Part No. 060329-10, Rev E
January 2013

OmniSwitch AOS Release 6 CLI Reference Guide

www.alcatel-lucent.com

This user guide documents release 6.4.5 of the OmniSwitch 6400 Series, OmniSwitch 6850E Series, OmniSwitch 6855 Series, and OmniSwitch 9000E Series
The functionality described in this guide is subject to change without notice.

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
support@ind.alcatel.com

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

Contents

About This Guide xlvii

Supported Platforms xlvii

Who Should Read this Manual? xlviii

When Should I Read this Manual? xlviii

What is in this Manual? xlviii

What is Not in this Manual? xlix

How is the Information Organized? xlix

Text Conventions xlix

Documentation Roadmap li

Related Documentation liii

User Manual CD lv

Technical Support lv

Chapter 1 **Ethernet Port Commands** 1-1

trap port link 1-4
interfaces speed 1-6
interfaces mode 1-8
interfaces autoneg 1-10
interfaces pause 1-14
interfaces e2e-flow-vlan 1-17
interfaces duplex 1-19
interfaces admin 1-21
interfaces cli-prompt 1-23
interfaces alias 1-25
interfaces ifg 1-26
interfaces no l2 statistics 1-27
interfaces max frame 1-29
interfaces flood 1-31
interfaces flood rate 1-33
interfaces flood action 1-35
interfaces violation-recovery-time 1-37
interfaces violation-recovery-maximum 1-39
interfaces violation-recovery-trap 1-41
interfaces clear-violation-all 1-42
interfaces wait-to-restore 1-43
interfaces transceiver ddm 1-45
interfaces link-monitoring admin-status 1-47
interfaces link-monitoring time-window 1-49
interfaces link-monitoring link-flap-threshold 1-51

interfaces link-monitoring link-error-threshold 1-53
interfaces clear-link-monitoring-stats 1-55
interfaces hybrid preferred-fiber 1-56
interfaces hybrid autoneg 1-57
interfaces hybrid crossover 1-59
interfaces hybrid duplex 1-61
interfaces hybrid speed 1-63
interfaces hybrid pause 1-65
show interfaces 1-68
show interfaces capability 1-72
show interfaces flow control 1-74
show interfaces pause 1-76
show interfaces e2e-flow-vlan 1-78
show interfaces accounting 1-79
show interfaces counters 1-81
show interfaces counters errors 1-83
show interfaces collisions 1-85
show interfaces status 1-87
show interfaces port 1-89
show interfaces violation-recovery 1-92
show interfaces ifg 1-94
show interfaces flood rate 1-96
show interfaces traffic 1-98
show interfaces transceiver 1-100
show interfaces hybrid 1-103
show interfaces hybrid status 1-107
show interfaces hybrid pause 1-109
show interfaces hybrid capability 1-111
show interfaces hybrid accounting 1-114
show interfaces hybrid counters 1-116
show interfaces hybrid counters errors 1-118
show interfaces hybrid collisions 1-120
show interfaces hybrid traffic 1-122
show interfaces hybrid port 1-124
show interfaces hybrid flood rate 1-126
show interfaces hybrid ifg 1-128
show interfaces link-monitoring config 1-130
show interfaces link-monitoring statistics 1-132
debug interfaces set backpressure 1-134
debug interfaces backpressure 1-135
link-fault-propagation group 1-137
link-fault-propagation group source 1-139
link-fault-propagation group destination 1-141
link-fault-propagation group wait-to-shutdown 1-143
show link-fault-propagation group 1-144
interfaces tdr-test-start 1-146
interfaces no tdr-statistics 1-147
show interfaces tdr-statistics 1-148

Chapter 2 UDLD Commands 2-1
udld 2-2

udld port 2-3
udld mode 2-5
udld probe-timer 2-7
udld echo-wait-timer 2-9
clear udld statistics port 2-11
interfaces clear-violation-all 2-12
show udld configuration 2-13
show udld configuration port 2-14
show udld statistics port 2-16
show udld neighbor port 2-18
show udld status port 2-20

Chapter 3 Power over Ethernet (PoE) Commands 3-1
lanpower start 3-3
lanpower stop 3-5
lanpower power 3-6
lanpower maxpower 3-8
lanpower priority 3-10
lanpower priority-disconnect 3-12
lanpower slot-priority 3-14
lanpower redundant-power 3-16
lanpower capacitor-detection 3-17
show lanpower 3-18
show lanpower capacitor-detection 3-21
show lanpower priority-disconnect 3-22
show lanpower slot-priority 3-23

Chapter 4 VLAN Management Commands 4-1
vlan 4-2
vlan stp 4-4
vlan mobile-tag 4-6
vlan authentication 4-8
vlan mtu-ip 4-10
vlan port default 4-11
vlan source-learning 4-13
show vlan 4-15
show vlan port 4-18
show vlan router mac status 4-21
show vlan gvrp 4-23
show vlan ipmvlan 4-26

Chapter 5 802.1Q Commands 5-1
vlan 802.1q 5-2
vlan 802.1q frame type 5-4
show 802.1q 5-6

Chapter 6 Distributed Spanning Tree Commands 6-1
bridge mode 6-4
spantree mode 6-6
bridge protocol 6-8
bridge cist protocol 6-10
bridge port loop-guard 6-12

bridge 1x1 protocol 6-14
bridge mst region name 6-16
bridge mst region revision level 6-18
bridge mst region max hops 6-19
bridge msti 6-21
bridge msti vlan 6-23
bridge priority 6-25
bridge cist priority 6-27
bridge msti priority 6-29
bridge 1x1 priority 6-31
bridge hello time 6-33
bridge cist hello time 6-35
bridge 1x1 hello time 6-37
bridge max age 6-39
bridge cist max age 6-41
bridge 1x1 max age 6-43
bridge forward delay 6-45
bridge cist forward delay 6-47
bridge 1x1 forward delay 6-49
bridge mode 1x1 pvst+ 6-51
bridge bpdu-switching 6-52
bridge path cost mode 6-54
bridge auto-vlan-containment 6-56
bridge port pvst+ 6-58
bridge 6-60
bridge cist 6-62
bridge 1x1 6-64
bridge priority 6-66
bridge cist priority 6-68
bridge msti priority 6-70
bridge 1x1 priority 6-72
bridge path cost 6-74
bridge cist path cost 6-78
bridge msti path cost 6-82
bridge 1x1 path cost 6-85
bridge mode 6-89
bridge cist mode 6-91
bridge 1x1 mode 6-93
bridge connection 6-95
bridge cist connection 6-97
bridge 1x1 connection 6-99
bridge cist admin-edge 6-101
bridge 1x1 admin-edge 6-103
bridge cist auto-edge 6-105
bridge 1x1 auto-edge 6-107
bridge cist restricted-role 6-109
bridge 1x1 restricted-role 6-111
bridge cist restricted-tcn 6-113
bridge 1x1 restricted-tcn 6-115
bridge cist txholdcount 6-117
bridge 1x1 txholdcount 6-118
bridge rrstp 6-119

bridge rrstp ring 6-120
bridge rrstp ring vlan-tag 6-122
bridge rrstp ring status 6-124
show spantree 6-125
show spantree cist 6-131
show spantree msti 6-135
show spantree 1x1 6-140
show spantree ports 6-144
show spantree cist ports 6-153
show spantree msti ports 6-157
show spantree 1x1 ports 6-162
show spantree mst region 6-168
show spantree msti vlan-map 6-170
show spantree cist vlan-map 6-172
show spantree map-msti 6-174
show spantree mst port 6-175
show bridge rrstp configuration 6-178
show bridge rrstp ring 6-179

Chapter 7 Link Aggregation Commands 7-1
static linkagg size 7-3
static linkagg name 7-5
static linkagg admin state 7-6
static agg agg num 7-7
lacp linkagg size 7-9
lacp linkagg name 7-12
lacp linkagg admin state 7-13
lacp linkagg actor admin key 7-15
lacp linkagg actor system priority 7-16
lacp linkagg actor system id 7-17
lacp linkagg partner system id 7-18
lacp linkagg partner system priority 7-20
lacp linkagg partner admin key 7-21
lacp agg actor admin key 7-22
lacp agg actor admin state 7-25
lacp agg actor system id 7-27
lacp agg actor system priority 7-29
lacp agg partner admin state 7-31
lacp agg partner admin system id 7-33
lacp agg partner admin key 7-35
lacp agg partner admin system priority 7-37
lacp agg actor port priority 7-39
lacp agg partner admin port 7-41
lacp agg partner admin port priority 7-43
lacp linkagg wait-to-restore-timer 7-45
lacp agg standby 7-47
lacp linkagg pre-empt 7-49
lacp linkagg pre-empt timer 7-51
dhl num 7-53
dhl num linka linkb 7-55
dhl num admin-state 7-57
dhl num vlan-map linkb 7-58

dhl num pre-emption-time 7-60
dhl num mac-flushing 7-62
show dhl 7-64
show dhl num 7-66
show dhl num link 7-69
show linkagg 7-71
show linkagg port 7-76
linkagg range 7-81
show linkagg range 7-83

Chapter 8 Multi-Chassis Commands 8-1
multi-chassis chassis-id hello-interval 8-2
multi-chassis hello-interval 8-4
multi-chassis chassis-group 8-6
multi-chassis ipc-vlan 8-8
multi-chassis loop-detection 8-10
multi-chassis loop-detection transmit-interval 8-12
multi-chassis vf-link create 8-14
multi-chassis vf-link member-ports 8-16
multi-chassis vf-link default-vlan 8-18
multi-chassis vip-vlan 8-20
show multi-chassis status 8-22
show multi-chassis loop-detection 8-24
show multi-chassis vf-link 8-26
show multi-chassis vf-link member-port 8-28
show multi-chassis consistency 8-30
show multi-chassis consistency linkagg 8-32
clear multi-chassis loop-detection 8-35

Chapter 9 Ethernet Ring Protection Commands 9-1
erp-ring 9-2
erp-ring reset-version-fallback 9-5
erp-ring rpl-node 9-6
erp-ring wait-to-restore 9-8
erp-ring enable 9-9
erp-ring guard-timer 9-10
erp-ring sub-ring 9-11
erp-ring virtual-channel 9-13
erp-ring revertive 9-15
erp-ring clear 9-17
erp-ring ethoam-event 9-18
clear erp statistics 9-20
show erp 9-22
show erp statistics 9-26

Chapter 10 Loopback Detection Commands 10-1
loopback-detection 10-2
loopback-detection port 10-3
loopback-detection transmission-timer 10-5
show loopback-detection 10-6
show loopback-detection port 10-8
show loopback-detection statistics port 10-10

Chapter 11 CPE Test Head Commands 11-1
test-oam 11-3
test-oam direction 11-5
test-oam src-endpoint dst-endpoint 11-6
test-oam port 11-8
test-oam vlan test-frame 11-10
test-oam role 11-12
test-oam duration rate packet-size 11-14
test-oam frame 11-16
test-oam start stop 11-19
show test-oam 11-21
show test-oam statistics 11-25
clear test-oam statistics 11-27
test-oam group 11-28
test-oam group tests 11-30
test-oam feeder-port 11-32
test-oam group src-endpoint dst-endpoint 11-33
test-oam group role 11-35
test-oam group port 11-36
test-oam group direction 11-38
test-oam group duration rate 11-40
test-oam group start 11-42
test-oam group stop 11-43
clear test-oam group statistics 11-44
show test-oam group 11-46
show test-oam group statistics 11-50

Chapter 12 Source Learning Commands 12-1
mac-address-table 12-2
mac-address-table vpls permanent sap 12-4
mac-address-table vpls permanent mesh-sdp 12-6
mac-address-table static-multicast 12-8
mac-address-table aging-time 12-10
source-learning 12-12
source-learning chassis-distributed 12-14
show mac-address-table 12-15
show mac-address-table all 12-18
show mac-address-table vpls 12-20
show mac-address-table vpls sap 12-22
show mac-address-table vpls mesh-sdp 12-24
show mac-address-table static-multicast 12-26
show mac-address-table count 12-29
show mac-address-table vpls count 12-31
show mac-address-table all count 12-33
show mac-address-table aging-time 12-35
show source-learning 12-36
show source-learning chassis-distributed 12-38

Chapter 13 PPPoE Intermediate Agent Commands 13-1
pppoe-ia 13-2
pppoe-ia trust 13-4

pppoe-ia client 13-6
pppoe-ia access-node-id 13-8
pppoe-ia circuit-id 13-10
pppoe-ia remote-id 13-13
clear pppoe-ia statistics 13-15
show pppoe-ia configuration 13-16
show pppoe-ia 13-19
show pppoe-ia statistics 13-21

Chapter 14 GVRP Commands 14-1
gvrp 14-2
gvrp port 14-3
gvrp transparent switching 14-5
gvrp maximum vlan 14-6
gvrp registration 14-7
gvrp applicant 14-9
gvrp timer 14-11
gvrp restrict-vlan-registration 14-13
gvrp restrict-vlan-advertisement 14-15
gvrp static-vlan restrict 14-17
clear gvrp statistics 14-19
show gvrp statistics 14-20
show gvrp last-pdu-origin 14-23
show gvrp configuration 14-24
show gvrp configuration port 14-26
show gvrp configuration linkagg/port 14-28
show gvrp timer 14-31

Chapter 15 MVRP Commands 15-1
vlan registration-mode 15-2
mvrp 15-4
mvrp port 15-5
mvrp linkagg 15-7
mvrp transparent-switching 15-9
mvrp maximum vlan 15-10
mvrp registration 15-11
mvrp applicant 15-13
mvrp timer join 15-15
mvrp timer leave 15-17
mvrp timer leaveall 15-19
mvrp timer periodic-timer 15-21
mvrp periodic-transmission 15-23
mvrp restrict-vlan-registration 15-24
mvrp restrict-vlan-advertisement 15-26
mvrp static-vlan-restrict 15-28
show mvrp configuration 15-30
show mvrp port 15-32
show mvrp linkagg 15-35
show mvrp timer 15-38
show mvrp statistics 15-41
show mvrp last-pdu-origin 15-44
show vlan registration-mode 15-46

show mvrp vlan-restrictions 15-47
show vlan mvrp 15-49
mvrp clear-statistics 15-51

Chapter 16 802.1AB Commands 16-1
lldp destination mac-address 16-3
lldp transmit fast-start-count 16-4
lldp transmit interval 16-5
lldp transmit hold-multiplier 16-6
lldp transmit delay 16-7
lldp reinit delay 16-8
lldp notification interval 16-9
lldp lldpdu 16-10
lldp notification 16-12
lldp network-policy 16-14
lldp med network-policy 16-16
lldp tlv management 16-18
lldp tlv dot1 16-20
lldp tlv dot3 mac-phy 16-22
lldp tlv med 16-24
show lldp config 16-26
show lldp network-policy 16-28
show lldp med network-policy 16-30
show lldp system-statistics 16-32
show lldp statistics 16-34
show lldp local-system 16-36
show lldp local-port 16-39
show lldp local-management-address 16-41
show lldp remote-system 16-42
show lldp remote-system med 16-44
lldp trust-agent 16-47
lldp trust-agent violation-action 16-49
show lldp trusted remote-agent 16-51
show lldp trust-agent 16-53

Chapter 17 Interswitch Protocol Commands 17-1
amap 17-2
amap discovery time 17-3
amap common time 17-5
show amap 17-7

Chapter 18 SIP Commands 18-1
sip-snooping enable 18-2
sip-snooping port enable 18-3
sip-snooping mode 18-5
sip-snooping trusted server 18-7
sip-snooping sip-control 18-9
sip-snooping sos-call number 18-10
sip-snooping sos-call dscp 18-11
sip-snooping udp port 18-12
sip-snooping tcp port 18-13
sip-snooping threshold 18-14

sip-snooping logging-threshold num-of-calls 18-16
show sip-snooping call-records 18-17
clear sip-snooping statistics 18-20
show sip-snooping config 18-21
show sip-snooping ports 18-23
show sip-snooping statistics 18-25
show qos dscp-table 18-28

Chapter 19 IP Commands 19-1
ip interface 19-5
ip managed-interface 19-8
ip interface dhcp-client 19-11
ip interface tunnel 19-13
ip router primary-address 19-15
ip router router-id 19-16
ip static-route 19-17
ip route-pref 19-19
ip default-ttl 19-21
ping 19-22
traceroute 19-25
ip dual-hash mode 19-27
ip directed-broadcast 19-28
ip service 19-29
ip redist 19-31
ip access-list 19-33
ip access-list address 19-34
ip route-map action 19-36
ip route-map match ip address 19-38
ip route-map match ipv6 address 19-40
ip route-map match ip-nexthop 19-42
ip route-map match ipv6-nexthop 19-44
ip route-map match tag 19-46
ip route-map match ipv4-interface 19-48
ip route-map match ipv6-interface 19-50
ip route-map match metric 19-52
ip route-map match route-type 19-54
ip route-map match protocol 19-56
ip route-map set metric 19-58
ip route-map set metric-type 19-60
ip route-map set tag 19-62
ip route-map set community 19-64
ip route-map set local-preference 19-66
ip route-map set level 19-68
ip route-map set ip-nexthop 19-70
ip route-map set ipv6-nexthop 19-72
vrf 19-74
ip export route-map 19-76
ip import vrf 19-78
show ip export 19-80
show ip import 19-81
show ip global-route-table 19-83
arp 19-85

clear arp-cache 19-87
ip dos arp-poison restricted-address 19-88
arp filter 19-89
clear arp filter 19-91
icmp type 19-92
icmp unreachable 19-95
icmp echo 19-97
icmp timestamp 19-99
icmp addr-mask 19-101
icmp messages 19-103
ip dos scan close-port-penalty 19-104
ip dos scan tcp open-port-penalty 19-105
ip dos scan udp open-port-penalty 19-106
ip dos scan threshold 19-107
ip dos trap 19-109
ip dos scan decay 19-110
show ip traffic 19-111
show ip interface 19-114
show ip managed-interface 19-120
show ip route 19-122
show ip route-pref 19-125
show ip redist 19-127
show ip access-list 19-129
show ip route-map 19-131
show ip router database 19-133
show ip emp-route 19-136
show ip config 19-138
show ip protocols 19-139
show ip service 19-141
show ip dynamic-proxy-arp 19-143
show vrf 19-145
show arp 19-146
show arp summary 19-148
show arp filter 19-149
show icmp control 19-151
show icmp statistics 19-153
show tcp statistics 19-155
show tcp ports 19-157
show udp statistics 19-159
show udp ports 19-160
show ip dos config 19-161
show ip dos statistics 19-163
show ip dos arp-poison 19-165
ip wccp admin-state 19-166
ip wccp service-group web-cache md5 19-167
ip wccp service-group web-cache restrict 19-169
clear ip wccp 19-171
show ip wccp status 19-172
show ip wccp services 19-173
show ip wccp cache-engines 19-175
show ip wccp restricts 19-177
show ip wccp service-group 19-179

show ip wccp service-group detail 19-181
show ip wccp service-group view 19-183
show ip wccp service-group statistics 19-185
ip dos anti-spoofing 19-187
ip dos anti-spoofing arp-only 19-188
ip dos anti-spoofing address 19-189
ip dos anti-spoofing address arp-only 19-190
ip dos anti-spoofing clear stats 19-191
ip dos anti-spoofing address clear stats 19-192
show ip dos anti-spoofing 19-193

Chapter 20 IPv6 Commands 20-1
ipv6 interface 20-3
ipv6 address 20-6
ipv6 address global-id 20-8
ipv6 address local-unicast 20-9
ipv6 interface tunnel source destination 20-11
ipv6 dad-check 20-12
ipv6 hop-limit 20-13
ipv6 pmtu-lifetime 20-14
ipv6 host 20-15
ipv6 neighbor stale-lifetime 20-16
ipv6 neighbor 20-17
ipv6 prefix 20-19
ipv6 static-route 20-21
ipv6 route-pref 20-23
ping6 20-25
traceroute6 20-27
show ipv6 hosts 20-29
show ipv6 icmp statistics 20-30
show ipv6 interface 20-33
show ipv6 pmtu table 20-38
clear ipv6 pmtu table 20-40
show ipv6 neighbors 20-41
clear ipv6 neighbors 20-43
show ipv6 prefixes 20-44
show ipv6 routes 20-46
show ipv6 route-pref 20-48
show ipv6 router database 20-49
show ipv6 tcp ports 20-51
show ipv6 traffic 20-53
clear ipv6 traffic 20-56
show ipv6 tunnel 20-57
show ipv6 udp ports 20-59
show ipv6 information 20-61
ipv6 redist 20-63
ipv6 access-list 20-65
ipv6 access-list address 20-66
show ipv6 redist 20-68
show ipv6 access-list 20-70
ipv6 load rip 20-72
ipv6 rip status 20-73

ipv6 rip invalid-timer 20-74
ipv6 rip garbage-timer 20-75
ipv6 rip holddown-timer 20-76
ipv6 rip jitter 20-77
ipv6 rip route-tag 20-78
ipv6 rip update-interval 20-79
ipv6 rip triggered-sends 20-80
ipv6 rip interface 20-81
ipv6 rip interface metric 20-83
ipv6 rip interface recv-status 20-84
ipv6 rip interface send-status 20-85
ipv6 rip interface horizon 20-86
show ipv6 rip 20-87
show ipv6 rip interface 20-89
show ipv6 rip peer 20-92
show ipv6 rip routes 20-94

Chapter 21 IPsec Commands 21-1
ipsec key 21-2
ipsec security-key 21-4
ipsec policy 21-6
ipsec policy rule 21-9
ipsec sa 21-11
show ipsec policy 21-14
show ipsec sa 21-17
show ipsec key 21-19
show ipsec ipv6 statistics 21-21

