 13-22
  LACPDU frames 13-25, 13-31
  local group MAC address 13-17
  local port MAC address 13-27
  optimization 13-45

remote group MAC address 13-18
remote port MAC address 13-33
dynamic VLAN assignment
mobile ports 20-36
dynamic VLAN port assignment
secondary VLANs 20-40
VLAN rules 20-1

E

Eadvrout.img file 32-3, 33-2, 33-3
editor 7-28
vi 7-38
error file 9-4
error frame 19-54
errors 46-4, 46-11
Esecu.img 43-35
Ethernet 19-1
debug interfaces 19-70
flow 19-5
interfaces 19-9
trap port 19-3
exit 6-26

F

Fadvrout.img file 32-3, 32-4, 33-2, 33-3
file system 7-3
file system check 7-27
flood rate 19-35
fragments
classifying 38-17
frame size 19-30
Fsecu.img 43-35

H

Hadvrout.img file 33-2, 33-3
Hardware Routing Engine (HRE) 11-1
health 37-2
high availability VLANs 42-1
displaying 42-9
egress ports 42-4
ingress ports 42-2, 42-8
Hsecu.img 43-35

I

inter-frame gap 19-24, 19-61, 19-63
interior gateway protocol
OSPF 30-1
Internet Protocol
arp 23-21
Denial of Service 23-39
global 23-4
ICMP messages 23-27
IP Multicast Switching
see IPMS
IP network address VLAN rule 20-26
IP routing
default route 23-9
IPMS 40-1
disabling 40-2
enabling 40-2
ipv6
address 24-6
clear Neighbor Table 24-40
clear pmtu table 24-37
dad-check 24-9
debug 24-21
hop-limit 24-10
host 24-12
interface 24-3
interface tunnel source destination 24-8
neighbor 24-13
ping6 24-17
pmtu-lifetime 24-11
prefix 24-14
rip 24-55
route 24-16
traceroute 24-19
traffic counters 24-50
IPX
clear route 28-7
extended RIP packets 28-20
extended SAP packets 28-20
filter 28-11
ping 28-9
routing 28-2
timers 28-22
type-20-propagation 28-18
IPX network address VLAN rule 20-28
IPX router ports 21-9

L

LACP
see dynamic link aggregation
lanpower 4-3
layer 2 statistics 19-26
LDAP servers
port numbers 43-6
link-state protocol
OSPF 30-1

M

MAC address table
duplicate MAC addresses 17-3, 17-6
MAC address VLAN rule 20-22, 20-24
MAC addresses
aging time 16-41, 16-43, 16-45, 17-7
dynamic link aggregation 13-17, 13-18, 13-27, 13-33
learned 17-2
statically assigned 17-2, 17-3, 17-5
MAC router mode 21-11
memory monitoring 45-1
debug 45-23
disabling kTrace 45-2
disabling sysTrace 45-10

enabling kTrace 45-2
enabling sysTrace 45-10
high-level monitoring 45-10
low-level monitoring 45-2
postmortem dumps
see PMD 45-19
mobile port properties
authentication 20-37, 20-39, 20-41, 20-42, 20-43
BPDU ignore 20-36, 20-37
default VLAN membership 20-40
restore default VLAN 20-38
status 20-47
mobile ports 20-36
trusted ports 38-7
VLAN rules 20-1
modules
fabric
see SFM 2-21
power 2-18
reloading 2-16
temperature 2-20
multicast address boundaries 34-5
multicast routing
debug 34-13
interface 34-4, 34-5, 34-9

N

Network Interface (NI) modules
reloading 2-14
NTP 5-1
broadcast 5-5
key 5-7
operation 5-4
server 5-2

O

OSPF
area 30-28
global 30-3
interface 30-35
link-state protocol 30-1
restart 30-56

P

pending configuration
commands associated with 38-36
erasing policy configuration 38-36
PIM-SM
debug 32-48
global 32-3
interface 32-25
PIM-SM v2 32-22
policies
save option 38-41
policy network groups
destination rewrite 38-154
source rewrite 38-150
policy servers
displaying information about 39-6
SSL 39-4
port mapping 22-2
port mirroring 35-2
port mobility
see mobile ports
port monitoring 35-6
port status 19-61
port VLAN rule 20-34
Power over Ethernet
see PoE 4-1
privileges
see attributes
see chmod
prompt 6-11
protocol VLAN rules 20-30
pseudo-CAM
see Hardware Routing Engine (HRE)

R

RDP
advertisement packets 25-5
maximum time 25-7, 25-11
minimum time 25-9
preference level 25-13
Remote Network Monitoring 36-1
resolver
see DNS resolver
RIP
debug 27-35
force-holddowntimer 27-13
global 27-3
host-route 27-15
interface 27-5, 27-31
redistribution 27-17
route-tag 27-16
security 27-31
status 27-4
router discovery protocol
see RDP 25-1

S

secure shell session 6-39
secure socket layer
see SSL
Server Load Balancing 41-1
adding clusters 41-4
adding servers 41-17
deleting clusters 41-4, 41-17
disabling 41-3
enabling 41-3
policy actions 38-156
server administrative status 41-17
server administrative weights 41-17
session management
banner 6-5

history buffer 6-19
kills 6-25
login attempt 6-3
more 6-36
more size 6-35
prompt 6-9
timeout 6-7
user profile 6-17
xon-xoff 6-10
SLB
see Server Load Balancing
smurf attack 23-18
snapshot 9-11
SNMP
community map 10-7
community strings 10-7
security 10-11
station 10-3
statistics 10-15
trap 10-19
source learning 17-1
MAC address table 17-1, 17-2, 17-5
Spanning Tree Algorithm and Protocol 16-1
1x1 operating mode 16-4, 16-12, 16-14, 16-17, 16-19, 16-26, 16-28
bridge ID 16-21, 16-23, 16-25, 16-27
flat operating mode 16-4, 16-12, 16-14, 16-17, 16-19, 16-26, 16-28
path cost 16-66, 16-70, 16-74, 16-77
port ID 16-57, 16-59, 16-61, 16-63
port states 16-80, 16-82, 16-84
Spanning Tree bridge parameters
maximum aging time 16-35
Spanning Tree port parameters
connection type 16-86, 16-88, 16-90
link aggregate ports 16-51, 16-53, 16-55
mode 16-80, 16-82, 16-84
path cost 16-82, 16-84
priority 16-57
Spanning Tree status 16-51, 16-53, 16-55
SSL 8-3
policy servers 39-4
static link aggregation
creating 13-3
deleting 13-3
optimization 13-45
static MAC addresses 17-2, 17-3, 17-5
Switch Fabric Module
see SFM 2-21
switch logging
application level 46-3
clear 46-9
global 46-2
output 46-6
syntax check 9-9
system information
administrative contact 2-3
date 2-6
location 2-5
name 2-4
time 2-6, 2-7, 2-9

T

telnet 6-38
timer session 9-6
Time-To-Live
see TTL
ToS
default queues 38-165
mapped to 802.1p or DSCP 38-146
QoS port default 38-178
trusted ports 38-167
TTL 34-4

U

user accounts
SNMP access 43-38
UTC 5-1

V

VLAN rules 20-1, 20-18
binding 20-10, 20-12, 20-14, 20-16, 20-20
custom (user) 20-32
DHCP 20-2, 20-4, 20-6, 20-8
IP network address 20-26
IPX network address 20-28
MAC address 20-22, 20-24
port 20-34
protocol 20-30
VLANs 21-1, 21-2
administrative status 21-2
authentication 21-8
default VLAN 21-13
description 21-2
high availability VLANs 42-1
IPMS 40-13, 40-15, 40-17
IPX router port 21-9
MAC router mode 21-11
operational status 21-2
port assignments 21-13
rules 20-1
secondary VLAN 21-13
Spanning Tree status 21-4
VRRP
configuring priority 29-3

W

wait time 19-7, 19-41
warnings 46-4, 46-11
WebView
enabling/disabling 8-2

Z

Zmodem 7-49