Chapter 22 RIP Commands 22-1
ip load rip 22-2
ip rip status 22-3
ip rip interface 22-4
ip rip interface status 22-6
ip rip interface metric 22-8
ip rip interface send-version 22-9
ip rip interface recv-version 22-11
ip rip force-holddowntimer 22-13
ip rip host-route 22-15
ip rip route-tag 22-16
ip rip interface auth-type 22-17
ip rip interface auth-key 22-18
ip rip update-interval 22-19
ip rip invalid-timer 22-20
ip rip garbage-timer 22-21
ip rip holddown-timer 22-22
show ip rip 22-23
show ip rip routes 22-25
show ip rip interface 22-28
show ip rip peer 22-30

Chapter 23 RDP Commands 23-1
ip router-discovery 23-2

ip router-discovery interface 23-3
ip router-discovery interface advertisement-address 23-5
ip router-discovery interface max-advertisement-interval 23-7
ip router-discovery interface min-advertisement-interval 23-9
ip router-discovery interface advertisement-lifetime 23-11
ip router-discovery interface preference-level 23-13
show ip router-discovery 23-15
show ip router-discovery interface 23-17

Chapter 24 BFD Commands 24-1
ip bfd-std status 24-3
ip bfd-std transmit 24-4
ip bfd-std receive 24-5
ip bfd-std mode 24-6
ip bfd-std echo interval 24-8
ip bfd-std l2-hold-timer 24-9
ip bfd-std interface 24-10
ip bfd-std interface status 24-11
ip bfd-std interface transmit 24-12
ip bfd-std interface receive 24-13
ip bfd-std interface multiplier 24-14
ip bfd-std interface echo-interval 24-15
ip bfd-std interface mode 24-16
ip bfd-std interface l2-hold-timer 24-18
ip ospf bfd-std status 24-19
ip ospf bfd-std all-interfaces 24-21
ip ospf interface bfd-std 24-22
ip ospf interface bfd-std drs-only 24-23
ip ospf interface bfd-std all-nbrs 24-24
ip bgp bfd-std status 24-25
ip bgp bfd-std all-neighbors 24-26
ip bgp neighbors bfd-std 24-27
vrrp bfd-std 24-28
vrrp track address bfd-std 24-29
ip static-route all bfd-std 24-30
ip static-routes bfd-std status 24-31
show ip bfd-std 24-32
show ip bfd-std interfaces 24-34
show ip bfd-std sessions 24-36
show ip bfd-std session 24-38

Chapter 25 DHCP and DHCPv6 Relay Commands 25-1
ip helper address 25-4
ip helper address vlan 25-6
ip helper standard 25-8
ip helper avlan only 25-9
ip helper per-vlan only 25-11
ip helper forward delay 25-13
ip helper maximum hops 25-15
ip helper agent-information 25-17
ip helper agent-information policy 25-19
ip helper pxe-support 25-21

ip helper traffic-suppression 25-22
ip helper dhcp-snooping 25-24
ip helper dhcp-snooping mac-address verification 25-25
ip helper dhcp-snooping option-82 data-insertion 25-26
ip helper dhcp-snooping option-82 format 25-28
ip helper dhcp-snooping option-82 format ascii circuit-id 25-30
ip helper dhcp-snooping option-82 format ascii remote-id 25-32
ip helper dhcp-snooping bypass option-82-check 25-34
ip helper dhcp-snooping vlan 25-35
ip helper dhcp-snooping port 25-37
ip helper dhcp-snooping linkagg 25-39
ip helper dhcp-snooping port traffic-suppression 25-41
ip helper dhcp-snooping port ip-source-filtering 25-43
ip helper dhcp-snooping binding 25-45
ip helper dhcp-snooping ip-source-filter 25-47
ip helper dhcp-snooping binding timeout 25-49
ip helper dhcp-snooping binding action 25-50
ip helper dhcp-snooping binding persistency 25-51
ip helper boot-up 25-52
ip helper boot-up enable 25-54
ip udp relay 25-55
ip udp relay vlan 25-58
ipv6 helper address 25-60
ipv6 helper standard 25-62
ipv6 helper per-vlan only 25-63
ipv6 helper address vlan 25-64
ipv6 helper maximum hops 25-66
ipv6 helper dhcp-snooping 25-67
ipv6 helper dhcp-snooping vlan 25-68
ipv6 helper dhcp-snooping port 25-69
ipv6 helper dhcp-snooping linkagg 25-71
ipv6 helper dhcp-snooping binding 25-73
ipv6 helper dhcp-snooping binding timeout 25-74
ipv6 helper dhcp-snooping binding action 25-75
ipv6 helper dhcp-snooping binding persistency 25-76
ipv6 helper interface-id prefix 25-77
ipv6 helper remote-id format 25-78
show ip helper 25-80
show ip helper stats 25-85
show ip helper dhcp-snooping vlan 25-87
show ip helper dhcp-snooping port 25-89
show ip helper dhcp-snooping binding 25-91
show ip udp relay service 25-93
show ip udp relay statistics 25-95
show ip udp relay destination 25-97
dhcp-server 25-99
clear dhcp-server statistics 25-100
show dhcp-server leases 25-101
show dhcp-server statistics 25-103
show ip helper dhcp-snooping ip-source-filter 25-108
show ipv6 helper 25-110
show ipv6 helper stats 25-113

show ipv6 helper dhcp-snooping vlan 25-115
show ipv6 helper dhcp-snooping port 25-116
show ipv6 helper dhcp-snooping binding 25-118

Chapter 26 VRRP Commands 26-1
vrrp 26-3
vrrp address 26-6
vrrp track 26-7
vrrp track-association 26-9
vrrp trap 26-10
vrrp delay 26-11
vrrp interval 26-12
vrrp priority 26-14
vrrp preempt 26-16
vrrp all 26-18
vrrp set 26-20
vrrp group 26-22
vrrp group all 26-24
vrrp group set 26-26
vrrp group-association 26-28
vrrp3 26-30
vrrp3 address 26-33
vrrp3 trap 26-34
vrrp3 track-association 26-35
show vrrp 26-36
show vrrp statistics 26-39
show vrrp track 26-42
show vrrp track-association 26-44
show vrrp group 26-46
show vrrp group-association 26-48
show vrrp3 26-50
show vrrp3 statistics 26-53
show vrrp3 track-association 26-55

Chapter 27 OSPF Commands 27-1
ip ospf status 27-3
ip load ospf 27-4
ip ospf exit-overflow-interval 27-5
ip ospf extlsdb-limit 27-6
ip ospf host 27-7
ip ospf mtu-checking 27-9
ip ospf default-originate 27-10
ip ospf route-tag 27-12
ip ospf spf-timer 27-13
ip ospf virtual-link 27-15
ip ospf neighbor 27-18
ip ospf area 27-20
ip ospf area default-metric 27-22
ip ospf area range 27-24
ip ospf interface 27-26
ip ospf interface status 27-27
ip ospf interface area 27-28

ip ospf interface auth-key 27-29
ip ospf interface auth-type 27-30
ip ospf interface dead-interval 27-32
ip ospf interface hello-interval 27-33
ip ospf interface md5 27-34
ip ospf interface md5 key 27-36
ip ospf interface type 27-38
ip ospf interface cost 27-40
ip ospf interface poll-interval 27-41
ip ospf interface priority 27-42
ip ospf interface retrans-interval 27-43
ip ospf interface transit-delay 27-44
ip ospf restart-support 27-45
ip ospf restart-interval 27-46
ip ospf restart-helper status 27-47
ip ospf restart-helper strict-lsa-checking status 27-49
ip ospf restart initiate 27-51
show ip ospf 27-52
show ip ospf border-routers 27-55
show ip ospf ext-lsdb 27-57
show ip ospf host 27-59
show ip ospf lsdb 27-61
show ip ospf neighbor 27-63
show ip ospf routes 27-66
show ip ospf virtual-link 27-68
show ip ospf virtual-neighbor 27-70
show ip ospf area 27-73
show ip ospf area range 27-76
show ip ospf area stub 27-78
show ip ospf interface 27-80
show ip ospf restart 27-86

Chapter 28 OSPFv3 Commands 28-1
ipv6 ospf status 28-3
ipv6 load ospf 28-4
ipv6 ospf host 28-5
ipv6 ospf mtu-checking 28-7
ipv6 ospf route-tag 28-8
ipv6 ospf spf-timer 28-9
ipv6 ospf virtual-link 28-11
ipv6 ospf area 28-13
ipv6 ospf interface 28-15
ipv6 ospf interface status 28-16
ipv6 ospf interface area 28-17
ipv6 ospf interface dead-interval 28-18
ipv6 ospf interface hello-interval 28-20
ipv6 ospf interface cost 28-21
ipv6 ospf interface priority 28-22
ipv6 ospf interface retrans-interval 28-23
ipv6 ospf interface transit-delay 28-24
show ipv6 ospf 28-25
show ipv6 ospf border-routers 28-28

show ipv6 ospf host 28-30
show ipv6 ospf lsdb 28-32
show ipv6 ospf neighbor 28-34
show ipv6 ospf routes 28-36
show ipv6 ospf virtual-link 28-38
show ipv6 ospf area 28-40
show ipv6 ospf interface 28-42

Chapter 29 IS-IS Commands 29-1
ip load isis 29-4
ip isis status 29-5
ip isis area-id 29-6
ip isis level-capability 29-7
ip isis auth-check 29-8
ip isis auth-type 29-9
ip isis csnp-auth 29-11
ip isis hello-auth 29-12
ip isis psnp-auth 29-13
ip isis lsp-lifetime 29-14
ip isis lsp-wait 29-15
ip isis spf-wait 29-17
ip isis summary-address 29-19
ip isis overload 29-21
ip isis overload-on-boot 29-23
ip isis graceful-restart 29-25
ip isis graceful-restart helper 29-26
ip isis strict-adjacency-check 29-27
ip isis level auth-type 29-28
ip isis level hello-auth 29-30
ip isis level csnp-auth 29-31
ip isis level psnp-auth 29-32
ip isis level wide-metrics-only 29-33
show ip isis adjacency 29-34
show ip isis database 29-37
show ip isis hostname 29-42
show ip isis routes 29-44
show ip isis spf 29-46
show ip isis spf-log 29-48
show ip isis statistics 29-50
show ip isis status 29-53
show ip isis summary-address 29-58
ip isis interface 29-60
ip isis interface status 29-61
ip isis interface interface-type 29-62
ip isis interface csnp-interval 29-63
ip isis interface hello-auth-type 29-64
ip isis interface level-capability 29-66
ip isis interface lsp-pacing-interval 29-67
ip isis interface passive 29-68
ip isis interface retransmit-interval 29-69
ip isis interface default-type 29-70
ip isis interface level hello-auth-type 29-71

ip isis interface level hello-interval 29-73
ip isis interface level hello-multiplier 29-74
ip isis interface level metric 29-75
ip isis interface level passive 29-77
ip isis interface level priority 29-78
show ip isis interface 29-80
clear ip isis adjacency 29-84
clear ip isis lsp-database 29-86
clear ip isis spf-log 29-87
clear ip isis statistics 29-88

Chapter 30 BGP Commands 30-1
ip load bgp 30-6
ip bgp status 30-7
ip bgp unicast 30-8
ip bgp autonomous-system 30-9
ip bgp bestpath as-path ignore 30-10
ip bgp cluster-id 30-12
ip bgp default local-preference 30-13
ip bgp fast-external-failover 30-15
ip bgp always-compare-med 30-17
ip bgp bestpath med missing-as-worst 30-18
ip bgp client-to-client reflection 30-19
ip bgp as-origin-interval 30-21
ip bgp synchronization 30-22
ip bgp confederation identifier 30-24
ip bgp maximum-paths 30-25
ip bgp log-neighbor-changes 30-26
ip bgp dampening 30-27
ip bgp dampening clear 30-30
ip bgp aggregate-address 30-31
ip bgp aggregate-address status 30-33
ip bgp aggregate-address as-set 30-35
ip bgp aggregate-address community 30-37
ip bgp aggregate-address local-preference 30-39
ip bgp aggregate-address metric 30-41
ip bgp aggregate-address summary-only 30-43
ip bgp network 30-45
ip bgp network status 30-47
ip bgp network community 30-49
ip bgp network local-preference 30-50
ip bgp network metric 30-52
ip bgp neighbor 30-54
ip bgp neighbor status 30-55
ip bgp neighbor advertisement-interval 30-56
ip bgp neighbor clear 30-57
ip bgp neighbor route-reflector-client 30-59
ip bgp neighbor default-originate 30-60
ip bgp neighbor timers 30-61
ip bgp neighbor conn-retry-interval 30-63
ip bgp neighbor auto-restart 30-65
ip bgp neighbor maximum-prefix 30-67

ip bgp neighbor md5 key 30-69
ip bgp neighbor ebgp-multihop 30-71
ip bgp neighbor description 30-73
ip bgp neighbor next-hop-self 30-74
ip bgp neighbor passive 30-76
ip bgp neighbor remote-as 30-77
ip bgp neighbor remove-private-as 30-79
ip bgp neighbor soft-reconfiguration 30-80
ip bgp neighbor stats-clear 30-82
ip bgp confederation neighbor 30-83
ip bgp neighbor update-source 30-84
ip bgp neighbor in-aspathlist 30-86
ip bgp neighbor in-communitylist 30-87
ip bgp neighbor in-prefixlist 30-88
ip bgp neighbor in-prefix6list 30-89
ip bgp neighbor out-prefix6list 30-90
ip bgp neighbor out-aspathlist 30-91
ip bgp neighbor out-communitylist 30-92
ip bgp neighbor out-prefixlist 30-93
ip bgp neighbor route-map 30-94
ip bgp neighbor clear soft 30-96
ip bgp policy aspath-list 30-97
ip bgp policy aspath-list action 30-99
ip bgp policy aspath-list priority 30-101
ip bgp policy community-list 30-103
ip bgp policy community-list action 30-105
ip bgp policy community-list match-type 30-107
ip bgp policy community-list priority 30-109
ip bgp policy prefix-list 30-111
ip bgp policy prefix-list action 30-113
ip bgp policy prefix-list ge 30-114
ip bgp policy prefix-list le 30-116
ip bgp policy prefix6-list 30-118
ip bgp policy route-map 30-120
ip bgp policy route-map action 30-122
ip bgp policy route-map aspath-list 30-123
ip bgp policy route-map asprepend 30-124
ip bgp policy route-map community 30-125
ip bgp policy route-map community-list 30-127
ip bgp policy route-map community-mode 30-128
ip bgp policy route-map lpref 30-130
ip bgp policy route-map lpref-mode 30-131
ip bgp policy route-map match-community 30-133
ip bgp policy route-map match-mask 30-135
ip bgp policy route-map match-prefix 30-136
ip bgp policy route-map match-regexp 30-137
ip bgp policy route-map med 30-139
ip bgp policy route-map med-mode 30-140
ip bgp policy route-map origin 30-142
ip bgp policy route-map prefix-list 30-144
ip bgp policy route-map weight 30-146
ip bgp policy route-map community-strip 30-147

show ip bgp 30-148
show ip bgp statistics 30-151
show ip bgp dampening 30-153
show ip bgp dampening-stats 30-155
show ip bgp path 30-157
show ip bgp routes 30-161
show ip bgp aggregate-address 30-163
show ip bgp network 30-165
show ip bgp neighbors 30-167
show ip bgp neighbors policy 30-172
show ip bgp neighbors timer 30-174
show ip bgp neighbors statistics 30-176
show ip bgp policy aspath-list 30-181
show ip bgp policy community-list 30-183
show ip bgp policy prefix-list 30-185
show ip bgp policy prefix6-list 30-187
show ip bgp policy route-map 30-189
ip bgp graceful-restart 30-192
ip bgp graceful-restart restart-interval 30-193
ipv6 bgp unicast 30-194
ip bgp neighbor activate-ipv6 30-195
ip bgp neighbor ipv6-nexthop 30-196
show ipv6 bgp path 30-197
show ipv6 bgp routes 30-202
ipv6 bgp network 30-204
ipv6 bgp network community 30-205
ipv6 bgp network local-preference 30-207
ipv6 bgp network metric 30-209
ipv6 bgp network status 30-211
show ipv6 bgp network 30-212
ipv6 bgp neighbor 30-214
ipv6 bgp neighbor clear soft 30-216
ipv6 bgp neighbor soft-reconfiguration 30-217
ipv6 bgp neighbor in-prefix6list 30-219
ipv6 bgp neighbor out-prefix6list 30-220
ipv6 bgp neighbor activate-ipv6 30-221
ipv6 bgp neighbor ipv6-nexthop 30-222
ipv6 bgp neighbor status 30-223
ipv6 bgp neighbor remote-as 30-224
ipv6 bgp neighbor timers 30-225
ipv6 bgp neighbor maximum-prefix 30-227
ipv6 bgp neighbor next-hop-self 30-229
ipv6 bgp neighbor conn-retry-interval 30-230
ipv6 bgp neighbor default-originate 30-231
ipv6 bgp neighbor update-source 30-232
ipv6 bgp neighbor ipv4-nexthop 30-233
show ipv6 bgp neighbors 30-234
show ipv6 bgp neighbors statistics 30-239
show ipv6 bgp neighbors timers 30-244
show ipv6 bgp neighbors policy 30-246

Chapter 31 Server Load Balancing Commands 31-1
ip slb admin 31-2
ip slb reset statistics 31-3
ip slb cluster 31-4
ip slb cluster admin status 31-6
ip slb cluster ping period 31-7
ip slb cluster ping timeout 31-9
ip slb cluster ping retries 31-11
ip slb cluster probe 31-12
ip slb server ip cluster 31-13
ip slb server ip cluster probe 31-15
ip slb probe 31-16
ip slb probe timeout 31-18
ip slb probe period 31-20
ip slb probe port 31-22
ip slb probe retries 31-24
ip slb probe username 31-26
ip slb probe password 31-27
ip slb probe url 31-28
ip slb probe status 31-29
ip slb probe send 31-30
ip slb probe expect 31-31
show ip slb 31-32
show ip slb clusters 31-34
show ip slb cluster 31-36
show ip slb cluster server 31-39
show ip slb servers 31-42
show ip slb probes 31-44

Chapter 32 IP Multicast Switching Commands 32-1
ip multicast status 32-4
ip multicast flood-unknown 32-5
ip multicast querier-forwarding 32-7
ip multicast version 32-9
ip multicast max-group 32-11
ip multicast vlan max-group 32-13
ip multicast port max-group 32-15
ip multicast static-neighbor 32-17
ip multicast static-querier 32-19
ip multicast static-group 32-21
ip multicast query-interval 32-23
ip multicast last-member-query-interval 32-25
ip multicast query-response-interval 32-27
ip multicast unsolicited-report-interval 32-29
ip multicast router-timeout 32-31
ip multicast source-timeout 32-33
ip multicast querying 32-35
ip multicast robustness 32-37
ip multicast spoofing 32-39
ip multicast zapping 32-41
ip multicast proxying 32-43
ip multicast helper-address 32-45

ipv6 multicast status 32-46
ipv6 multicast querier-forwarding 32-48
ipv6 multicast version 32-50
ipv6 multicast max-group 32-52
ipv6 multicast vlan max-group 32-54
ipv6 multicast port max-group 32-56
ipv6 multicast static-neighbor 32-58
ipv6 multicast static-querier 32-60
ipv6 multicast static-group 32-62
ipv6 multicast query-interval 32-64
ipv6 multicast last-member-query-interval 32-66
ipv6 multicast query-response-interval 32-68
ipv6 multicast unsolicited-report-interval 32-70
ipv6 multicast router-timeout 32-72
ipv6 multicast source-timeout 32-74
ipv6 multicast querying 32-76
ipv6 multicast robustness 32-78
ipv6 multicast spoofing 32-80
ipv6 multicast zapping 32-82
ipv6 multicast proxying 32-84
ip multicast static-ssm-map 32-86
show ip multicast static-ssm-map 32-88
show ip multicast 32-89
show ip multicast port 32-94
show ip multicast forward 32-97
show ip multicast neighbor 32-99
show ip multicast querier 32-101
show ip multicast group 32-103
show ip multicast source 32-105
show ip multicast tunnel 32-107
show ipv6 multicast 32-108
show ipv6 multicast port 32-113
show ipv6 multicast forward 32-115
show ipv6 multicast neighbor 32-117
show ipv6 multicast querier 32-119
show ipv6 multicast group 32-121
show ipv6 multicast source 32-123
show ipv6 multicast tunnel 32-125

Chapter 33 IP Multicast VLAN Commands 33-1
vlan ipmvlan 33-2
vlan ipmvlan ctag 33-4
vlan ipmvlan address 33-6
vlan ipmvlan sender-port 33-8
vlan ipmvlan receiver-port 33-10
show vlan ipmvlan c-tag 33-12
show vlan ipmvlan address 33-13
show vlan ipmvlan port-config 33-15
show ipmvlan port-config 33-17

Chapter 34 DVMRP Commands 34-1
ip load dvmrp 34-2
ip dvmrp status 34-3
ip dvmrp flash-interval 34-5
ip dvmrp graft-timeout 34-6
ip dvmrp interface 34-7
ip dvmrp interface metric 34-8
ip dvmrp neighbor-interval 34-9
ip dvmrp neighbor-timeout 34-10
ip dvmrp prune-lifetime 34-11
ip dvmrp prune-timeout 34-12
ip dvmrp report-interval 34-13
ip dvmrp route-holddown 34-14
ip dvmrp route-timeout 34-15
ip dvmrp subord-default 34-16
ip dvmrp tunnel 34-18
ip dvmrp tunnel ttl 34-20
ip dvmrp debug-level 34-22
ip dvmrp debug-type 34-23
show ip dvmrp 34-25
show ip dvmrp interface 34-28
show ip dvmrp neighbor 34-30
show ip dvmrp nexthop 34-32
show ip dvmrp prune 34-34
show ip dvmrp route 34-36
show ip dvmrp tunnel 34-38
show ip dvmrp debug 34-40

Chapter 35 PIM Commands 35-1
ip load pim 35-3
ip pim sparse status 35-5
ip pim sparse bfd-std status 35-6
ip pim interface bfd-std 35-7
ip pim dense redundant path status 35-9
ip pim dense status 35-11
ip pim ssm group 35-12
ip pim dense group 35-14
ip pim cbsr 35-16
ip pim static-rp 35-18
ip pim candidate-rp 35-20
ip pim rp-threshold 35-22
ip pim keepalive-period 35-23
ip pim max-rps 35-25
ip pim probe-time 35-27
ip pim register checksum 35-28
ip pim register-suppress-timeout 35-29
ip pim spt status 35-30
ip pim state-refresh-interval 35-31
ip pim state-refresh-limit 35-32
ip pim state-refresh-ttl 35-33
ip pim interface 35-34
ip pim neighbor-loss-notification-period 35-37

ip pim invalid-register-notification-period 35-38
ip pim invalid-joinprune-notification-period 35-39
ip pim rp-mapping-notification-period 35-40
ip pim interface-election-notification-period 35-41
show ip pim sparse 35-42
show ip pim dense 35-44
show ip pim ssm group 35-46
show ip pim dense group 35-48
show ip pim neighbor 35-50
show ip pim candidate-rp 35-53
show ip pim group-map 35-55
show ip pim interface 35-57
show ip pim static-rp 35-61
show ip pim cbsr 35-63
show ip pim bsr 35-65
show ip pim notifications 35-67
show ip pim groute 35-70
show ip pim sgroute 35-74
ipv6 pim sparse status 35-79
ipv6 pim dense status 35-80
ipv6 pim ssm group 35-81
ipv6 pim dense group 35-83
ipv6 pim cbsr 35-85
ipv6 pim static-rp 35-87
ipv6 pim candidate-rp 35-89
ipv6 pim rp-switchover 35-91
ipv6 pim spt status 35-92
ipv6 pim interface 35-93
show ipv6 pim sparse 35-96
show ipv6 pim dense 35-98
show ipv6 pim ssm group 35-100
show ipv6 pim dense group 35-102
show ipv6 pim interface 35-104
show ipv6 pim neighbor 35-108
show ipv6 pim static-rp 35-112
show ipv6 pim group-map 35-114
show ipv6 pim candidate-rp 35-116
show ipv6 pim cbsr 35-118
show ipv6 pim bsr 35-120
show ipv6 pim groute 35-122
show ipv6 pim sgroute 35-126

Chapter 36 Multicast Routing Commands 36-1
ip mroute-boundary 36-3
ipv6 mroute-boundary 36-5
ip mroute interface ttl 36-6
ipv6 mroute interface ttl 36-7
show ip mroute-boundary 36-8
show ipv6 mroute-boundary 36-10
show ip mroute 36-12
show ipv6 mroute 36-14
show ip mroute interface 36-16

show ipv6 mroute interface 36-18
show ip mroute-nexthop 36-20
show ipv6 mroute-nexthop 36-22

Chapter 37 QoS Commands 37-1
qos 37-3
qos trust ports 37-5
qos default servicing mode 37-7
qos forward log 37-9
qos log console 37-10
qos log lines 37-11
qos log level 37-12
qos default bridged disposition 37-14
qos default routed disposition 37-16
qos default multicast disposition 37-17
qos user-port 37-18
qos dei 37-21
qos stats interval 37-23
qos nms priority 37-24
qos phones 37-26
qos quarantine mac-group 37-28
qos quarantine path 37-30
qos quarantine page 37-31
debug qos 37-32
debug qos internal 37-34
qos clear log 37-36
qos apply 37-37
qos revert 37-38
qos flush 37-39
qos reset 37-41
qos stats reset 37-42
qos port reset 37-43
qos port 37-44
qos port trusted 37-46
qos port servicing mode 37-48
qos port q minbw maxbw 37-50
qos port maximum egress-bandwidth 37-52
qos port maximum ingress-bandwidth 37-54
qos port default 802.1p 37-56
qos port default dscp 37-58
qos port default classification 37-60
qos port dei 37-62
qos port monitor 37-64
show qos port 37-66
show qos port monitor 37-68
show qos queue 37-70
show qos slice 37-73
show qos log 37-75
show qos config 37-77
show qos statistics 37-80

Chapter 38 QoS Policy Commands 38-1
aclman 38-6
policy rule 38-7
policy validity period 38-11
policy list 38-14
policy network group 38-17
policy service group 38-19
policy mac group 38-21
policy port group 38-23
policy vlan group 38-25
policy map group 38-27
policy service 38-29
policy service protocol 38-32
policy service source tcp port 38-34
policy service destination tcp port 38-36
policy service source udp port 38-38
policy service destination udp port 38-40
policy condition 38-42
policy condition source ip 38-47
policy condition source ipv6 38-49
policy condition destination ip 38-51
policy condition destination ipv6 38-53
policy condition multicast ip 38-55
policy condition source network group 38-57
policy condition destination network group 38-59
policy condition multicast network group 38-61
policy condition source ip port 38-63
policy condition destination ip port 38-65
policy condition source tcp port 38-67
policy condition destination tcp port 38-69
policy condition source udp port 38-71
policy condition destination udp port 38-73
policy condition ethertype 38-75
policy condition established 38-77
policy condition tcpflags 38-79
policy condition service 38-81
policy condition service group 38-82
policy condition icmptype 38-84
policy condition icmpcode 38-86
policy condition ip protocol 38-88
policy condition ipv6 38-90
policy condition nh 38-92
policy condition flow-label 38-94
policy condition tos 38-96
policy condition dscp 38-98
policy condition source mac 38-100
policy condition destination mac 38-102
policy condition source mac group 38-104
policy condition destination mac group 38-106
policy condition source vlan 38-108
policy condition source vlan group 38-110
policy condition inner source vlan 38-112

policy condition inner source vlan group 38-114
policy condition destination vlan 38-116
policy condition 802.1p 38-118
policy condition inner 802.1p 38-120
policy condition source port 38-122
policy condition destination port 38-124
policy condition source port group 38-126
policy condition destination port group 38-128
policy condition vrf 38-130
policy action 38-132
policy action disposition 38-135
policy action shared 38-137
policy action priority 38-139
policy action maximum bandwidth 38-141
policy action maximum depth 38-143
policy action cir 38-145
policy action tos 38-148
policy action 802.1p 38-150
policy action dscp 38-152
policy action map 38-154
policy action permanent gateway ip 38-156
policy action port-disable 38-158
policy action redirect port 38-160
policy action redirect linkagg 38-162
policy action no-cache 38-164
policy action mirror 38-165
show policy classify 38-167
show policy classify source port 38-170
show policy classify destination port 38-172
show policy classify source mac 38-174
show policy classify destination mac 38-176
show policy classify source vlan 38-178
show policy classify destination vlan 38-180
show policy classify source interface type 38-182
show policy classify destination interface type 38-184
show policy classify 802.1p 38-186
show policy classify source ip 38-187
show policy classify destination ip 38-189
show policy classify multicast ip 38-191
show policy classify tos 38-193
show policy classify dscp 38-195
show policy classify ip protocol 38-197
show policy classify source ip port 38-199
show policy classify destination ip port 38-201
show policy network group 38-203
show policy service 38-205
show policy service group 38-207
show policy mac group 38-209
show policy port group 38-211
show policy vlan group 38-213
show policy map group 38-215
show policy action 38-217

show policy condition 38-220
show active policy rule 38-223
show active policy rule meter-statistics 38-226
show policy rule 38-229
show policy validity period 38-232
show active policy list 38-234
show policy list 38-236

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 40 802.1X Commands 40-1
802.1x 40-3
802.1x initialize 40-6
802.1x re-authenticate 40-7
802.1x supp-polling retry 40-8
802.1x supplicant bypass 40-10
802.1x non-supplicant allow-eap 40-12
802.1x pass-through 40-14
captive-portal pass-through 40-15
802.1x supplicant policy authentication 40-17
802.1x non-supplicant policy authentication 40-20
802.1x non-supplicant policy 40-23
802.1x policy default 40-25
802.1x captive-portal policy authentication 40-27
802.1x captive-portal session-limit 40-29
802.1x captive-portal name 40-31
802.1x captive-portal inactivity-logout 40-32
802.1x captive-portal retry-count 40-33
802.1x captive-portal address 40-35
802.1x captive-portal proxy-server-url 40-36
802.1x captive-portal proxy-server-port 40-38
802.1x captive-portal dns-keyword-list 40-39
802.1x captive-portal success-redirect-url 40-41
802.1x captive-portal fail-redirect-url 40-43
802.1x auth-server-down 40-45
802.1x auth-server-down policy 40-46
802.1x auth-server-down re-authperiod 40-48
show 802.1x 40-49
show 802.1x users 40-52
show 802.1x statistics 40-54
show 802.1x device classification policies 40-56
show 802.1x non-supplicant 40-58
show 802.1x rate-limit 40-60
show 802.1x auth-server-down 40-62

show 802.1x captive-portal configuration 40-64

Chapter 41 AAA Commands 41-1
aaa radius-server 41-5
aaa radius agent preferred 41-8
aaa tacacs+-server 41-10
aaa ldap-server 41-12
aaa ace-server clear 41-15
system fips 41-16
show system fips-status 41-18
aaa test-radius-server 41-19
aaa authentication vlan single-mode 41-21
aaa authentication vlan multiple-mode 41-23
aaa vlan no 41-25
aaa avlan dns 41-26
aaa avlan default dhcp 41-27
aaa authentication 41-28
aaa authentication default 41-31
aaa tacacs command-authorization 41-33
aaa authentication 802.1x 41-35
aaa authentication mac 41-37
aaa certificate-password 41-39
aaa accounting 802.1x 41-40
aaa accounting mac 41-42
aaa accounting vlan 41-44
aaa accounting session 41-46
aaa accounting session-id 41-48
aaa accounting command 41-49
avlan default-traffic 41-51
avlan port-bound 41-53
avlan auth-ip 41-55
aaa avlan http language 41-57
user 41-58
password 41-62
user password-size min 41-64
user password-expiration 41-65
user password-policy cannot-contain-username 41-67
user password-policy min-uppercase 41-68
user password-policy min-lowercase 41-69
user password-policy min-digit 41-70
user password-policy min-nonalpha 41-71
user password-history 41-72
user password-min-age 41-73
user lockout-window 41-74
user lockout-threshold 41-76
user lockout-duration 41-78
user lockout unlock 41-80
aaa admin-logout 41-81
end-user profile 41-83
end-user profile port-list 41-85
end-user profile vlan-range 41-87
aaa user-network-profile 41-89

aaa classification-rule mac-address 41-92
aaa classification-rule mac-address-range 41-94
aaa classification-rule ip-address 41-96
aaa hic server-name 41-98
aaa hic redundancy background-poll-interval 41-100
aaa hic server-failure mode 41-102
aaa hic server-failure policy user-network-profile change 41-103
aaa hic allowed-name 41-105
aaa hic 41-107
aaa hic web-agent-url 41-109
aaa hic custom-proxy-port 41-110
show aaa server 41-111
show aaa authentication vlan 41-114
show aaa authentication 41-116
show aaa authentication 802.1x 41-118
show aaa authentication mac 41-120
show aaa accounting 802.1x 41-121
show aaa accounting mac 41-122
show aaa accounting vlan 41-124
show aaa accounting 41-126
show user 41-128
show user password-size 41-132
show user password-expiration 41-133
show user password-policy 41-134
show user lockout-setting 41-136
show avlan user 41-138
show aaa avlan config 41-140
show aaa avlan auth-ip 41-142
debug command-info 41-144
debug end-user profile 41-146
show end-user profile 41-148
show aaa user-network-profile 41-150
show aaa classification-rule 41-152
show aaa hic 41-154
show aaa hic host 41-156
show aaa hic server 41-158
show aaa hic server-failure policy 41-160
show aaa hic allowed 41-162
show aaa priv hexa 41-164
show aaa-device all-users 41-167
show aaa-device supplicant-users 41-170
show aaa-device non-supplicant-users 41-173
show aaa-device captive-portal-users 41-176
802.1x kerberos 41-179
aaa kerberos mac-move 41-181
aaa kerberos inactivity-timer 41-182
aaa kerberos ip-address 41-183
aaa kerberos server-timeout 41-185
aaa kerberos authentication-pass policy-list-name 41-186
aaa kerberos authentication-pass domain 41-189
show aaa kerberos configuration 41-191
show aaa kerberos port 41-194

show aaa kerberos users 41-196
show aaa kerberos statistics 41-198
show aaa kerberos port statistics 41-200
clear aaa kerberos statistics 41-202
clear aaa kerberos port statistics 41-203

Chapter 42 UNP Commands 42-1
unp name 42-3
unp port 42-5
unp port default-unp 42-8
unp port mac-authentication 42-10
unp port mac-authentication pass-alternate 42-12
unp port classification 42-14
unp port trust-tag 42-16
unp classification mac-address 42-18
unp classification mac-range 42-20
unp classification ip-address 42-22
unp classification vlan-tag 42-24
unp dynamic-vlan-configuration 42-26
unp dynamic-profile-configuration 42-28
unp auth-server-down-unp 42-30
unp auth-server-down-timeout 42-31
show unp 42-32
show unp global configuration 42-34
show unp classification 42-37
show unp port 42-41
show unp user 42-44

Chapter 43 Port Mobility Commands 43-1
vlan dhcp mac 43-2
vlan dhcp mac range 43-4
vlan dhcp port 43-6
vlan dhcp generic 43-8
vlan binding mac-ip-port 43-10
vlan binding mac-port 43-12
vlan binding port-protocol 43-14
vlan mac 43-16
vlan mac range 43-18
vlan ip 43-20
vlan ipx 43-22
vlan protocol 43-24
vlan port 43-26
vlan port mobile 43-28
vlan port default vlan restore 43-30
vlan port default vlan 43-32
vlan port authenticate 43-34
vlan port 802.1x 43-35
show vlan rules 43-37
show vlan port mobile 43-39

Chapter 44 Network Security Commands 44-1
netsec group port 44-2
netsec group anomaly 44-4
show netsec summary 44-7
show netsec traffic 44-10
show netsec statistics 44-13
show netsec config 44-16
show netsec operation 44-18
show netsec group port 44-21

Chapter 45 Port Mapping Commands 45-1
port mapping user-port network-port 45-2
port mapping 45-4
port mapping 45-6
port mapping unknown-unicast-flooding 45-8
port mapping dynamic-proxy-arp 45-10
show port mapping status 45-12
show port mapping 45-14

Chapter 46 Learned Port Security Commands 46-1
port-security 46-2
port-security shutdown 46-4
port-security maximum 46-7
port-security max-filtering 46-9
port-security convert-to-static 46-11
port-security mac 46-13
port-security mac-range 46-15
port-security violation 46-17
port-security release 46-19
port-security learn-trap-threshold 46-21
show port-security 46-23
show port-security shutdown 46-26
show port-security brief 46-28

Chapter 47 Port Mirroring and Monitoring Commands 47-1
port mirroring source destination 47-2
port mirroring 47-5
port monitoring source 47-7
port monitoring 47-9
show port mirroring status 47-10
show port monitoring status 47-13
show port monitoring file 47-15

Chapter 48 sFlow Commands 48-1
sflow agent 48-3
sflow receiver 48-4
sflow sampler 48-6
sflow poller 48-8
show sflow agent 48-10
show sflow receiver 48-12
show sflow sampler 48-14
show sflow poller 48-16

Chapter 49 RMON Commands 49-1
rmon probes 49-2
show rmon probes 49-4
show rmon events 49-7

Chapter 50 VLAN Stacking Commands 50-1
ethernet-service 50-2
ethernet-service custom-L2-protocol 50-4
ethernet-service source-learning 50-7
ethernet-service service-name 50-9
ethernet-service svlan nni 50-11
ethernet-service nni 50-13
ethernet-service sap 50-16
ethernet-service sap uni 50-18
ethernet-service sap cvlan 50-20
ethernet-service sap-profile 50-22
ethernet-service sap sap-profile 50-25
ethernet-service uni-profile 50-27
ethernet-service uni uni-profile 50-31
ethernet-service uni-profile custom-L2-protocol 50-33
show ethernet-service custom-L2-protocol 50-35
show ethernet-service mode 50-37
show ethernet-service vlan 50-38
show ethernet-service 50-40
show ethernet-service sap 50-43
show ethernet-service port 50-45
show ethernet-service nni 50-48
show ethernet-service nni l2pt-statistics 50-50
clear ethernet-service nni l2pt-statistics 50-52
show ethernet-service uni 50-54
show ethernet-service uni l2pt-statistics 50-56
clear ethernet-service uni l2pt-statistics 50-59
show ethernet-service uni-profile 50-61
show ethernet-service sap-profile 50-63
loopback-test 50-65
show loopback-test 50-68

Chapter 51 Ethernet OAM Commands 51-1
ethoam vlan 51-3
ethoam domain 51-5
ethoam domain mhf 51-7
ethoam domain id-permission 51-8
ethoam association 51-9
ethoam association mhf 51-11
ethoam association id-permission 51-13
ethoam association ccm-interval 51-15
ethoam association endpoint-list 51-17
clear ethoam statistics 51-19
ethoam default-domain level 51-20
ethoam default-domain mhf 51-21
ethoam default-domain id-permission 51-22
ethoam default-domain primary-vlan 51-23

ethoam endpoint 51-25
ethoam endpoint admin-state 51-27
ethoam endpoint rfp 51-29
ethoam endpoint ccm 51-31
ethoam endpoint priority 51-33
ethoam endpoint lowest-priority-defect 51-35
ethoam linktrace 51-37
ethoam loopback 51-39
ethoam fault-alarm-time 51-41
ethoam fault-reset-time 51-43
ethoam one-way-delay 51-45
ethoam two-way-delay 51-47
clear ethoam 51-49
show ethoam 51-50
show ethoam domain 51-52
show ethoam domain association 51-54
show ethoam domain association end-point 51-56
show ethoam default-domain configuration 51-59
show ethoam default-domain 51-61
show ethoam remote-endpoint domain 51-63
show ethoam cfmstack 51-65
show ethoam linktrace-reply 51-67
show ethoam linktrace-tran-id 51-70
show ethoam vlan 51-72
show ethoam statistics 51-73
show ethoam config-error 51-75
show ethoam one-way-delay 51-77
show ethoam two-way-delay 51-79

Chapter 52 LINK OAM Commands 52-1
efm-oam 52-3
efm-oam port status 52-4
efm-oam port mode 52-6
efm-oam port keepalive-interval 52-8
efm-oam port hello-interval 52-9
efm-oam port remote-loopback 52-11
efm-oam port remote-loopback start 52-13
efm-oam port propagate-events 52-15
efm-oam errored-frame-period 52-17
efm-oam errored-frame 52-19
efm-oam errored-frame-seconds-summary 52-21
efm-oam multiple-pdu-count 52-23
efm-oam port l1-ping 52-24
show efm-oam configuration 52-26
show efm-oam port 52-27
show efm-oam port detail 52-31
show efm-oam port statistics 52-34
show efm-oam port remote detail 52-38
show efm-oam port history 52-40
show efm-oam port l1-ping detail 52-42
clear efm-oam statistics 52-44
clear efm-oam log-history 52-45

Chapter 53 Service Assurance Agent Commands 53-1
saa 53-2
saa type ip-ping 53-4
saa type ethoamloopback 53-6
saa type ethoam-two-way-delay 53-9
saa type mac-ping 53-11
saa start 53-14
saa stop 53-16
show saa 53-18
show saa type config 53-20
show saa statistics 53-24
show saa statistics history index 53-30

Chapter 54 MPLS LDP Commands 54-1
configure router ldp shutdown 54-3
configure router ldp interface-parameters interface 54-4
configure router ldp interface-parameters interface shutdown 54-6
configure router ldp interface-parameters hello 54-7
configure router ldp interface-parameters keepalive 54-9
configure router ldp interface-parameters transport-address 54-11
configure router ldp targeted-session hello 54-13
configure router ldp targeted-session keepalive 54-15
configure router ldp graceful-restart-helper 54-17
configure router ldp reconnect-time 54-19
configure router ldp fwd-state-holding-time 54-21
configure router ldp maximum-recovery-time 54-23
configure router ldp neighbor-liveness-time 54-25
oam lsp-ping 54-27
oam lsp-trace 54-30
show router ldp bindings 54-33
show router ldp bindings fec-type 54-36
show router ldp bindings ingress-label 54-39
show router ldp bindings egress-label 54-42
show router ldp bindings prefix 54-45
show router ldp bindings active 54-47
show router ldp bindings vc-type 54-49
show router ldp bindings service-id 54-52
show router ldp discovery 54-54
show router ldp discovery peer 54-57
show router ldp discovery interface 54-60
show router ldp interface 54-63
show router ldp parameters 54-66
show router ldp peer 54-70
show router ldp session 54-73
show router ldp status 54-77

Chapter 55 MPLS Static LSP and FRR Commands 55-1
configure router mpls shutdown 55-3
configure router mpls interface 55-4
configure router mpls interface shutdown 55-5
configure router mpls interface label-map 55-6
configure router mpls interface label-map swap next-hop 55-8

configure router mpls interface label-map pop 55-10
configure router mpls interface label-map shutdown 55-12
configure router mpls static-lsp 55-14
configure router mpls static-lsp shutdown 55-16
configure router mpls static-lsp to 55-18
configure router mpls static-lsp push next-hop 55-20
configure router mpls interface label-map protect-swap next-hop 55-22
show router mpls interface 55-24
show router mpls label 55-27
show router mpls label-range 55-31
show router mpls static-lsp 55-33
show router mpls status 55-36

Chapter 56 Virtual Private LAN Service (VPLS) Commands 56-1
configure service customer create 56-3
configure service customer contact 56-5
configure service customer phone 56-7
configure service customer description 56-9
configure service sdp create 56-11
configure service sdp description 56-13
configure service sdp far-end 56-15
configure service sdp shutdown 56-17
configure service sdp ldp 56-19
configure service sdp signaling 56-21
configure service sdp lsp 56-23
configure service sdp adv-mtu-override 56-25
configure service sdp path-mtu 56-27
configure service vpls create 56-29
configure service vpls description 56-31
configure service vpls shutdown 56-33
configure service vpls def-mesh-vc-id 56-35
configure service vpls send-flush-on-failure 56-37
configure service vpls service-mtu 56-39
configure service vpls mesh-sdp 56-41
configure service vpls mesh-sdp shutdown 56-43
configure service vpls mesh-sdp egress vc-label 56-45
configure service vpls mesh-sdp ingress vc-label 56-47
configure service vpls mesh-sdp static-mac 56-49
configure service l2profile 56-51
configure service port mode access 56-54
configure service port l2profile 56-56
configure service port encap-type 56-58
configure service vpls sap create 56-60
configure service vpls sap description 56-62
configure service vpls sap trusted 56-64
configure service vpls sap shutdown 56-66
configure service vpls sap static-mac 56-68
clear service id fdb 56-70
clear service id mesh-sdp ingress-vc-label 56-72
show service l2profile 56-74
show service port 56-76
show service customer 56-78

show service sdp 56-80
show service id all 56-84
show service id base 56-88
show service id labels 56-91
show service id sap 56-93
show service id sdp 56-96
show service sap-using 56-100
show service sdp-using 56-102
show service egress-label 56-104
show service ingress-label 56-106
show service fdb-info 56-108
show service fdb-mac 56-110

Chapter 57 Switch Logging Commands 57-1
swlog 57-2
swlog syslog-facility-id 57-3
swlog console level 57-5
swlog appid interface level 57-7
swlog remote command-log 57-10
swlog output 57-11
swlog output flash file-size 57-13
swlog clear 57-14
show log swlog 57-15
show swlog 57-18

Chapter 58 Health Monitoring Commands 58-1
health threshold 58-2
health interval 58-4
health statistics reset 58-5
show health threshold 58-6
show health interval 58-8
show health 58-9
show health all 58-11
show health slice 58-13
show health fabric 58-15

Chapter 59 CMM Commands 59-1
reload 59-2
reload working 59-4
reload issu 59-6
copy running-config working 59-8
write memory 59-10
write memory flash-synchro 59-11
copy working certified 59-13
copy flash-synchro 59-15
takeover 59-16
show running-directory 59-18
show reload 59-21
show microcode 59-22
show microcode history 59-24
show microcode issu 59-25
usb 59-27

usb auto-copy 59-28
usb disaster-recovery 59-30
mount 59-31
umount 59-32
show usb statistics 59-33
show issu status 59-35
show issu signature 59-38

Chapter 60 Chassis Management and Monitoring Commands 60-1
system contact 60-3
system name 60-4
system location 60-5
system date 60-6
system time 60-7
system time-and-date synchro 60-8
system timezone 60-9
system daylight savings time 60-12
update 60-14
update lanpower 60-16
reload ni 60-17
reload all 60-19
reload pass-through 60-21
power ni 60-23
temp-threshold 60-24
stack set slot 60-25
stack clear slot 60-27
show system 60-29
show hardware info 60-31
show chassis 60-33
show cmm 60-35
show ni 60-38
show module 60-41
show module long 60-43
show module status 60-45
show power 60-47
show fan 60-49
show temperature 60-51
show stack topology 60-53
show stack status 60-56
hash-control 60-58
show hash-control 60-60
license apply 60-61
show license info 60-62
show license file 60-63
power slot bps connector-priority 60-65
power bps mode 60-67
update bps firmware 60-68
show power bps connector-priority 60-69
show power supply bps 60-71

Chapter 61 Chassis MAC Server (CMS) Commands 61-1
mac-range eeprom 61-2
mac-retention status 61-4
mac-retention dup-mac-trap 61-5
mac release 61-6
show mac-range 61-7
show mac-range alloc 61-9
show mac-retention status 61-11

Chapter 62 Network Time Protocol Commands 62-1
ntp server 62-2
ntp server synchronized 62-4
ntp server unsynchronized 62-5
ntp client 62-6
ntp src-ip preferred 62-7
ntp broadcast-client 62-9
ntp broadcast-delay 62-10
ntp key 62-11
ntp key load 62-13
ntp authenticate 62-14
ntp master 62-15
ntp interface 62-16
ntp max-associations 62-17
ntp broadcast 62-18
ntp peer 62-20
show ntp status 62-22
show ntp client 62-24
show ntp client server-list 62-26
show ntp server client-list 62-28
show ntp server status 62-30
show ntp keys 62-34
show ntp peers 62-36
show ntp server disabled-interfaces 62-38

Chapter 63 Session Management Commands 63-1
session login-attempt 63-3
session login-timeout 63-4
session banner 63-5
session timeout 63-7
session reauth-interval 63-9
session prompt default 63-11
session xon-xoff 63-13
prompt 63-14
show prefix 63-16
alias 63-17
show alias 63-19
user profile save 63-20
user profile save global-profile 63-21
user profile reset 63-23
history size 63-24
show history 63-25
! 63-27

command-log 63-29
kill 63-30
exit 63-31
whoami 63-32
who 63-35
show session config 63-37
show session xon-xoff 63-39
more size 63-40
more 63-41
show more 63-42
telnet 63-43
telnet6 63-45
ssh 63-47
ssh6 63-49
ssh enforce pubkey-auth 63-51
show ssh config 63-52
show command-log 63-54
show command-log status 63-56

Chapter 64 File Management Commands 64-1
cd 64-3
pwd 64-5
mkdir 64-6
rmdir 64-8
ls 64-10
dir 64-12
rename 64-14
rm 64-16
delete 64-18
cp 64-19
scp 64-21
mv 64-23
move 64-25
chmod 64-27
attrib 64-28
freespace 64-29
fsck 64-30
newfs 64-32
rcp 64-33
rrm 64-35
rls 64-36
vi 64-38
view 64-39
tty 64-40
show tty 64-42
more 64-43
ftp 64-45
ftp6 64-47
scp-sftp 64-49
show ssh config 64-50
sftp 64-52
sftp6 64-54

tftp 64-56
rz 64-58

Chapter 65 Web Management Commands 65-1
http server 65-2
http ssl 65-3
http port 65-4
https port 65-5
debug http sessiondb 65-6
show http 65-8

Chapter 66 Configuration File Manager Commands 66-1
configuration apply 66-2
configuration error-file limit 66-4
show configuration status 66-6
configuration cancel 66-8
configuration syntax check 66-9
configuration snapshot 66-11
show configuration snapshot 66-14
write terminal 66-18

Chapter 67 SNMP Commands 67-1
snmp station 67-3
snmp source ip preferred 67-5
show snmp station 67-6
snmp community map 67-8
snmp community map mode 67-10
show snmp community map 67-11
snmp security 67-12
show snmp security 67-14
show snmp statistics 67-16
show snmp mib family 67-18
snmp trap absorption 67-19
snmp trap to webview 67-20
snmp trap replay 67-21
snmp trap filter 67-23
snmp authentication trap 67-25
show snmp trap replay 67-26
show snmp trap filter 67-28
show snmp authentication trap 67-30
show snmp trap config 67-31
show snmp object 67-33

Chapter 68 DNS Commands 68-1
ip domain-lookup 68-2
ip name-server 68-3
ipv6 name-server 68-5
ip domain-name 68-7
show dns 68-8

Appendix A **Software License and Copyright Statements** A-1

Alcatel-Lucent License Agreement A-1
ALCATEL-LUCENT 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 2.8, 17 August 2003 ..... 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-12
L. Wind River Systems, Inc. A-12
M. Network Time Protocol Version 4 ..... A-12
N. Remote-ni A-13
O. GNU Zip A-13
P. FREESCALE SEMICONDUCTOR SOFTWARE LICENSE AGREEMENT A-13
Q. Boost C++ Libraries A-14
R. U-Boot A-14
S. Solaris A-14
T. Internet Protocol Version 6 ..... A-14
U. CURSES A-15
V. ZModem A-15
W. Boost Software License A-15
X. OpenLDAP A-15
Y. BITMAP.C A-16
Z. University of Toronto A-16
AA.Free/OpenBSD A-16

CLI Quick Reference

Index Index-1

About This Guide

This *OmniSwitch AOS Release 6 CLI Reference Guide* is a comprehensive resource to all Command Line Interface (CLI) commands available on the OmniSwitch 6400 Series, OmniSwitch 6855 Series, OmniSwitch 6850E Series, and OmniSwitch 9000E Series switches.

Supported Platforms

This information in this guide applies to the following products:

- OmniSwitch 6850E Series
- OmniSwitch 9000E Series (9700E and 9800E switches)
- OmniSwitch 6400 Series
- OmniSwitch 6855 Series

Note. This *OmniSwitch AOS Release 6 CLI Reference Guide* covers Release 6.4.5, which is supported on the OmniSwitch 6400 Series, OmniSwitch 6855 Series, OmniSwitch 6850E Series, and OmniSwitch 9000E Series switches.

Unsupported Platforms

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

- OmniSwitch (original version with no numeric model name)
- OmniSwitch 6850
- OmniSwitch 6600 Family
- OmniSwitch 6800 Family
- OmniSwitch 7700/7800
- OmniSwitch 8800
- OmniSwitch 9000
- 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 AOS Release 6 CLI Reference Guide*, *OmniSwitch AOS Release 6 Network Configuration Guide*, and the *OmniSwitch AOS Release 6 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.

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 *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 related OmniSwitch AOS Release 6 user manuals:

- *OmniSwitch 6400 Series Getting Started Guide*

  Describes the hardware and software procedures for getting an OmniSwitch 6400 Series switch up and running. Also provides information on fundamental aspects of OmniSwitch software and stacking architecture.

- *OmniSwitch 6855 Series Getting Started Guide*

  Describes the basic information you need to unpack and identify the components of your OmniSwitch 6855 shipment. Also provides information on the initial configuration of the switch.

- *OmniSwitch 6850E Series Getting Started Guide*

  Describes the hardware and software procedures for getting an OmniSwitch 6850E Series up and running. Also provides information on fundamental aspects of OmniSwitch software architecture.

- *OmniSwitch 9000E Series Getting Started Guide*

  Describes the hardware and software procedures for getting an OmniSwitch 9000E Series switch up and running. Also provides information on fundamental aspects of OmniSwitch software architecture

- *OmniSwitch 6400 Series Hardware Users Guide*

  Complete technical specifications and procedures for all OmniSwitch 6400 Series chassis, power supplies, and fans. Also includes comprehensive information on assembling and managing stacked configurations.

- *OmniSwitch 6855 Series Hardware User Guide*

  Complete technical specifications and procedures for all OmniSwitch 6855 Series chassis, power supplies, and fans.

- *OmniSwitch 6850E Series Hardware Users Guide*

  Complete technical specifications and procedures for all OmniSwitch 6850E Series chassis, power supplies, fans, and Network Interface (NI) modules.

- *OmniSwitch 9000E Series Hardware User Guide*

  Complete technical specifications and procedures for all OmniSwitch 9000E Series chassis, power supplies, and fans.

- *OmniSwitch AOS Release 6 CLI Reference Guide*

  Complete reference to all CLI commands supported on the OmniSwitch 6400, 6850E, 6855, and 9000E. Includes syntax definitions, default values, examples, usage guidelines and CLI-to-MIB variable mappings.

- *OmniSwitch AOS Release 6 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 AOS Release 6 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), security options (authenticated VLANs), Quality of Service (QoS), and link aggregation.

- *OmniSwitch AOS Release 6 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), and OSPF.

- *OmniSwitch AOS Release 6 Transceivers Guide*

  Includes information on Small Form Factor Pluggable (SFPs) and 10 Gbps Small Form Factor Pluggables (XFPs) transceivers.

- Technical Tips, Field Notices

  Includes information published by Alcatel-Lucent’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 Manual CD

Some products are shipped with documentation included on a User Manual CD that accompanies the switch. This CD also includes documentation for other Alcatel-Lucent data enterprise products.

All products are shipped with a Product Documentation Card that provides details for downloading documentation for all OmniSwitch and other Alcatel-Lucent data enterprise products.

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

Note. In order to take advantage of the documentation CD's global search feature, it is recommended that you select the option for *searching PDF files* before downloading Acrobat Reader freeware.

To verify that you are using Acrobat Reader with the global search option, look for the following button in the toolbar:

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-Lucent 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-Lucent 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-Lucent'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-Lucent's technical support, open a new case or access helpful release notes, technical bulletins, and manuals. For more information on Alcatel-Lucent's Service Programs, see our web page at service.esd.alcatel-lucent.com, call us at 1-800-995-2696, or email us at esd.support@alcatel-lucent.com.

1 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**
Interfaces commands	**interfaces speed** **interfaces mode** **interfaces autoneg** **interfaces pause** **interfaces e2e-flow-vlan** **interfaces duplex** **interfaces admin** **interfaces cli-prompt** **interfaces alias** **interfaces ifg** **interfaces no l2 statistics** **interfaces max frame** **interfaces flood** **interfaces flood rate** **interfaces flood action** **interfaces wait-to-restore** **interfaces transceiver ddm** **show interfaces** **show interfaces capability** **show interfaces flow control** **show interfaces pause** **show interfaces e2e-flow-vlan** **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** **show interfaces transceiver**
Combo port commands	**interfaces hybrid preferred-fiber** **interfaces hybrid autoneg** **interfaces hybrid crossover** **interfaces hybrid duplex** **interfaces hybrid speed** **interfaces hybrid pause** **show interfaces hybrid** **show interfaces hybrid status** **show interfaces hybrid pause** **show interfaces hybrid capability** **show interfaces hybrid accounting** **show interfaces hybrid counters** **show interfaces hybrid counters errors** **show interfaces hybrid collisions** **show interfaces hybrid traffic** **show interfaces hybrid port** **show interfaces hybrid flood rate**

Debug interfaces commands	**debug interfaces set backpressure** **debug interfaces backpressure**
Link monitoring commands	**interfaces link-monitoring admin-status** **interfaces link-monitoring time-window** **interfaces link-monitoring link-flap-threshold** **interfaces link-monitoring link-error-threshold** **interfaces clear-link-monitoring-stats** **show interfaces link-monitoring config** **show interfaces link-monitoring statistics**
Link fault propagation commands	**link-fault-propagation group** **link-fault-propagation group source** **link-fault-propagation group destination** **link-fault-propagation group wait-to-shutdown** **show link-fault-propagation group**
TDR commands	**interfaces tdr-test-start** **interfaces no tdr-statistics** **show interfaces tdr-statistics**
Interface violation commands	**interfaces violation-recovery-time** **interfaces violation-recovery-maximum** **interfaces violation-recovery-trap** **interfaces clear-violation-all** **show interfaces port** **show interfaces violation-recovery**

trap port link

Enables or disables trap link messages for a specific slot or port. If enabled, a message is displayed on the Network Management Station (NMS) whenever the specified port changes state.

trap {*slot* | *slot*/*port***[-***port2***]} port link {enable | disable | on | off}**

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Enter a slot number to enable or disable trap link messages for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to enable or disable trap link messages on a specific interface or range of interfaces.
- When trap generation is set to **disable**, the events are logged in the switch log file only when the debug level for the application is set to **debug1** or other lower severity level (**debug2** or **debug3**) using the **swlog appid interface level** command.
- Similarly, when trap generation is set to **enable**, the events are logged in the switch log file with a level of **info** if debug level for application is set to **info** or other lower severity level (**debug1**, **debug2** or **debug3**).

Examples

```
-> trap 3/1 port link enable
-> trap 3 port link enable
-> trap 3/1-6 port link enable
```

Release History

Release 6.1; command was introduced.

Related Commands

show interfaces status	Displays interface line settings.
swlog appid interface level	Defines the level at which switch logging information will be filtered for the specified application.

MIB Objects

```
ifLinkUpDownTrapEnable
```

interfaces speed

Configures interface line speed.

interfaces {*slot* | *slot*/*port***[-***port2***]} speed {auto | 10 | 100 | 1000 | 10000 | max {100 | 1000}}**

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
auto	The switch automatically sets 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}	Auto

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The **auto** option sets the speed to auto-sensing.
- The 10 Gigabit fiber ports only support 10000 Mbps.
- Enter a slot number to configure the interface speed for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to configure the interface speed for a specific interface or range of interfaces.

Examples

```
-> interfaces 3/1 speed auto
-> interfaces 3 speed 100
-> interfaces 3/1-8 speed auto
```

Release History

Release 6.1; 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 mode

Configures the mode of the ports to allow the switch to act in standalone or stacking mode.

interfaces {*slot* | *slot/port***} mode {uplink | stacking}**

Syntax Definitions

slot	The slot number for a specific module.
slot/port	The slot and port number (3/1).
uplink	Configures the ports as uplinks allowing the switch to act in standalone mode for network connectivity.
stacking	Configures the ports as stacking to allow the switch to be stacked in a virtual chassis.

Defaults

parameter	default
mode	uplink

Platforms Supported

OmniSwitch 6850E, 6855-U24X

Usage Guidelines

- Mode change does not take affect until the switch is rebooted.
- Only supported on the 10-Gigabit SFP+ ports
- Changing the mode of one port automatically changes the other port to the same mode. Mixing port modes is not supported.
- After changing the mode a message will display in approximately 5 seconds indicating success or failure. Re-enter the command if the change is not successful.
- Enter a slot number to configure the mode for all interfaces on a specific slot.
- Enter a slot and port number to configure the mode for a specific interface.

Examples

```
-> interfaces 4/25 mode stacking
WED JUL 01 18:08:29 : HSM-CHASSIS (101) info message:
+++ Ni 4 Port 25,26 are set to stackable for next boot:OK

-> interfaces 4 mode uplink
WED JUL 01 18:08:29 : HSM-CHASSIS (101) info message:
+++ Ni 4 Port 25,26 are set to uplink for next boot:OK
```

Release History

Release 6.4.2; command was introduced.

Related Commands

show stack topology	Displays the current operating topology of switches in a stacked configuration.
show stack status	Displays the current redundant stacking status for a stacked configuration.
show ni	Displays the current status for a switch in standalone mode.

MIB Objects

```
esmPortModeTable
   esmPortModeIndex
   esmPortSavedMode
```

interfaces autoneg

Enables or disables auto negotiation on a single port, a range of ports, or an entire Network Interface (NI).

interfaces {*slot* | *slot*/*port***[-***port2***]} autoneg {enable | disable | on | off}**

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
enable	Enables auto negotiation.
disable	Disables auto negotiation.
on	Same as enable.
off	Same as disable.

Defaults

parameter	default
enable | **disable** | **on** | **off**	enable

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Copper Gigabit ports do not support disabling of auto negotiation.
- Enter a slot number to configure auto-negotiation for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to configure auto-negotiation for a specific interface or range of interfaces.

Examples

```
-> interfaces 3 autoneg disable
-> interfaces 3/1 autoneg disable
-> interfaces 3/1-4 autoneg disable
```

Release History

Release 6.1; command was introduced.

Related Commands

interfaces speed	Configures interface speed.
show interfaces status	Displays interface line settings.
show interfaces capability	Displays auto negotiation, speed, duplex, and crossover settings.

MIB Objects

```
esmConfTable
   esmPortCfgAutoNegotiation
```

interfaces pause

Configures whether or not the switch will transmit, honor, or transmit and honor flow control PAUSE frames on the specified interface. PAUSE frames are used to temporarily pause the flow of traffic between two connected devices to help prevent packet loss when traffic congestion occurs between switches.

interfaces {*slot* | *slot*/*port***[-***port2***]} pause {tx | rx | tx-and-rx | disable}**

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
tx	Transmits PAUSE frames to peer switches when traffic congestion occurs on the local interface. Does not honor PAUSE frames from peer switches.
rx	Allows interface to honor PAUSE frames from peer switches and temporarily stop sending traffic to the peer. Does not transmit PAUSE frames to peer switches.
tx-and-rx	Transmits and honors PAUSE frames when traffic congestion occurs between peer switches.
disable	Disables flow control on the interface.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Defaults

By default, flow control is disabled on all switch interfaces.

Usage Guidelines

- Note that if the standalone switch is a 24-port unit, then only the **interfaces pause** command is required to enable end-to-end (E2E) flow control. However, if the switch is a 48-port unit, then a flow control VLAN, which is configured using the **interfaces e2e-flow-vlan** command, is required in addition to enabling RX/TX pause flow control.
- A stack of switches or a chassis-based switch will honor receive pause frames.
- Flow control is only supported on interfaces configured to run in full-duplex mode; half-duplex mode is not supported.
- If both autonegotiation and flow control are enabled on the same local interface, autonegotiation calculates operational flow control settings for that interface. Note that the operational settings, as shown in the following table, override the configured settings as long as autonegotiation and flow control are both enabled for the interface:

Configured Local Tx	Configured Local Rx	Configured Remote Tx	Configured Remote Rx	Operational Local Tx	Operational Local Rx
No	No	No	No	No	No
Yes	Yes	Yes	Yes	Yes	Yes
Yes	No	Yes	No	No	No
No	Yes	No	Yes	Yes	Yes
No	No	No	Yes	No	No
Yes	Yes	No	No	No	No
Yes	No	Yes	Yes	No	No
No	Yes	Yes	No	No	Yes
No	No	Yes	No	No	No
Yes	Yes	No	Yes	Yes	Yes
Yes	No	No	No	No	No
No	Yes	Yes	Yes	Yes	Yes
No	No	Yes	Yes	No	No
Yes	Yes	Yes	No	No	No
Yes	No	No	Yes	Yes	No
No	Yes	No	No	No	No

- If autonegotiation is disabled, the configured flow control settings are applied to the local interface.
- Enter a slot number to configure how flow control PAUSE frames are processed for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to configure how flow control PAUSE frames are processed on a specific interface or range of interfaces.

Examples

```
-> interfaces 3/1 pause tx
-> interfaces 4/2 pause rx
-> interfaces 1 tx-and-rx
-> interfaces 3/1-6 pause tx
-> interfaces 3/1-6 disable
```

Release History

Release 6.3.2; command was introduced.

Related Commands

interfaces hybrid pause	Configures flow control settings for combo ports.
interfaces e2e-flow-vlan	Configures a dedicated VLAN for carrying end-to-end (E2E) flow control messages to remote systems.
show interfaces pause	Displays interface flow control settings.

MIB Objects

```
esmConfigTable
   esmPortCfgFlow
dot3PauseTable
   dot3PauseAdminMode
```

interfaces e2e-flow-vlan

Configures a dedicated VLAN for carrying end-to-end (E2E) flow control messages to remote systems. Creating this type of VLAN is required to enable E2E flow control on 48-port models.

interfaces e2e-flow-vlan *vlan_id*

interfaces no e2e-flow-vlan

Syntax Definitions

vlan_id	The VLAN ID number for the dedicated flow VLAN.

Platforms Supported

OmniSwitch 6400, 6850E

Defaults

N/A

Usage Guidelines

- Note that if the standalone switch is a 24-port unit, then only the **interfaces pause** command is required to enable end-to-end (E2E) flow control. However, if the switch is a 48-port unit, then a flow control VLAN, which is configured using the **interfaces e2e-flow-vlan** command, is required in addition to enabling RX/TX pause flow control.
- Use the **no** form of this command to remove the flow VLAN from the switch configuration.
- There is only one flow control VLAN allowed per switch.
- No other standard VLAN management commands are allowed once a VLAN is configured as a dedicated flow control VLAN.

Examples

```
-> interfaces e2e-flow-vlan 10
-> interfaces no e2e-flow-vlan
```

Release History

Release 6.3.4; command was introduced.

Related Commands

show interfaces e2e-flow-vlan	Displays the E2E flow control VLAN configuration.
interfaces pause	Configures whether or not the switch will transmit, honor, or transmit and honor flow control PAUSE frames.
show interfaces pause	Displays interface flow control settings.

MIB Objects

```
esmE2EFlowVlan
```

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 {*slot* | *slot*/*port***[-***port2***]} duplex {full | half | auto}**

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
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	**full**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Half duplex mode is not supported on Gigabit modules if a port is detected as Gigabit (1000 Mbps).
- On OS9-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.
- Gigabit and 10 Gigabit fiber ports only support full duplex.
- Enter a slot number to configure the duplex mode for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to configure the duplex mode for a specific interface or range of interfaces.

Examples

```
-> interfaces 3/1 duplex auto
-> interfaces 3 duplex half
-> interfaces 3/1-4 auto
```

Release History

Release 6.1; 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 (for example, speed, and mode).

MIB Objects

```
esmConfTable
   esmPortAutoDuplexMode
```

interfaces admin

Administratively enables or disables interfaces.

interfaces {*slot* | *slot*/*port***[-***port2***]} admin {up | down}**

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
up	Enables the interface.
down	Disables the interface.

Defaults

parameter	default
up | **down**	up

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Enter a slot number to administratively enable or disable all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to administratively enable or disable a specific interface or range of interfaces.
- The port link status changes based on the **admin** status.

Examples

```
-> interfaces 3/1 admin up
-> interfaces 3 admin down
-> interfaces 3/1-4 admin up
```

Release History

Release 6.1; command was introduced.

Related Commands

show interfaces	Displays general interface information (for example, hardware, MAC address, input errors, and output errors).
show interfaces port	Displays the administrative, operational, violation, and recovery status and configuration for the specified port.

MIB Objects

```
ifTable
   ifAdminStatus
```

interfaces cli-prompt

Enables or disables the display of a confirmation prompt when an interface is administratively disabled using the **interfaces admin {up | down}** command**.**

interfaces cli-prompt {enable | disable}

Syntax Definitions

enable	Enables the display of a confirmation prompt when an interface is administratively disabled.
disable	Disables the display of a confirmation prompt when an interface is administratively disabled.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- This command is used in conjunction with the **interfaces admin** command to enable or disable the confirmation prompt.
- By default, the warning prompt will not be displayed.
- If the interface is already operationally down, the warning prompt will not be displayed.
- If a range of interfaces or slots is provided in the interfaces admin down command and the display of confirmation prompt is enabled, then the prompt will be displayed irrespective of the operational status of the interface.
- The configuration of this command can be captured in the snapshot when the display of the warning prompt is enabled.
- The configuration of this command cannot be captured in any interface show commands.

Examples

```
-> interfaces cli-prompt enable
-> interfaces 1/1 admin down
-> Confirm Command (Y/N) :

-> interfaces cli-prompt disable
-> interfaces 1/1 admin down
```

Release History

Release 6.3.4; the command was introduced.

Related Commands

interfaces admin	Administratively enables or disables interfaces.

MIB Objects

N/A

interfaces alias

Configures a description (alias) for a single port.

interfaces *slot/port* **alias** *description*

Syntax Definitions

slot/port	The slot and port number (3/1).
description	A description for the port, which can be up to 40 characters long. Spaces must be contained within quotes (for example, “IP Phone”).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- To remove an alias use a description consisting of two quotes without any spaces (for example, "").
- On combo ports the configuration changes made with the **interfaces alias** command apply to both the fiber and to the copper port. You cannot configure separate aliases.

Examples

```
-> interfaces 3/1 alias switch_port
-> interfaces 2/2 alias "IP Phone"
-> interfaces 3/1 alias ""
```

Release History

Release 6.1; command was introduced.

Related Commands

show interfaces	Displays general interface information (for example, hardware, MAC address, input errors, and output errors).
show interfaces port	Displays the administrative, operational, violation, and recovery status and configuration for the specified port.

MIB Objects

```
ifXTable
   ifAlias
```

interfaces ifg

Configures the inter-frame gap on Gigabit Ethernet interfaces.

interfaces {*slot* | *slot*/*port***[-***port2***]} ifg** *bytes*

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
bytes	Inter-frame gap value, in bytes. Valid range is 9–12.

Defaults

parameter	default
bytes	12

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Enter a slot number to configure the inter-frame gap value for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to configure the inter-frame gap value for a specific interface or range of interfaces.

Examples

```
-> interfaces 3/1 ifg 10
-> interfaces 3 ifg 10
-> interfaces 3/1-4 ifg 10
```

Release History

Release 6.1; 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 {*slot* | *slot*/*port***[-***port2***]} no l2 statistics [cli]**

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
cli	Clears the counters from the CLI only; SNMP statistics continue to maintain cumulative totals.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- This command requires an upper or lower case “L” character in front of the “2” character. Entering the digit “1” (one) will result in an error message.
- When the **cli** parameter is not specified, both CLI and SNMP statistics are cleared.
- Enter a slot number to reset the statistics counters for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to reset the statistics counters for a specific interface or range of interfaces.

Examples

```
-> interfaces 3/1 no l2 statistics
-> interfaces 3 no l2 statistics
-> interfaces 3/1-6 no l2 statistics
```

Release History

Release 6.1; command was introduced.
Release 6.3.1; **cli** parameter was added.

Related Commands

show interfaces	Displays general interface information, including when statistics were last cleared.
show interfaces accounting	Displays interface accounting information (for example, packets received/transmitted and deferred frames received).
show interfaces counters	Displays interface counters information (for example, unicast, broadcast, and multi-cast packets received/transmitted).
show interfaces counters errors	Displays interface error frame information (for example, CRC errors, transit errors, and receive errors).
show interfaces collisions	Displays interface collision information (for example, number of collisions and number of retries).

MIB Objects

```
alcetherStatsTable
   alcetherClearStats
```

interfaces max frame

Configures the maximum frame size for Gigabit Ethernet interfaces.

interfaces {*slot* | *slot*/*port***[-***port2***]} max frame** *bytes*

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
bytes	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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Enter a slot number to configure the maximum frame size for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to configure the maximum frame size on a specific interface or range of interfaces.

Examples

```
-> interfaces 3/1 max frame 1518
-> interfaces 3 max frame 1518
-> interfaces 3/1-3 max frame 1518
```

Release History

Release 6.1; command was introduced.

Related Commands

show interfaces	Displays general interface information (for example, hardware, MAC address, input errors, and output errors).

MIB Objects

```
esmConfTable
   esmPortCfgMaxFrameSize
```

interfaces flood

Enables broadcast, multicast or unknown unicast traffic storm control on the specified interface.

interfaces {*slot* **|** *slot*/*port***[-***port2***]} flood [broadcast | multicast | unknown-unicast | all] [enable | disable]**

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
broadcast	Packets with a destination MAC address of FF:FF:FF:FF:FF:FF.
multicast	Packets with a multicast MAC address.
unknown-unicast	Unicast packets with an unknown destination MAC address.
all	Applies to broadcast, multicast, and unknown unicast packets.
enable	Enables broadcast, multicast, or unknown unicast rate limiting.
disable	Disables broadcast, multicast, or unknown unicast rate limiting.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Enter a slot number to enable or disable traffic storm control for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to enable or disable traffic storm control on a specific interface or range of interfaces.
- The keyword **all** applies to all traffic types; broadcast, multicast and unknown-unicast.

Examples

```
-> interfaces 3 flood broadcast enable
-> interfaces 1/47 flood broadcast enable
-> interfaces 3 flood multicast enable
-> interfaces 1/45-48 flood multicast enable
-> interfaces 3 flood unknown-unicast enable
-> interfaces 1/47 flood unknown-unicast enable
```

```
-> interfaces 3 flood all enable
-> interfaces 1/47 flood all enable
-> interfaces 1/45-48 flood all enable
```

Release History

Release 6.4.3; command was introduced.

Related Commands

show interfaces flood rate	Displays interface peak flood rate settings.
interfaces flood rate	Configures the peak flood rate for an interface.

MIB Objects

```
esmConfTable
   esmPortMaxFloodRate
   esmPortMaxMcastFloodRate
   esmPortMaxUnknownUcastFloodRate
   esmPortFloodMcastEnable
   esmPortFloodBcastEnable
   esmPortFloodUnknownUcastEnable
   esmPortMaxFloodRateLimit
   esmPortMaxUnknownUcastFloodRateLimit
   esmPortMaxMcastFloodRateLimit
```

interfaces flood rate

Configures flood rate limiting for broadcast, multicast, or unknown unicast traffic on the specified interface.

interfaces {*slot* | *slot/port***[-***port2***]} flood {broadcast | multicast | unknown-unicast | all} rate {mbps** *mbps* **| pps** *pps* **| percentage** *percent* | **default} [low-threshold** *num***]**

Syntax Definitions

slot	The slot number for a specific module.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
mbps	The number of megabits per second.
pps	The number of packets per second.
percent	The percentage of the port speed.
default	Default speed of the port.
num	The low threshold value. The low threshold value must be lesser than the high threshold (rate limiting) value.

Defaults

- The default flood limit settings:

port speed	flood limit
10 mbps	**4 mbps**
100 mbps	**49 mbps**
1 Gig	**496 mbps**
10 Gig	**997 mbps**

- The default value for low threshold is ‘0’. This means, by default, auto recovery is not enabled.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- By default, unknown unicast and multicast traffic is flooded to all Layer 2 ports in a VLAN.
- Enter a slot number to configure flood rate limiting for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to configure flood rate limiting on a specific interface or range of interfaces.
- The keyword **all** applies to all traffic types, broadcast, multicast and unknown-unicast.

- The CLI command '**interfaces** *slot***[**/*port***[**-*port2***]] flood rate** *num***'** is supported only during boot up process for backward compatibility.
- The high (rate limit value) and low threshold (if) configured will have same threshold type [Mbps or PPS or percentage].
- Low threshold cannot be configured for unknown unicast traffic.
- The violated port is displayed as "Storm" violation in the "show interface port" command.
- The violated port can be recovered by any of the following ways when low threshold is not configured on the port:
  - Use 'interface slot/port admin down', then 'interface slot/port admin up' command on the port.
  - Unplug and replug the cable.
  - Use 'interface slot/port clear-violation-all' command to clear all the violation on the port.
- The global interface violation recovery timer is not applicable for storm threshold violation.

Examples

```
-> interfaces 1/1-5 flood all rate mbps 10
-> interfaces 1/1 flood broadcast rate pps 500
-> interfaces 1/2 flood multicast rate percentage 35
-> interfaces 1/3 flood unknown-unicast rate mbps 5
-> interfaces 1/2 flood multicast rate percentage 35 low-threshold 30
```

Release History

Release 6.1; command was introduced.
Release 6.4.3; **broadcast**, **multicast**, **unknown-unicast**, and **all** parameters added.
Release 6.4.5; **low-threshold** parameter added.

Related Commands

show interfaces flood rate	Displays interface peak flood rate settings.
interfaces flood	Enables traffic storm control on the specified interface.
interfaces flood action	Configures the storm control action when the port reaches the storm violated state.

MIB Objects

```
esmConfTable
   esmPortMaxFloodRate
   esmPortMaxMcastFloodRate
   esmPortMaxUnknownUcastFloodRate
   esmPortFloodMcastEnable
   esmPortFloodBcastEnable
   esmPortFloodUnknownUcastEnable
   esmPortMaxFloodRateLimit
   esmPortMaxUnknownUcastFloodRateLimit
   esmPortMaxMcastFloodRateLimit
```

interfaces flood action

Configures the storm control action when the port reaches the storm violated state.

interfaces {*slot* | *slot/port***[-***port2***]} flood [broadcast | multicast] action [shutdown | trap | default]**

Syntax Definitions

slot	The slot number for a specific module.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
broadcast	Packets with a destination MAC address of FF:FF:FF:FF:FF:FF.
multicast	Packets with a multicast MAC address.
shutdown	When the ingress storm traffic exceeds high threshold value, the port moves to violated state (Storm Violation) and a violation trap is generated. The port state moves to operationally down and admin enable**.** When the ingress traffic reaches the low threshold or goes below the low threshold, the port state moves to normal state, and a trap is generated.
trap	When the ingress storm traffic exceeds high threshold value, the port controls the storm by rate limiting the traffic, and a violation trap is generated. The port remains in the normal state. When the ingress traffic reaches the low threshold, a trap is generated.
default	When the ingress storm traffic exceeds high threshold value, the port controls the storm by rate limiting the traffic. No trap is generated, and the port remains in the normal state.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

For more information on the action performed based on the configured high and low threshold value, refer to “Configuring Ethernet Ports” chapter in *OmniSwitch AOS Release 6 Network Configuration Guide*.

Examples

```
-> interfaces 1/1 flood broadcast action shutdown
-> interfaces 1/1 flood broadcast action trap
-> interfaces 1/1 flood broadcast action default
```

Release History

Release 6.4.5; command introduced.

Related Commands

show interfaces flood rate	Displays interface peak flood rate settings.
interfaces flood rate	Configures flood rate limiting for broadcast, multicast, or unknown unicast traffic on the specified interface.

MIB Objects

```
esmPortFloodThresholdAction
```

interfaces violation-recovery-time

Configures the time interval after which the port is automatically re-activated if the port was shutdown for any violation. This value is configurable on a global basis (applies to all ports on all modules) and on a per-slot or per-port basis.

interfaces [*slot* | *slot*/*port***[-***port2***]] violation-recovery-time {***seconds* | **default}**

interfaces {*slot* | *slot*/*port***[-***port2***]} violation-recovery-time default**

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
seconds	The number of seconds after which a port is reactivated. The valid range is 30-600 seconds or specify 0 to disable the recovery timer.
default	Sets the recovery time to the global value for the specified ports. This parameter is only available when a slot, port, or range of ports is specified with this command.

Defaults

- By default, this command configures the global recovery time. The global value applies to all ports on all modules in the switch.
- By default, the violation recovery time is set to 300 seconds.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- When the recovery timer expires, the interface is operationally re-enabled and the violation on the interface is cleared.
- The violation recovery time value does not apply to interfaces that are in a permanent shutdown state. A port in this state is only recoverable using the **interfaces clear-violation-all** command.
- The interface violation recovery mechanism is not supported on link aggregates, but is supported on the link aggregate member ports.
- Set the recovery time to 0 to disable this violation recovery mechanism.
- Enter a slot number to configure the recovery time for all interfaces on a specific slot.
- Enter a slot and port number or a range of ports to configure the recovery time for a specific interface or a range of interfaces.
- When this command is used to configure the recovery time for all ports on a slot or for a specific port or range of ports, the value specified overrides the global maximum recovery time configured for the switch.

- When configuring the time for a specific slot, port, or range of ports, use the **default** parameter to reset this value to the global maximum number of attempts.

Examples

```
-> interfaces violation-recovery-time 600
-> interfaces 2 violation-recovery-time 100
-> interfaces 2/3 violation-recovery-time 200
-> interfaces 2/4-9 violation-recovery-time 500
-> interfaces 2/4-9 violation-recovery-maximum default
-> interfaces 2/3 violation-recovery-time 0
-> interfaces violation-recovery-time 0
```

Release History

Release 6.4.4; command introduced.

Related Commands

interfaces violation-recovery-maximum	Configures the maximum number of recovery attempts before a port is permanently shut down.
show interfaces port	Displays the administrative, operational, violation, and recovery status and configuration for the specified port.
show interfaces violation-recovery	Displays the globally configured recovery time, SNMP recovery trap enable/disable status and maximum recovery attempts.

MIB Objects

```
alaPortViolationRecoveryTable
   alaPortViolationRecoveryTime
```

interfaces violation-recovery-maximum

Configures the maximum number of recovery attempts allowed before the port is permanently shut down. This value is configurable on a global basis (applies to all ports on all modules) and on a per-slot or per-port basis.

interfaces [*slot* | *slot*/*port***[-***port2***]] violation-recovery-maximum** *max_attempts*

interfaces {*slot* | *slot*/*port***[-***port2***]} violation-recovery-maximum default**

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
max_attempts	The maximum number of recovery attempts. Valid range is 0-50.
default	Sets the number of recovery attempts to the global value for the specified ports. This parameter is only available when a slot, port, or range of ports is specified with this command.

Defaults

By default, this command configures the global maximum number of recovery attempts. The global value applies to all ports on all modules in the switch.

parameter	default
max_attempts	10

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Set the maximum number of recovery attempts value to 0 to disable this recovery mechanism.
- Enter a slot number to configure the number of recovery attempts for all interfaces on a specific slot.
- Enter a slot and port number or a range of ports to configure the number of recovery attempts for a specific interface or a range of interfaces.
- When this command is used to configure the number of recovery attempts for all ports on a slot or for a specific port or range of ports, the value specified overrides the global maximum number of attempts configured for the switch.
- When configuring the number of recovery attempts for a specific slot, port, or range of ports, use the **default** parameter to reset this value to the global maximum number of attempts.
- The number of recovery attempts increments whenever a port recovers using automatic recovery timer mechanism. When the number of recovery attempts exceeds the configured threshold, the port is permanently shut down.

- Once an interface is permanently shut down, only the **interface clear-violations-all** command can be used to recover the interface.
- The recovery mechanism tracks the number of recoveries within a fixed time window (FTW). The FTW = 2 * maximum recovery number * recovery timer. For example, if the maximum number of recovery attempts is set to 4 and the recovery timer is set to 5, the FTW is 40 seconds (2 * 4 * 5=40).

Examples

```
-> interfaces violation-recovery-maximum 25
-> interfaces 2 violation-recovery-maximum 10
-> interfaces 2/3 violation-recovery-maximum 20
-> interfaces 2/4-9 violation-recovery-maximum 50
-> interfaces 2/4-9 violation-recovery-maximum default
-> interfaces 2/3 violation-recovery-maximum 0
-> interfaces violation-recovery-maximum 0
```

Release History

Release 6.4.4; command was introduced.

Related Commands

interfaces violation-recovery-time	Configures the time interval after which the port is automatically re-activated if the port was shut down for any violation.
show interfaces port	Displays the administrative, operational, violation, and recovery status and configuration for the specified port.
show interfaces violation-recovery	Displays the globally configured recovery time, SNMP recovery trap status, and maximum recovery attempts.

MIB Objects

```
alaPortViolationRecoveryTable
   alaPortViolationRecoveryMaximum
```

interfaces violation-recovery-trap

Enables or disables the sending of a violation recovery trap when any port is re-enabled after the violation recovery time has expired.

interface violation-recovery-trap {enable | disable}

Syntax Definitions

enable	Enables the ports to send violation recovery traps.
disable	Disables the ports from sending violation recovery traps.

Defaults

By default, the sending of a violation recovery trap is disabled.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

This is a global command that is applied to all ports on all modules.

Examples

```
-> interfaces violation-recovery-trap enable
-> interfaces violation-recovery-trap disable
```

Release History

Release 6.4.3; command was introduced.

Related Commands

interfaces violation-recovery-time	Configures the time interval to automatically re-enable the ports that were shutdown due to a violation.
show interfaces violation-recovery	Displays the globally configured recovery time, SNMP recovery trap status, and maximum recovery attempts.

MIB Objects

```
esmViolationRecovery
   esmViolationRecoveryTrap
```

interfaces clear-violation-all

Clears all port violations set by various applications on the switch for the given port.

interfaces {*slot* | *slot/port***[-***port2***]} clear-violation-all**

Syntax Definitions

slot	The slot number for a specific module.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

All application violations associated with a specific port are cleared when this command is used.

Examples

```
-> interfaces 1/3 clear-violation-all
-> interfaces 1 clear-violation-all
-> interfaces 1/3-7 clear-violation-all
```

Release History

Release 6.3.1; command was introduced.

Related Commands

show interfaces port	Displays the administrative, operational, violation, and recovery status and configuration for the specified port.

MIB Objects

```
esmConfTable
   esmPortViolationClearAll
```

interfaces wait-to-restore

Configures the wait to restore timer on a specific slot, port, or a range of specified ports. The timer is enabled when a link up event is detected. Other applications are notified of the link up event only after the wait to restore timer has elapsed.

interfaces {*slot* | *slot/port***[-***port2***]} wait-to-restore** *seconds*

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
seconds	The number of seconds the switch waits before notifying other applications. The valid range is 0-300 in multiples of 5.

Defaults

By default, the timer is set to zero (disabled).

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Set the wait-to-restore timer to zero to disable the timer.
- Enter a slot number to configure the timer value for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to configure the timer value for a specific interface or a range of interfaces.

Example

```
-> interfaces 1 wait-to-restore 30
-> interfaces 1/1 wait-to-restore 10
-> interfaces 1/1-7 wait-to-restore 250
```

Release History

Release 6.4.4; command introduced.

Related Commands

show interfaces port	Displays the administrative, operational, violation, and recovery status and configuration for the specified port.

MIB Objects

```
esmConfTable
   esmPortWaitToRestoreTimer
```

interfaces transceiver ddm

Configures the DDM administrative status or trap capability.

interfaces transceiver ddm [trap] {enable | disable}

Syntax Definitions

trap	Indicates the enable / disable parameter applies to the traps functionality.
enable	Enables DDM functionality or traps warning/alarm threshold violations.
disable	Disables DDM functionality or traps warning/alarm threshold violations.

Defaults

parameter	default
ddm	**disable**
trap	**disable**

By default, the polling period is set 1 second for the OS6400/6855.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- DDM capability will vary based on the transceiver manufacturer.
- DDM status must be enabled in order to enable traps; traps are enabled separately.
- Information will be read sequentially from a different SFP at the predefined Polling intervals listed in the defaults table above. The number of SFPs in the switch will determine how often each SFP is polled.

Examples

```
-> interfaces transceiver ddm enable
-> interfaces transceiver ddm trap enable
-> interfaces transceiver ddm trap disable
-> interfaces transceiver ddm disable
```

Release History

Release 6.4.2; command was introduced.

Related Commands

show interfaces transceiver	Displays the interface DDM status.

MIB Objects

```
ddmConfiguration
   ddmConfig
   ddmTrapConfig
   ddmNotificationType
```

interfaces link-monitoring admin-status

Enables or disables link monitoring on a specific slot, port, or a range of specified ports.

interfaces {*slot* | *slot/port***[-***port2***]} link-monitoring admin-status {enable | disable}**

Syntax Definitions

slot	The slot number for a specific module.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
enable	Enables link monitoring for the specified port.
disable	Disables link monitoring for the specified port.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Configuring link monitoring parameters are allowed even if the link monitoring status is disabled for the specified ports.
- The Automatic Recovery Timer and link monitoring must not be enabled on Remote Fault Propagation (RFP) enabled ports.
- Enter a slot number to configure link monitoring for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to configure link monitoring for a specific interface or range of interfaces.

Example

```
-> interfaces 1 link-monitoring admin-status enable
-> interfaces 1/1 link-monitoring admin-status enable
-> interfaces 1/1-7 link-monitoring admin-status enable
-> interfaces 2/5 link-monitoring admin-status disable
-> interfaces 2/5-20 link-monitoring admin-status disable
```

Release History

Release 6.4.4; command introduced.

Related Commands

show interfaces port	Displays the administrative, operational, violation, and recovery status and configuration for the specified port.
show interfaces link-monitoring config	Displays the link monitoring configuration for the specified ports.
show interfaces link-monitoring statistics	Displays the link monitoring statistics for the specified ports.

MIB Objects

```
alaLinkMonConfigTable
   alaLinkMonStatus
```

interfaces link-monitoring time-window

Configures the monitoring time window on a specific slot, port, or a range of specified ports. This is the length of time during which the link is monitored.

interfaces {*slot* | *slot/port***[-***port2***]} link-monitoring time-window** *seconds*

Syntax Definitions

slot	The slot number for a specific module.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
seconds	The length of time during which the link is monitored. The valid range is 0–3600 seconds.

Defaults

By default, the time window value is set to 300 seconds.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Enter a slot number to configure the monitoring time window for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to configure the monitoring time window for a specific interface or a range of interfaces.

Example

```
-> interfaces 1 link-monitoring time-window 20
-> interfaces 1/1 link-monitoring time-window 40
-> interfaces 1/1-7 link-monitoring time-window 2500
```

Release History

Release 6.4.4; command introduced.

Related Commands

show interfaces port	Displays the administrative, operational, violation, and recovery status and configuration for the specified port.
show interfaces link-monitoring config	Displays the link monitoring configuration for the specified ports.
show interfaces link-monitoring statistics	Displays the link monitoring statistics for the specified ports.

MIB Objects

```
alaLinkMonConfigTable
   alaLinkMonTimeWindow
```

interfaces link-monitoring link-flap-threshold

Configures the number of link flaps allowed on a specific slot, port, or a range of specified ports in the time interval, before the port is shutdown.

interfaces {*slot* | *slot/port***[-***port2***]} link-monitoring link-flap-threshold** *link_flaps*

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
link_flaps	The number of link flaps. The valid range is 2-10.

Defaults

By default, the number of link flaps allowed is set to 5.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Enter a slot number to configure the number of link flaps allowed for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to configure the number of link flaps allowed for a specific interface or a range of interfaces.

Example

```
-> interfaces 1 link-monitoring link-flap-threshold 6
-> interfaces 1/1 link-monitoring link-flap-threshold 3
-> interfaces 1/1-7 link-monitoring link-flap-threshold 10
```

Release History

Release 6.4.4; command introduced.

Related Commands

show interfaces port	Displays the administrative, operational, violation, and recovery status and configuration for the specified port.
show interfaces link-monitoring config	Displays the link monitoring configuration for the specified ports.
show interfaces link-monitoring statistics	Displays the link monitoring statistics for the specified ports.

MIB Objects

```
alaLinkMonConfigTable
   alaLinkMonLinkFlapThreshold
```

interfaces link-monitoring link-error-threshold

Configures the number of MAC errors allowed on a specific slot, port, or a range of specified ports in the time interval, before the port is shutdown. MAC errors refer to lost frames, error frames, alignment frames and cyclic redundancy check (CRC).

interfaces {*slot* | *slot/port***[-***port2***]} link-monitoring link-error-threshold** *mac_errors*

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
mac_errors	The number of MAC errors. The valid range is 1-100.

Defaults

By default, the number of MAC errors allowed is set to 5.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Enter a slot number to configure the number of MAC errors allowed on all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to configure the number of MAC errors allowed on a specific interface or on a range of interfaces.

Example

```
-> interfaces 1 link-monitoring link-error-threshold 30
-> interfaces 1/1 link-monitoring link-error-threshold 10
-> interfaces 1/1-7 link-monitoring link-error-threshold 35
```

Release History

Release 6.4.4; command introduced.

Related Commands

show interfaces port	Displays the administrative, operational, violation, and recovery status and configuration for the specified port.
show interfaces link-monitoring config	Displays the link monitoring configuration for the specified ports.
show interfaces link-monitoring statistics	Displays the link monitoring statistics for the specified ports.

MIB Objects

```
alaLinkMonConfigTable
   alaLinkMonLinkErrorThreshold
```

interfaces clear-link-monitoring-stats

Clears the link monitoring statistics on a specific slot, port, or a range of specified ports.

interfaces {*slot* | *slot/port***[-***port2***]} clear-link-monitoring-stats**

Syntax Definitions

slot	The slot number for a specific module.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Enter a slot number to clear monitoring statistics for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to clear monitoring statistics for a specific interface or a range of interfaces.

Example

```
-> interfaces 1 clear-link-monitoring-stats
-> interfaces 1/1 clear-link-monitoring-stats
-> interfaces 1/1-7 clear-link-monitoring-stats
```

Release History

Release 6.4.4; command introduced.

Related Commands

show interfaces port	Displays the administrative, operational, violation, and recovery status and configuration for the specified port.
show interfaces link-monitoring config	Displays the link monitoring configuration for the specified ports.
show interfaces link-monitoring statistics	Displays the link monitoring statistics for the specified ports.

MIB Objects

```
alaLinkMonStatsTable
   alaLinkMonStatsClearStats
```

interfaces hybrid preferred-fiber

Configures one or more combo ports to use the fiber SFP port(s) instead of the equivalent copper 10/100/1000 RJ-45 port(s), when both ports are enabled and have a valid link. In addition, this mode configures automatic failover to copper if a valid copper link is present on RJ-45 side and fiber link fails to come up.

interfaces {*slot* | *slot/port***[-***port2***]} hybrid preferred-fiber**

Syntax Definitions

slot	The slot number for a specific module.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).

Defaults

All combo ports are set to preferred-fiber by default.

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

This command is no longer required, preferred-fiber is the only mode supported.

Examples

```
-> interfaces 1/47 hybrid preferred-fiber
-> interfaces 1/47-48 hybrid preferred-fiber
-> interfaces 1 hybrid preferred-fiber
```

Release History

Release 6.1; command was introduced.
Release 6.4.4; preferred-fiber parameter introduced.

Related Commands

show interfaces hybrid status	Displays interface line settings (for example, speed, mode) for combo ports only.

MIB Objects

```
esmHybridConfTable
   esmPortCfgHybridMode
   esmPortCfgHybridType
```

interfaces hybrid autoneg

Enables or disables auto-negotiation on a single combo port, a range of combo ports, or all combo ports on a switch.

interfaces {*slot* | *slot/port***[-***port2***]} hybrid {fiber | copper} autoneg {enable | disable | on | off}**

Syntax Definitions

slot	The slot number for a specific module.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
fiber	Specifies that configuration changes will be made to the SFP port(s).
copper	Specifies that changes will be made to the copper 10/100/1000 RJ-45 port(s).
enable	Enables auto negotiation.
disable	Disables auto negotiation.
on	Same as enable.
off	Same as disable.

Defaults

By default, auto-negotiation is enabled for the interface.

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- Refer to the *Hardware Users Guide* for combo port numbering.
- The MIB table and MIB object listed in the “MIB Objects” section below apply to the inactive configured media only. See the “MIB Objects” section in the **interfaces autoneg** section for the MIB table and MIB object for the active configured media.
- Enter a slot number to configure auto-negotiation for all interfaces on a specific slot.
- Enter a slot and port number or a range of ports to configure auto-negotiation for a specific interface on a specific slot.

Examples

```
-> interfaces 1/47 hybrid copper autoneg disable
-> interfaces 1/47-48 hybrid copper autoneg disable
-> interfaces 1 hybrid copper autoneg disable
```

Release History

Release 6.1; command was introduced.

Related Commands

interfaces hybrid speed	Configures interface speed for combo ports.
interfaces hybrid crossover	Configures crossover port settings for combo ports.
interfaces hybrid speed	Enables or disables flow (pause).
show interfaces hybrid status	Displays interface line settings for combo ports.
show interfaces hybrid capability	Displays auto negotiation, speed, duplex, and crossover settings for combo ports.

MIB Objects

```
esmHybridConfTable
   esmHybridPortCfgAutoNegotiation
```

interfaces hybrid crossover

Configures port crossover settings on a single port, a range of ports, or an entire Network Interface (NI).

interfaces {*slot* | *slot/port***[-***port2***]} hybrid copper crossover {auto | mdix | mdi}**

Syntax Definitions

slot	The slot number for a specific module.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
copper	Specifies that changes will be made to the copper 10/100/1000 RJ-45 port(s).
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.

Defaults

By default, the interface is configured to automatically detect crossover settings.

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- Refer to the *Hardware Users Guide* for combo port numbering.
- You cannot configure crossover settings on fiber ports. These ports use the MDI standard.
- The MIB table and MIB object listed in the “MIB Objects” section below apply to the inactive configured media only.
- Enter a slot number to configure the crossover settings for all interfaces on a specific slot.
- Enter a slot and port number or a range of ports to configure the crossover settings for a specific interface or a range of interfaces.

Examples

```
-> interfaces 1/47 hybrid copper crossover disable
-> interfaces 1/47-48 hybrid copper crossover mdix
```

Release History

Release 6.1; command was introduced.

Related Commands

interfaces hybrid speed	Configures interface speed for combo ports.
interfaces hybrid autoneg	Enables and disables auto negotiation for combo ports.
interfaces hybrid speed	Enables or disables flow (pause) for combo ports.
show interfaces hybrid status	Displays interface line settings for combo ports.
show interfaces hybrid capability	Displays auto negotiation, speed, duplex, and crossover settings for combo ports.

MIB Objects

```
esmHybridConfTable
   esmHybridPortCfgCrossover
```

interfaces hybrid duplex

Configures duplex mode on combo ports. 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 {*slot* | *slot/port***[-***port2***]} hybrid {fiber | copper} duplex {full | half | auto}**

Syntax Definitions

slot	The slot number for a specific module.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
fiber	Specifies that configuration changes will be made to the SFP port(s).
copper	Specifies that changes will be made to the copper 10/100/1000 RJ-45 port(s).
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

By default, the duplex mode is set to full for the interface.

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- Refer to the *Hardware Users Guide* for combo port numbering.
- The MIB table and MIB object listed in the “MIB Objects” section below apply to the inactive configured media only. See the “MIB Objects” section in the **interfaces duplex** section for the MIB table and MIB object for the active configured media.
- Enter a slot number to configure the duplex mode for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to configure the duplex mode for a specific interface or a range of interfaces.

Examples

```
-> interfaces 1/47 hybrid copper duplex auto
-> interfaces 1/47-48hybrid copper duplex half
-> interfaces 1 hybrid copper fiber full
```

Release History

Release 6.1; command was introduced.

Related Commands

interfaces hybrid speed	Configures interface line speed for combo ports. Set to **auto** to set speed and duplex mode to auto-sensing.
show interfaces hybrid status	Displays interface line settings (for example, speed, mode) for combo ports.

MIB Objects

```
esmHybridConfTable
   esmHybridPortCfgDuplexMode
```

interfaces hybrid speed

Configures interface line speed on combo ports.

interfaces {*slot* | *slot/port***[-***port2***]} hybrid {fiber | copper} speed {auto | 10 | 100 | 1000 | 10000 | max {100 | 1000}}**

Syntax Definitions

slot	The slot number for a specific module.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
fiber	Specifies that configuration changes will be made to the SFP port(s).
copper	Specifies that changes will be made to the copper 10/100/1000 RJ-45 port(s).
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. This option is currently not supported.
max 100	Sets the maximum speed to 100 megabits.
max 1000	Sets the maximum speed to 1000 megabits (1 Gigabit)

Defaults

By default, the line speed is automatically set to match the speed of the attached device.

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- Refer to the *Hardware Users Guide* for combo port numbering.
- The MIB table and MIB object listed in the “MIB Objects” section below apply to the inactive configured media only. See the “MIB Objects” section in the **interfaces speed** section for the MIB table and MIB object for the active configured media.
- Enter a slot number to configure the line speed for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to configure the line speed for a specific interface or a range of interfaces.

Examples

```
-> interfaces 1/47 hybrid copper speed auto
-> interfaces 1/47-48 hybrid copper speed 100
-> interfaces 1/47 hybrid fiber speed 1000
```

Release History

Release 6.1; command was introduced.

Related Commands

interfaces hybrid duplex	Configures duplex mode for combo ports.
interfaces hybrid autoneg	Enables and disables auto negotiation for combo ports.
show interfaces hybrid status	Displays interface line settings for combo ports.

MIB Objects

```
esmHybridConfTable
   esmHybridPortCfgSpeed
```

interfaces hybrid pause

Configures whether or not the switch will transmit, honor, or transmit and accept flow control PAUSE frames on the specified combo port. PAUSE frames are used to temporarily pause the flow of traffic between two connected devices to help prevent packet loss when traffic congestion occurs between switches.

interfaces {*slot* | *slot/port***[-***port2***]} hybrid {fiber | copper} pause {tx | rx | tx-and-rx | disable}**

Syntax Definitions

slot	The slot number for a specific module.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
fiber	Specifies that configuration changes will be made to the SFP port(s).
copper	Specifies that changes will be made to the copper 10/100/1000 RJ-45 port(s).
tx	Transmits PAUSE frames to peer switches when traffic congestion occurs on the local interface. Does not honor PAUSE frames from peer switches.
rx	Allows interface to honor PAUSE frames from peer switches and temporarily stop sending traffic to the peer. Does not transmit PAUSE frames to peer switches.
tx-and-rx	Transmits and honors PAUSE frames when traffic congestion occurs between peer switches.
disable	Disables flow control on the interface.

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Defaults

By default, flow control is disabled on all combo ports.

Usage Guidelines

- Note that if the standalone switch is a 24-port unit, then only the **interfaces pause** command is required to enable end-to-end (E2E) flow control. However, if the switch is a 48-port unit, then a flow control VLAN, which is configured using the **interfaces e2e-flow-vlan** command, is required in addition to enabling RX/TX pause flow control.
- Flow control is only supported on interfaces configured to run in full-duplex mode; half-duplex mode is not supported.

- If both autonegotiation and flow control are enabled on the same local interface, autonegotiation calculates operational flow control settings for that interface. Note that the operational settings, as shown in the following table, override the configured settings as long as autonegotiation and flow control are both enabled for the interface.

Configured Local Tx	Configured Local Rx	Configured Remote Tx	Configured Remote Rx	Negotiated Local Tx	Negotiated Local Rx
No	No	No	No	No	No
Yes	Yes	Yes	Yes	Yes	Yes
Yes	No	Yes	No	No	No
No	Yes	No	Yes	Yes	Yes
No	No	No	Yes	No	No
Yes	Yes	No	No	No	No
Yes	No	Yes	Yes	No	No
No	Yes	Yes	No	No	Yes
No	No	Yes	No	No	No
Yes	Yes	No	Yes	Yes	Yes
Yes	No	No	No	No	No
No	Yes	Yes	Yes	Yes	Yes
No	No	Yes	Yes	No	No
Yes	Yes	Yes	No	No	No
Yes	No	No	Yes	Yes	No
No	Yes	No	No	No	No

- If autonegotiation is disabled, the configured flow control setting is applied to the local interface.
- Enter a slot number to configure the flow control settings for all interfaces on a specific slot.
- Enter a slot and port number or range of port numbers to configure the flow control settings for a specific interface or a range of interfaces.

Examples

```
-> interfaces 3/21 hybrid fiber pause tx
-> interfaces 4/24 hybrid copper pause rx
-> interfaces 1 hybrid fiber tx-and-rx
-> interfaces 3/21-24 hybrid copper pause tx
-> interfaces 3/21-24 hybrid copper disable
```

Release History

Release 6.3.2; command was introduced.

Related Commands

interfaces pause	Configures flow control settings for switch interfaces.
show interfaces hybrid pause	Displays flow control settings for combo ports.

MIB Objects

```
esmHybridConfigTable
   esmHybridPortCfgFlow
dot3PauseTable
   dot3PauseAdminMode
```

show interfaces

Displays general interface information (for example, hardware, MAC address, input errors, and output errors).

show interfaces [*slot* | *slot*/*port***[-***port2***]]**

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).

Defaults

By default, interface information is displayed for all ports on all modules.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Enter a slot number to display information for all interfaces on that slot.
- Enter a slot and port number or a range of port numbers to display information for a specific interface or a range of interfaces.

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,
  SFP/XFP                : Not Present,
  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 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,
  Error 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. (Currently this field is only displayed on OmniSwitch 6800 Series switches.)
Number of Status Change	The total number of times that the configuration of this interface has changed. (Currently this field is only displayed on OmniSwitch 6800 Series switches.)
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.
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 6.1; command was introduced.

Related Commands

show interfaces accounting	Displays interface accounting information (for example, packets received/transmitted).
show interfaces counters	Displays interface counter information (for example, unicast packets received/transmitted).
show interfaces counters errors	Displays interface error frame information (for example, CRC errors, transit errors, and receive errors).
show interfaces collisions	Displays interface collision information (for example, number of collisions and number of retries).
show interfaces status	Displays the interface line settings (for example, speed and 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 [*slot* | *slot*/*port***[-***port2***]] capability**

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).

Defaults

By default, information is displayed for all ports on all modules.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Enter a slot number to display information for all interfaces on that slot.
- Enter a slot and port number or a range of port numbers to display information for a specific interface or a range of interfaces.
- 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,** the field displays the valid auto negotiation configurations for the port. In the row label **DEF,** the 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,** the field displays the valid flow configurations for the port. In the row label **DEF,** the field displays the default flow settings for the port. The possible values are **EN** (enabled) or **DIS** (disabled).
Crossover	In the row labeled **CAP,** the field displays the valid cross over configurations for the port. In the row label **DEF,** the 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,** the field displays the valid line speed configurations for the port. In the row label **DEF,** the 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,** the field displays the valid duplex configurations for the port. In the row label **DEF,** the field displays the default duplex settings for the port. The possible values are **Full**, **Full/Half**, or **Auto**.

Release History

Release 6.1; command was introduced.

Related Commands

interfaces autoneg	Enables and disables auto negotiation.
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 flow control

Displays interface flow control wait time settings.

show interfaces [*slot* | *slot*/*port***[-***port2***]] flow [control]**

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
control	Optional command syntax. It displays the same information as **show interfaces flow**.

Defaults

By default, flow control wait time settings are displayed for all ports on all modules.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Enter a slot number to display information for all interfaces on that slot.
- Enter a slot and port number or a range of port numbers to display information for a specific interface or a range of interfaces.

Examples

```
-> show interfaces 3/20-24 flow
Slot/Port   Active   Wait time(usec)   Cfg-Flow     Cfg-Cross
-----------+--------+----------------+--------+-----------
 3/20         -              0           Pause      MDIX
 3/21         -              0           Pause      MDIX
 3/22         -              0           Pause      MDIX
 3/23         -              0              Go      MDIX
 3/24         -              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 (**Pause** or **Go**).
Cfg-Cross	The user-configured cross-over setting (**Auto**, **MDI**, or **MDIX**).

Release History

Release 6.1; command was introduced.
Release 6.3.2; command deprecated on the OmniSwitch 6855.
Release 6.4.3; command deprecated on OmniSwitch 6400.

Related Commands

show interfaces hybrid pause	Displays interface flow control wait time settings for combo ports.

MIB Objects

```
esmConfTable
   esmPortSlot
   esmPortIF
   esmPortPauseSlotTime
   esmPortCfgCrossover
dot3PauseTable
   dot3PauseSlotTime
```

show interfaces pause

Displays the flow control pause configuration for the specified interface(s).

show interfaces [*slot* | *slot*/*port***[-***port2***]] pause**

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).

Defaults

By default, the flow control pause configuration is displayed for all ports on all modules.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Enter a slot number to display information for all interfaces on that slot.
- Enter a slot and port number or a range of port numbers to display information for a specific interface or a range of interfaces.

Examples

```
-> show interfaces pause
 Slot/Port   Active  Wait time(usec) Cfg-Pause  Cfg-Cross Hybrid Type
-----------+--------+---------------+---------+-----------+-----------
    1/1         -               0       DIS        MDIX         -
    1/2         -               0       DIS        MDIX         -
    1/3         -               0       DIS        MDIX         -
    1/4         -               0       DIS        MDIX         -
    1/5         -               0       DIS        MDIX         -
    1/6         -               0       DIS        MDIX         -
    1/7         -               0       DIS        Auto         -
    1/8         -               0       DIS        Auto         -
    1/9         -           65535       DIS        Auto        NA
    1/10        -               0       DIS        Auto         -
    1/11        -           65535       DIS        Auto        NA
    1/12        -               0       DIS        Auto         -
    1/13        -               0       DIS        Auto         -
    1/14        -               0       DIS        Auto         -
    1/15        -               0       DIS        Auto         -
    1/16        -               0       DIS        Auto         -
    1/17        -               0       DIS        Auto         -
    1/18        -               0       DIS        Auto         -
    1/19        -               0       DIS        Auto         -
    1/20        -               0       DIS        Auto         -
    1/21        -               0       DIS         MDI         -
    1/21        -               0       DIS        Auto         -
```

```
    1/22        -               0       DIS         MDI         -
    1/22        -               0       DIS        Auto         -
    1/23        -               0       DIS         MDI         -
    1/23        -               0       DIS        Auto         -
    1/24        -               0       Tx          MDI         -
    1/24     Active         65535     Tx-N-Rx      Auto         C

-> show interfaces 1/24 pause
 Slot/Port   Active  Wait time(usec) Cfg-Pause  Cfg-Cross Hybrid Type
-----------+--------+---------------+--------+-----------+-----------
    1/24        -               0       Tx          MDI         -
    1/24     Active         65535     Tx-N-Rx      Auto         C
```

output definitions

Slot/Port	Interface slot and port number
Active	Interface status.
Wait time	The amount of time, in microseconds, the neighbor interface will wait after receiving a PAUSE frame from the local interface.
Cfg-Pause	The flow control setting (**Tx** = transmit, **Rx** = receive, **Tx-N-Rx** = transmit and receive). Configured through the **interfaces pause** command.
Cfg-Cross	The user-configured cross-over setting (**Auto**, **MDI**, or **MDIX**).
Hybrid Type	The configured active media type for a hybrid port (**F** = fiber, **C** = copper, **NA** = not applicable).

Release History

Release 6.3.2; command was introduced.

Related Commands

show interfaces hybrid pause	Displays flow control pause settings for combo ports.

MIB Objects

```
esmConfTable
   esmPortSlot
   esmPortIF
   esmPortPauseSlotTime
   esmPortCfgCrossover
   esmPortActiveHybridType
dot3PauseTable
   dot3PauseSlotTime
```

show interfaces e2e-flow-vlan

Displays the end-to-end (E2E) flow control VLAN configuration for the switch.

show interfaces e2e-flow-vlan

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E

Usage Guidelines

- This command is available only on standalone 48-port OmniSwitch 6400 and 6850E switches.
- There is only one dedicated E2E flow control VLAN configured per switch.

Examples

```
-> show interfaces e2e-flow-vlan
Configured End-To-End Flow Vlan - 10
```

Release History

Release 6.3.4; command was introduced.

Related Commands

interfaces e2e-flow-vlan	Configures a dedicated VLAN for carrying end-to-end (E2E) flow control messages to remote systems.
show interfaces pause	Displays the flow control pause configuration for the specified interface(s).

MIB Objects

```
esmE2EFlowVlan
```

show interfaces accounting

Displays interface accounting information (for example, packets received/transmitted and deferred frames received).

show interfaces [*slot* | *slot*/*port***[-***port2***]] accounting**

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).

Defaults

By default, accounting information is displayed for all ports on all modules.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Enter a slot number to display information for all interfaces on that slot.
- Enter a slot and port number or a range of port numbers to display information for a specific interface or a range of interfaces.

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.

output definitions (continued)

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 6.1; command was introduced.

Related Commands

show interfaces	Displays general interface information (for example, hardware, MAC address, and input/output errors).
show interfaces counters	Displays interface counter information (for example, 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 (for example, unicast, broadcast, and multi-cast packets received/ transmitted).

show interfaces [*slot* | *slot*/*port***[-***port2***]] counters**

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).

Defaults

By default, information is displayed for all ports on all modules.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Enter a slot number to display information for all interfaces on that slot.
- Enter a slot and port number or a range of port numbers to display information for a specific interface or a range of interfaces.
- These counters do not apply to Gigabit Ethernet traffic.
- This command also displays sampling interval statistics that show an average traffic rate per second for active switch interfaces. These statistics are taken every 5 seconds. The actual statistics shown are those taken from the last completed 5-second time interval.
- Note that the sampling interval time period is set to five seconds and is not a configurable value at this time. In addition, the sampling interval is a global value that applies to all switch ports.

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,
Sampling Interval 5 second
  InPkts / s    =                  11,   OutPkts / s    =                 11,
  Inbits / s    =              111111,   Outbits / s    =             111111,
```

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.
Sampling Interval	The sampling interval used to determine the average rate per second.
InPkts / s	The average number of packets received per second.
OutPkts / s	The average number of packets transmitted per second.
Inbits / s	The average number of bits received per second.
Outbits / s	The average number of bits transmitted per second.

Release History

Release 6.1; command was introduced.
Release 6.3.4; **Sampling Interval** fields (**InPkts**, **OutPkts**, **Inbits**, **Outbits**) were added.

Related Commands

show interfaces counters errors	Displays interface error frame information (for example, CRC errors, transit errors, and 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 (for example, CRC errors, transit errors, and receive errors).

show interfaces [*slot* | *slot*/*port***[-***port2***]] counters errors**

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).

Defaults

By default, information is displayed for all ports on all modules.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Enter a slot number to display information for all interfaces on that slot.
- Enter a slot and port number or a range of port numbers to display information for a specific interface or a range of interfaces.
- 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 received error frames.
IfOutErrors	Number of transmitted error frames.
Undersize pkts	Number of undersized packets.
Oversize pkts	Number of oversized packets (more than 1518 octets).

Release History

Release 6.1; command was introduced.

Related Commands

show interfaces counters	Displays interface counters information (for example, unicast, broadcast, and 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 (for example, number of collisions and number of retries).

show interfaces [*slot* | *slot*/*port***[-***port2***]] collisions**

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).

Defaults

By default, information is displayed for all ports on all modules.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Enter a slot number to display information for all interfaces on that slot.
- Enter a slot and port number or a range of port numbers to display information for a specific interface or a range of interfaces.
- 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.
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 receive collisions.
Rx Single Collision	Number of successfully received frames for which reception was inhibited by one collision.

output definitions (continued)

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 6.1; command was introduced.

Related Commands

show interfaces	Displays general interface information (for example, hardware, MAC address, input errors, and output errors).

MIB Objects

```
esmConfTable
   esmPortSlot
   esmPortIF
alcetherStatsTable
   alcetherStatsRxCollisions
dot3StatsTable
   dot3StatsSingleCollisionFrames
   dot3StatsMultipleCollisionFrames
   dot3StatsExcessiveCollisions
```

show interfaces status

Displays interface line settings (for example, speed and mode).

show interfaces [*slot* | *slot*/*port***[-***port2***]] status**

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).

Defaults

By default, line settings are displayed for all ports on all modules.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Enter a slot number to display information for all interfaces on that slot.
- Enter a slot and port number or a range of port numbers to display information for a specific interface or a range of interfaces.

Examples

The following is an example for a non combo port:

```
-> 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      -
```

The following is an example for a combo port:

```
-> show interfaces 1/47 status
                       DETECTED           CONFIGURED
Slot/ AutoNego  Speed Duplex Hybrid  Speed   Duplex Hybrid  Trap
Port           (Mbps)         Type   (Mbps)         Mode   LinkUpDown
-----+--------+------+------+------+--------+------+------+------
 1/47  Enable    -      -      -        1000  Full    PF      -
 1/47  Enable    -      -      -       Auto   Auto    PF      -

FF - ForcedFiber PF - PreferredFiber  F - Fiber
FC - ForcedCopper PC - PreferredCopper C - Copper
```

output definitions

Slot/Port	Interface slot/port number.
AutoNego	Autonegotiation 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	The detected combo port type, which can be **F** (fiber) or **C** (copper). (This field is only relevant for OmniSwitch 6800 Series 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	The configured combo port type, which can be **FF** (Forced Fiber), **PF** (Preferred Fiber), **FC** (Forced Copper), or **PC** (Preferred Copper).
Trap Link Up/Down	Trap Link status (up/down).

Release History

Release 6.1; 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.
interfaces hybrid preferred-fiber	Configures one or more combo ports to use the fiber SFP port(s) instead of the equivalent copper 10/100/1000 RJ-45 port(s) when both ports are enabled and have a valid link.
interfaces hybrid autoneg	Configures one or more combo ports to use the copper 10/100/1000 RJ-45 port(s) instead of the fiber SFP port(s) when both ports are enabled and have a valid link.

MIB Objects

```
ifTable
   ifLinkUpDownTrapEnable
esmConfTable
   esmPortSlot
   esmPortIF
   esmPortAutoSpeed
   esmPortAutoDuplexMode
   esmPortCfgSpeed
   esmPortCfgDuplexMode
esmHybridConfTable
   esmPortCfgHybridMode
   esmPortCfgHybridType
```

show interfaces port

Displays the administrative status, link status, violations, recovery time, maximum recovery attempts and the value of the wait-to-restore timer for the specified port or ports.

show interfaces [*slot* | *slot*/*port***[-***port2***]] port**

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).

Defaults

By default, information is displayed for all ports on all modules.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Enter a slot number to display information for all interfaces on that slot.
- Enter a slot and port number or a range of port numbers to display information for a specific interface or a range of interfaces.
- On a combo port with SFP fiber ports, the status of the SFP ports will be displayed. See the **show interfaces hybrid port** command for more information.
- The hash symbol (#) is displayed before the wait-to-restore value if the link state is WAIT (i.e., the wait-to-restore timer is running.

Examples

```
-> show interfaces 1/1 port
Legends: WTR - Wait To Restore
         #   - WTR Timer is Running & Port is in wait-to-restore state
         *   - Permanent Shutdown
Slot/    Admin     Link    Violations  Recovery   Recovery      WTR      Alias
Port     Status   Status                 Time       Max        (sec)
------+----------+---------+----------+----------+----------+----------+--------
1/1     enable      down      none       300         1           0         ""
```

```
-> show interfaces 1 port
Legends: WTR - Wait To Restore
         #   - WTR Timer is Running & Port is in wait-to-restore state
         *   - Permanent Shutdown

Slot/    Admin     Link    Violations  Recovery   Recovery      WTR      Alias
Port     Status   Status                 Time       Max        (sec)
------+----------+---------+----------+----------+----------+----------+--------
  1/1    enable    down      none         300        10          0        ""
  1/2    enable    down      none         300        10          0        ""
  1/3    enable    down      none         300        10          0        ""
  1/4    enable    down      none         300        10          0        ""
  1/5    enable    down      none         300        10          0        ""
  1/6    enable    down      none         300        10          0        ""
  1/7    enable    down      none         300        10          0        ""
  1/8    enable    down      none         300        10          0        ""
  1/9*   enable    down      LinkMon      30         2           0        ""
  .
  .
  .
  1/26   enable    down      none          0          0          0        ""
```

output definitions

Slot/Port	Interface slot and port number. An asterisk (*) with slot/port indicates that the port is permanently shutdown.
Admin Status	Port status - **enable**, **disable**. Configured through the **interfaces admin** command.
Link Status	Operational status - **up**, **down**.
Violations	Applications that have blocked the port due to a specific violation.
Recovery Time	The recovery time for the port. Configured through the **interfaces violation-recovery-time** command.
Recovery Max	The maximum recovery attempts for the port Configured through the **interfaces violation-recovery-maximum** command.
WTR (sec)	The wait-to-restore timer value, in seconds, for the port. The value of 0 indicates the timer is disabled. Configured through the **interfaces wait-to-restore** command.
Alias	Interface alias. Configured through the **interfaces alias** command.

Release History

Release 6.1; command was introduced.
Release 6.3.1; **Violations** field was added.
Release 6.4.4; **Recovery Time, Recovery Max, WTR (sec)** fields were added.

Related Commands

show interfaces hybrid port	Displays interface port status (up or down) for combo ports.
show interfaces violation-recovery	Displays the globally configured recovery time, SNMP recovery trap enable/disable status and maximum recovery attempts.

MIB Objects

```
esmConfTable
   esmPortSlot
   esmPortIF
   esmPortViolationBitMap
   esmWaitToRestoreTimer
ifXTable
   ifAdminStatus
   ifOperStatus
   ifAlias
alaPortViolationRecoveryTable
   alaPortViolationRecoveryTime
   alaPortViolationRecoveryMaximum
```

show interfaces violation-recovery

Displays the globally configured recovery time, SNMP recovery trap enable/disable status and maximum recovery attempts.

show interfaces violation-recovery

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show interfaces violation-recovery
UserPorts Shutdown Recovery Time: 200
UserPorts Shutdown Recovery Trap: Enable
UserPorts Shutdown Maximum Recovery: 2
```

output definitions

UserPorts Shutdown Recovery Time	The recovery time configured for the port.
UserPorts Shutdown Recovery Trap	SNMP recovery trap status - **enable**, **disable**.
UserPorts Shutdown Maximum Recovery	The maximum recovery attempts configured for the port before a port is permanently shut down.

Release History

Release 6.4.4; command was introduced.

Related Commands

interfaces violation-recovery-time	Configures the time interval after which the port is automatically re-activated if the port was shut down for any violation.
interfaces violation-recovery-maximum	Configures the maximum number of recovery attempts before a port is permanently shut down.
show interfaces port	Displays the administrative, operational, violation, and recovery status and configuration for the specified port.

MIB Objects

```
esmViolationRecovery
   esmViolationRecoveryTime
   esmViolationRecoveryTrap
   esmViolationRecoveryMaximum
```

show interfaces ifg

Displays interface inter-frame gap values.

show interfaces [*slot* | *slot*/*port***[-***port2***]] ifg**

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).

Defaults

By default, information is displayed for all ports on all modules.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Enter a slot number to display information for all interfaces on that slot.
- Enter a slot and port number or a range of port numbers to display information for a specific interface or a range of interfaces.

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 6.1; 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 [*slot* | *slot/port* **[-***port2***]] flood rate**

Syntax Definitions

slot	The slot number for a specific module.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).

Defaults

By default, information is displayed for all ports on all modules.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Enter a slot number to display information for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to display information for a specific interface or a range of interfaces.

Examples

```
-> show interfaces flood rate

Slot/    Bcast      Bcast  Bcast     Ucast    Ucast  Ucast      Mcast  Mcast  Mcast
Port     Value      Type   Status    Value    Type   Status     Value  Type   Status
--------+----------+-----+---------+---------+-----+---------+----------+-----+---
 1/1         500   pps   enable        496   mbps   enable    496     mbps enable
 1/2          33   mbps  enable        496   mbps   enable     35      %   enable
 1/3         496   mbps  enable          5   mbps   enable    496     mbps enable
 1/4         496   mbps  enable        496   mbps   enable    496     mbps enable
 1/5         496   mbps  enable        496   mbps   enable    496     mbps enable

-> show interfaces 1/2 flood rate

Slot/    Bcast      Bcast  Bcast     Ucast    Ucast  Ucast      Mcast  Mcast  Mcast
Port     Value      Type   Status    Value    Type   Status     Value  Type   Status
--------+----------+-----+---------+---------+-----+---------+----------+-----+---
 1/2      33        mbps  enable      496   mbps   enable       35       %   enable
```

output definitions

Slot/Port	Interface slot and port numbers.
Bcast Value	The broadcast storm value based on the type.
Bcast Type	The type of broadcast (**mbps**, **pps**, **percentage**).

output definitions (continued)

Bcast Status	The status of brodcast, **enable** or **disable**.
Ucast Value	The unknown-unicast storm value based on the type.
Ucast Type	The type of unknown-unicast (**mbps**, **pps**, **percentage**)
Ucast Status	The status of unicast, **enable** or **disable**.
Mcast Value	The multicast storm value based on the type.
Mcast Type	The type of multicast (**mbps**, **pps**, **percentage**)
Mcast Status	The status of multicast, **enable** or **disable**.

Release History

Release 6.1; command was introduced.

Related Commands

interfaces flood	Enables traffic storm control on the specified interface.
interfaces flood rate	Configures the peak flood rate for an interface.

MIB Objects

```
esmConfTable
   esmPortSlot
   esmPortIF
   esmPortMaxFloodRate
   esmPortFloodMcastEnable
```

show interfaces traffic

Displays interface traffic statistics.

show interfaces [*slot* | *slot*/*port***[-***port2***]] traffic**

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).

Defaults

By default, information is displayed for all ports on all modules.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Enter a slot number to display information for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to display information for a specific interface or a range of interfaces.

Examples

```
-> show interfaces traffic

Slot/Port   Input packets     Input bytes   Output packets    Output bytes
---------+----------------+-------------+----------------+----------------

01/24         4222877       326616952         46792         742062003/01
```

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 6.1; command was introduced.

Related Commands

show interfaces	Displays general interface information (for example, hardware, MAC address, and input/output errors).
show interfaces counters	Displays interface counter information (for example, unicast packets received/transmitted).

MIB Objects

```
esmConfTable
   esmPortSlot
   esmPortIF
ifXTable
   ifHCInOctets
   ifHCInUcastPkts
   ifHCInMulticastPkts
   ifHCInBroadcastPkts
   ifHCOutOctets
   ifHCOutUcastPkts
   ifHCOutMulticastPkts
   ifHCOutBroadcastPkts
```

show interfaces transceiver

Displays the DDM information for the specified transceivers.

show interfaces [*slot* | *slot*/*port***[-***port2***]] transceiver [ddm | w-low | w-high | a-low | a-high | actual]**

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
ddm	Displays the administrative and trap status of the DDM feature.
w-low	Displays the Warning Low threshold for temperature, voltage, current, RX power and TX power.
w-high	Displays the Warning High threshold for temperature, voltage, current RX power and TX power.
a-low	Displays the Alarm Low threshold for temperature, voltage, current RX power and TX power.
a-high	Displays the Alarm High threshold for temperature, voltage, current RX power and TX power.
actual	Displays the Actual values for temperature, voltage, current RX power and TX power.

Defaults

By default, information is displayed for all ports on all modules and for all DDM parameter options.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Transceiver DDM capability will vary based on the transceiver manufacturer.
- Enter a slot number to display information for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to display information for a specific interface or a range of interfaces.
- The transceiver DDM must be enabled with **interfaces transceiver ddm enable** command before using this command.

Examples

```
-> show interfaces transceiver w-low
Slot/Port Temp C Voltage(V) Current(mA) Output(dBm) Input(dBm)
---------+------+----------+-----------+----------+---------+
1/1         48      5.15         50        2.50      2.50
1/2         47      5.35         49        2.43      2.43
1/3         NA       NA          NA          NA        NA

-> show interfaces transceiver a-high

Slot/Port Temp C Voltage(V) Current(mA) Output(dBm) Input(dBm)
---------+------+----------+-----------+----------+---------+
1/1         50      5.75        75         3.22       3.22
1/2         50      5.95        65         3.22       3.22
1/3         NA       NA          NA          NA        NA

-> show interfaces 1/1 transceiver

Threshold    Temp C Voltage(V) Current(mA) Output(dBm) Input(dBm)
------------+------+----------+-----------+----------+---------+
Actual         50    1.95(WL)     75         4.92(AH)   3.22
Alarm High     120    5.75       100         4.91       4.91
Warning High   90     3.00        90         4.77       4.77
Warning Low    10     2.00        60         0.00       0.00
Alarm Low      -5     1.75        20        -3.01      -10

-> show interfaces transceiver ddm
DDM Status      : enable
DDM Trap Status : disable
```

output definitions

Slot/Port	Interface slot and port numbers.
Temp C	The transceiver temperature, in degrees centigrade.
Voltage (V)	The transceiver supply voltage, in volts.
Current (mA)	The transceiver transmit bias current, in milliamps.
Output (dBm)	The transceiver output power, in decibels.
Input (dBm)	The transceiver received optical power, in decibels.
DDM Status	The administrative status of DDM.
DDM Trap Status	The administrative status of DDM traps.
Actual	The real-time values indicated by the transceiver. Values displayed in parentheses indicate the Warning or Alarm value that has been reached.
Alarm High (AH)	Indicates the value at which the transceiver's functionality may be affected.
Warning High (WH)	Indicates the transceiver is approaching the High Alarm value.
Warning Low (WL)	Indicates the transceiver is approaching the Low Alarm value.
Alarm Low (AL)	Indicates the value at which the transceiver's functionality may be affected.
N/A	Indicates the transceiver does support DDM.

Release History

Release 6.4.2; command was introduced.

Related Commands

interfaces transceiver ddm	Configures the DDM administrative status or trap capability.

MIB Objects

```
ddmNotifications
   ddmTemperature
   ddmTempLowWarning
   ddmTempLowAlarm
   ddmTempHiWarning
   ddmTempHiAlarm
   ddmSupplyVoltage
   ddmSupplyVoltageLowWarning
   ddmSupplyVoltageLowAlarm
   ddmSupplyVoltageHiWarning
   ddmSupplyVoltageHiAlarm
   ddmTxBiasCurrent
   ddmTxBiasCurrentLowWarning
   ddmTxBiasCurrentLowAlarm
   ddmTxBiasCurrentHiWarning
   ddmTxBiasCurrentHiAlarm
   ddmTxOutputPower
   ddmTxOutputPowerLowWarning
   ddmTxOutputPowerLowAlarm
   ddmTxOutputPowerHiWarning
   ddmTxOutputPowerHiAlarm
   ddmRxOpticalPower
   ddmRxOpticalPowerLowWarning
   ddmRxOpticalPowerLowAlarm
   ddmRxOpticalPowerHiWarning
   ddmRxOpticalPowerHiAlarm
```

show interfaces hybrid

Displays general interface information (for example, hardware, MAC address, input errors, output errors) for combo ports.

show interfaces [*slot* **|** *slot*/*port***[-***port2***]] hybrid {fiber | copper}**

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
fiber	Specifies that the status of the SFP port(s) will be displayed.
copper	Specifies that the status of the copper 10/100/1000 RJ-45 port(s) will be displayed.

Defaults

By default, information is displayed for all ports on all modules.

Platforms Supported

OmniSwitch 6400, 6855, 6850E

Usage Guidelines

- Enter a slot number to display information for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to display information for a specific interface or a range of interfaces.

Examples

```
   -> show interfaces 1/24 hybrid copper

 Slot/Port  1/24 :

  Operational Status     : up,
  Last Time Link Changed : THU DEC 06 01:30:12 ,
  Number of Status Change: 1,
  Type                   : Ethernet,
  SFP/XFP                : Not Present,
  MAC address            : 00:e0:b1:d3:09:18,
  BandWidth (Megabits)   :      100,            Duplex           : Full,
  Autonegotiation        :   1  [ 1000-F 100-F 100-H 10-F 10-H ],
  Long Frame Size(Bytes) : 1553,
```

```
 Rx              :
 Bytes Received  :            326833563, Unicast Frames :                30820,
 Broadcast Frames:              3110737, M-cast Frames  :              1083616,
 UnderSize Frames:                    0, OverSize Frames:                    0,
 Lost Frames     :                    0, Error Frames   :                    1,
 CRC Error Frames:                    1, Alignments Err :                    1,
 Tx              :
 Bytes Xmitted   :              7431026, Unicast Frames :                17024,
 Broadcast Frames:                 5586, M-cast Frames  :                24325,
 UnderSize Frames:                    0, OverSize Frames:                    0,
 Lost Frames     :                    0, Collided Frames:                    0,
 Error Frames    :                    0

-> show interfaces 1/47 hybrid fiber

 Slot/Port  1/47 :
  Operational Status     : down,
  Last Time Link Changed : FRI DEC 27 15:10:23 ,
  Number of Status Change: 0,
  Type                   : Ethernet,
  MAC address            : 00:d0:95:b2:39:b2,
  BandWidth (Megabits)   : 1000,                Duplex           : -,
  Autonegotiation        :   1  [ 1000-F                        ],
  Long Accept            : Enable,              Runt Accept      : Disable,
  Long Frame Size(Bytes) : 9216,                Runt Size(Bytes) : 64,
  Rx              :
  Bytes Received  :                    0, Unicast Frames :                    0,
  Broadcast Frames:                    0, M-cast Frames  :                    0,
  UnderSize Frames:                    0, OverSize Frames:                    0,
  Lost Frames     :                    0, Error Frames   :                    0,
  CRC Error Frames:                    0, Alignments Err :                    0,
  Tx              :
  Bytes Xmitted   :                    0, Unicast Frames :                    0,
  Broadcast Frames:                    0, M-cast Frames  :                    0,
  UnderSize Frames:                    0, OverSize Frames:                    0,
  Lost Frames     :                    0, Collided Frames:                    0,
  Error 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).

output definitions (continued)

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 r oversized frames received.
Rx Lost Frames	Number of Lost Frames received.
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 6.1; command was introduced.

Related Commands

show interfaces hybrid accounting	Displays interface accounting information (for example, packets received/transmitted) for combo ports.
show interfaces hybrid counters	Displays interface counter information (for example, unicast packets received/transmitted) for combo ports.
show interfaces hybrid counters errors	Displays interface error frame information (for example, CRC errors, transit errors, receive errors) for combo ports.
show interfaces hybrid collisions	Displays interface collision information (for example, number of collisions, number of retries) for combo ports.
show interfaces hybrid status	Displays the interface line settings (for example, speed, mode) for combo ports.
show interfaces hybrid traffic	Displays interface traffic statistics (input/output bytes and packets) for combo ports.

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 hybrid status

Displays interface line settings (for example, speed, mode) for combo ports only.

show interfaces [*slot* | *slot*/*port***[-***port2***]] hybrid {fiber | copper} status**

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
fiber	Specifies that the status of the SFP port(s) will be displayed.
copper	Specifies that the status of the copper 10/100/1000 RJ-45 port(s) will be displayed.

Defaults

By default, information is displayed for all ports on all modules.

Platforms Supported

OmniSwitch 6400, 6855, 6850E

Usage Guidelines

- Enter a slot number to display information for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to display information for a specific interface or a range of interfaces.

Examples

```
-> show interfaces hybrid fiber status
                        DETECTED           CONFIGURED
Slot/ AutoNego  Speed Duplex Hybrid  Speed   Duplex Hybrid  Trap
Port           (Mbps)         Type   (Mbps)         Mode   LinkUpDown
-----+--------+------+------+------+--------+------+------+------
 1/45  Enable    -      -      -        1000  Full    PF      -
 1/46  Enable    -      -      -        1000  Full    PF      -
 1/47  Enable    -      -      -        1000  Full    PF      -
 1/48  Enable    -      -      -        1000  Full    PF      -
 2/45  Enable    -      -      -        1000  Full    PF      -
 2/46  Enable    -      -      -        1000  Full    PF      -
 2/47  Enable    -      -      -        1000  Full    PF      -
 2/48  Enable    -      -      -        1000  Full    PF      -

FF - ForcedFiber PF - PreferredFiber  F - Fiber
FC - ForcedCopper PC - PreferredCopper C - Copper
```

output definitions

Slot/Port	Interface slot/port number.
AutoNego	Autonegotiation 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	The detected combo port type, which can be **F** (fiber) or **C** (copper).
Configured Speed	Configured line speed (10/100/Auto/1000/10000 Mbps).
Configured Duplex	Configured line duplex (Half duplex/Full duplex/Auto).
Configured Hybrid Type	The configured combo port type, which can be **FF** (Forced Fiber), **PF** (Preferred Fiber), **FC** (Forced Copper), or **PC** (Preferred Copper).
Trap Link Up/Down	Trap Link status (up/down).

Release History

Release 6.1; command was introduced.

Related Commands

trap port link	Enables/disables Trap LinkUpDown.
interfaces hybrid speed	Configures interface line speed on combo ports.
interfaces hybrid duplex	Configures duplex mode on combo ports.
interfaces hybrid preferred-fiber	Configures one or more combo ports to use the fiber SFP port(s) instead of the equivalent copper 10/100/1000 RJ-45 port(s) when both ports are enabled and have a valid link.
interfaces hybrid autoneg	Configures one or more combo ports to use the copper 10/100/1000 RJ-45 port(s) instead of the fiber SFP port(s) when both ports are enabled and have a valid link.

MIB Objects

```
ifTable
   ifLinkUpDownTrapEnable
esmConfTable
   esmPortSlot
   esmPortIF
   esmPortAutoSpeed
   esmPortAutoDuplexMode
esmHybridConfTable
   esmPortCfgHybridMode
   esmPortCfgHybridType
   esmHybridPortCfgSpeed
   esmHybridPortCfgDuplexMode
```

show interfaces hybrid pause

Displays the flow control pause configuration for combo ports.

show interfaces [*slot* | *slot*/*port***[-***port2***]] hybrid {fiber |copper} pause**

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
fiber	Specifies that the configuration of the SFP port(s) will be displayed.
copper	Specifies that the configuration of the copper 10/100/1000 RJ-45 port(s) will be displayed.

Defaults

By default, information is displayed for all ports on all modules.

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- Refer to the *Hardware Users Guide* for combo port numbering.
- Enter a slot number to display information for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to display information for a specific interface or a range of interfaces.

Examples

```
-> show interfaces hybrid fiber pause
 Slot/Port   Active  Wait time(usec) Cfg-Pause  Cfg-Cross Hybrid Type
-----------+--------+---------------+---------+-----------+-----------
    1/21        -               0       DIS         MDI         -
    1/22        -               0       DIS         MDI         -
    1/23        -               0       DIS         MDI         -
    1/24        -               0       Tx          MDI         -

-> show interfaces hybrid copper pause
 Slot/Port   Active  Wait time(usec) Cfg-Pause  Cfg-Cross Hybrid Type
-----------+--------+---------------+---------+-----------+-----------
    1/21        -               0       DIS        Auto         -
    1/22        -               0       DIS        Auto         -
    1/23        -               0       DIS        Auto         -
    1/24     Active         65535     Tx-N-Rx      Auto         C
```

output definitions

Slot/Port	Interface slot and port number
Active	Interface status.
Wait time	The amount of time, in microseconds, the neighbor interface will wait after receiving a PAUSE frame from the local interface.
Cfg-Pause	The flow control setting (**Tx** = transmit, **Rx** = receive, **Tx-N-Rx** = transmit and receive). Configured through the **interfaces hybrid pause** command.
Cfg-Cross	The user-configured cross-over setting (**Auto**, **MDI**, or **MDIX**). Configured through the **interfaces hybrid crossover** command.
Hybrid Type	The configured active media type for the hybrid port (**F** = fiber, **C** = copper, **NA** = not applicable).

Release History

Release 6.3.2; command was introduced.

Related Commands

show interfaces pause	Displays the interface flow control pause settings.

MIB Objects

```
esmConfTable
   esmPortCfgSlot
   esmPortCfgIF
   esmPortPauseSlotTime
   esmPortActiveHybridType
esmHybridConfTable
   esmHybridPortCfgFlow
   esmHybridPortCfgCrossover
dot3PauseTable
   dot3PauseSlotTime
```

show interfaces hybrid capability

Displays default auto negotiation, speed, duplex, flow, and cross-over settings for a single combo port, a range of combo ports, or all combo ports on a switch.

show interfaces [*slot* | *slot*/*port***[-***port2***]] hybrid {fiber |copper} capability**

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
fiber	Specifies that the configuration of the SFP port(s) will be displayed.
copper	Specifies that the configuration of the copper 10/100/1000 RJ-45 port(s) will be displayed.

Defaults

By default, displays information for all ports on all modules.

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- This command displays defaults settings in two rows of data for each combo port. The first row of data, identified by the label **CAP**, displays the valid user-defined configuration settings available for the combo port. The second row, identified by the label **DEF**, displays the default settings for the combo port.
- Enter a slot number to display information for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to display information for a specific interface or a range of interfaces.

Examples

```
-> show interfaces hybrid copper capability
   Slot/Port   AutoNeg     Flow   Crossover      Speed    Duplex
-----------+---------+--------+-----------+----------+----------
  1/21 CAP     EN/DIS   EN/DIS  MDI/X/Auto  10/100/1G  Full/Half
  1/21 DEF         EN      DIS        Auto       Auto       Auto
  1/22 CAP     EN/DIS   EN/DIS  MDI/X/Auto  10/100/1G  Full/Half
  1/22 DEF         EN      DIS        Auto       Auto       Auto
  1/23 CAP     EN/DIS   EN/DIS  MDI/X/Auto  10/100/1G  Full/Half
  1/23 DEF         EN      DIS        Auto       Auto       Auto
  1/24 CAP     EN/DIS   EN/DIS  MDI/X/Auto  10/100/1G  Full/Half
  1/24 DEF         EN      DIS        Auto       Auto       Auto
```

```
-> show interfaces 1/24 hybrid copper capability

   Slot/Port   AutoNeg     Flow   Crossover      Speed    Duplex
-----------+---------+--------+-----------+----------+----------
  1/24 CAP     EN/DIS   EN/DIS  MDI/X/Auto  10/100/1G  Full/Half
  1/24 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).
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**, 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 6.1; command was introduced.

Related Commands

interfaces hybrid autoneg	Enables and disables auto negotiation for combo ports.
interfaces hybrid crossover	Configures crossover port settings for combo ports.
interfaces hybrid speed	Configures interface speed for combo ports.
interfaces hybrid duplex	Configures duplex settings for combo ports.
show interfaces hybrid status	Displays interface line settings for combo ports.

MIB Objects

```
esmConfTable
   esmPortCfgSlot
   esmPortCfgIfIndex
```

```
esmHybridConfTable
   esmHybridPortCfgAutoNegotiation
   esmHybridPortCfgFlow
   esmHybridPortCfgCrossover
   esmHybridPortCfgSpeed
   esmHybridPortCfgDuplex
```

show interfaces hybrid accounting

Displays interface accounting information (for example, packets received/transmitted, deferred frames received) for combo ports.

show interfaces [*slot* | *slot*/*port***[-***port2***]] hybrid {fiber |copper} accounting**

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
fiber	Specifies that statistics for the SFP port(s) will be displayed.
copper	Specifies that statistics for the copper 10/100/1000 RJ-45 port(s) will be displayed.

Defaults

By default information is displayed for all ports on all modules.

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- Enter a slot number to display information for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to display information for a specific interface or range of interfaces.

Examples

```
-> show interfaces hybrid copper accounting
 1/24: --------------------- RX --------------------------------- TX ---------
     Undersize    =                    0,  Undersize    =                    0,
     Oversize     =                    0,  Oversize     =                    0,
     Jabber       =                    0,
     : ------------------ RX / TX -----------------------------------------
         64 Octets=               3073380,
  65 ~  127 Octets=                989343,
 128 ~  255 Octets=                103655,
 256 ~  511 Octets=                100026,
 512 ~ 1023 Octets=                  8946,
1024 ~ 1518 Octets=                     0,
1519 ~ 4095 Octets=                     0,
4096 ~  MAX Octets=                     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 6.1; command was introduced.

Related Commands

show interfaces hybrid	Displays general interface information (for example, hardware, MAC address, input/output errors) for combo ports.
show interfaces hybrid counters	Displays interface counter information (for example, unicast packets received/transmitted) for combo ports.

MIB Objects

```
esmConfTable
   esmPortCfgSlot
   esmPortCfgIfIndex
alcetherStatsTable
   alcetherStatRxsUndersizePkts
   alcetherStatTxsUndersizePkts
   alcetherStatsTxOversizePkts
   alcetherStatsPkts64Octets
   alcetherStatsPkts65to127Octets
   alcetherStatsPkts128to255Octets
   alcetherStatsPkts256to511Octets
   alcetherStatsPkts512to1023Octets
   alcetherStatsPkts1024to1518Octets
   gigaEtherStatsPkts1519to4095Octets
   gigaEtherStatsPkts4096to9215Octets
   alcetherStatsRxJabber
dot3StatsTable
   dot3StatsFrameTooLong
   dot3StatsDeferredTransmissions
```

show interfaces hybrid counters

Displays interface counters information (for example, unicast, broadcast, multi-cast packets received/transmitted) for combo ports.

show interfaces [*slot* | *slot*/*port***[-***port2***]] hybrid {fiber |copper} counters**

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
fiber	Specifies that statistics for the SFP port(s) will be displayed.
copper	Specifies that statistics for the copper 10/100/1000 RJ-45 port(s) will be displayed.

Defaults

By default, information is displayed for all ports on all modules.

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- Enter a slot number to display information for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to display information for a specific interface or range of interfaces.
- These counters do not apply to Gigabit Ethernet traffic.

Examples

```
-> show interfaces 1/24 hybrid copper counters

 1/24,
  InOctets      =            327192315,  OutOctets      =              7457698,
  InUcastPkts   =                31079,  OutUcastPkts   =                17261,
  InMcastPkts   =              1085360,  OutMcastPkts   =                24350,
  InBcastPkts   =              3112659,  OutBcastPkts   =                 5592,
  InPauseFrames =                    0,  OutPauseFrames =                    0,
  Sampling Interval 5 seconds
  InPkts/s      =                    6,  OutPkts/s      =                    2,
  InBits/s      =                 3104,  OutBits/s      =                  608
```

output definitions

InOctets	Number of octets received.
OutOctets	Number of octets transmitted.

output definitions (continued)

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.
Sampling Interval	Packet sampling interval in seconds
InPkts	Total number of packets incoming
OutPkts	Total number of packets outgoing
InBits	Total number of bits incoming
OutBits	Total number of bits outgoing

Release History

Release 6.1; command was introduced.

Related Commands

show interfaces hybrid counters errors	Displays interface error frame information (for example, CRC errors, transit errors, receive errors).

MIB Objects

```
esmConfTable
   esmPortCfgSlot
   esmPortCfgIfIndex
ifXTable
   IfHCInOctets
   IfHCOutOctets
   IfHCInUcastPkts
   IfHCOutUcastPkts
   IfHCInMulticastPkts
   IfHCOutMulticastPkts
   IfHCInBroadcastPkts
   IfHCOutBroadcastPkts
dot3PauseTable
   dot3InPauseFrame
   dot3OutPauseFrame
```

show interfaces hybrid counters errors

Displays interface error frame information (for example, CRC errors, transit errors, receive errors) for combo ports.

show interfaces [*slot* | *slot*/*port***[-***port2***]] hybrid {fiber |copper} counters errors**

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
fiber	Specifies that statistics for the SFP port(s) will be displayed.
copper	Specifies that statistics for the copper 10/100/1000 RJ-45 port(s) will be displayed.

Defaults

By default, information is displayed for all ports on all modules.

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- Enter a slot number to display information for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to display information for a specific interface or range of interfaces.
- These counters do not apply to Gigabit Ethernet traffic.

Examples

```
-> show interfaces 1/47 hybrid copper counters errors

01/47,
  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 received error frames.
IfOutErrors	Number of transmitted error frames.

output definitions (continued)

Undersize pkts	Number of undersized packets.
Oversize pkts	Number of oversized packets (more than 1518 octets).

Release History

Release 6.1; command was introduced.

Related Commands

show interfaces hybrid counters Displays interface counters information (for example, unicast, broadcast, multi-cast packets received/transmitted).

MIB Objects

```
esmConfTable
   esmPortCfgSlot
   esmPortCfgIfIndex
ifTable
   ifInErrors
   ifOutErrors
alcetherStatsTable
   alcetherStatsRxUndersizePkts
dot3StatsTable
   dot3StatsAlignmentErrors
   dot3StatsFCSErrors
   dot3StatsFrameTooLong
```

show interfaces hybrid collisions

Displays interface collision information (for example, number of collisions, number of retries) for combo ports.

show interfaces [*slot* | *slot*/*port***[-***port2***]] hybrid {fiber |copper} collisions**

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
fiber	Specifies that statistics for the SFP port(s) will be displayed.
copper	Specifies that statistics for the copper 10/100/1000 RJ-45 port(s) will be displayed.

Defaults

By default, information is displayed for all ports on all modules.

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- Enter a slot number to display information for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to display information for a specific interface or range of interfaces.
- These counters do not apply to Gigabit Ethernet traffic.

Examples

```
-> show interfaces hybrid copper collisions
 1/24,
  Tx Collisions          =                   0,  Tx Single Collision      =  0,
  Tx Multiple Collisions =                   0,  Tx Excessive Collisions  =  0,
  Rx Collisions          =                   0
```

For recieve enabled ports

```
-> show interfaces 1/47 hybrid copper 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.
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 receive 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 6.1; command was introduced.

Related Commands

show interfaces hybrid	Displays general interface information (for example, hardware, MAC address, input errors, output errors) for combo ports.

MIB Objects

```
esmConfTable
   esmPortCfgSlot
   esmPortCfgIfIndex
alcetherStatsTable
   alcetherStatsRxCollisions
dot3StatsTable
   dot3StatsSingleCollisionFrames
   dot3StatsMultipleCollisionFrames
   dot3StatsExcessiveCollisions
```

show interfaces hybrid traffic

Displays interface traffic statistics for combo ports.

show interfaces [*slot* | *slot*/*port***[-***port2***]] hybrid {fiber |copper} traffic**

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
fiber	Specifies that statistics for the SFP port(s) will be displayed.
copper	Specifies that statistics for the copper 10/100/1000 RJ-45 port(s) will be displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- Enter a slot number to display information for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to display information for a specific interface or range of interfaces.

Examples

```
-> show interfaces hybrid fiber traffic

Slot/Port   Input packets     Input bytes      Output packets    Output bytes
---------+-----------------+-----------------+-----------------+----------------

01/45                  0                         0                 0
01/46                  0                         0                0
01/47                  0                         0                0
01/48                  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 6.1; command was introduced.

Related Commands

show interfaces hybrid	Displays general interface information (for example, hardware, MAC address, input/output errors) for combo ports.
show interfaces hybrid counters	Displays interface counter information (for example, unicast packets received/transmitted) for combo ports.

MIB Objects

```
esmConfTable
   esmPortCfgSlot
   esmPortCfgIfIndex
ifXTable
   ifHCInOctets
   ifHCInUcastPkts
   ifHCInMulticastPkts
   ifHCInBroadcastPkts
   ifHCOutOctets
   ifHCOutUcastPkts
   ifHCOutMulticastPkts
   ifHCOutBroadcastPkts
```

show interfaces hybrid port

Displays interface port status (up or down) for combo ports.

show interfaces [*slot* | *slot*/*port***[-***port2***]] hybrid {fiber |copper} port**

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
fiber	Specifies that the status of the SFP combo port(s) will be displayed.
copper	Specifies that the status of the copper combo 10/100/1000 RJ-45 port(s) will be displayed.

Defaults

By default, information is displayed for all hybrid ports on all modules.

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- Enter a slot number to display information for all hybrid interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to display information for a specific hybrid interface or a range of hybrid interfaces.

Examples

```
-> show interfaces hybrid fiber port
Legends: WTR - Wait To Restore
         #   - WTR Timer is Running & Port is in wait-to-restore state
         *   - Permanent Shutdown
Slot/    Admin     Link    Violations  Recovery   Recovery      WTR      Alias
Port     Status   Status                 Time       Max        (sec)
------+----------+---------+----------+----------+----------+----------+--------
1/21   enable      up        none           300         10          0 ""
1/22#  enable      down      none           300         10          0 ""
1/23   enable      down      none           300         10          0 ""
1/24*  enable      down      none           300         10          0 ""
```

output definitions

Slot/Port	Interface slot and port number.
Admin Status	Port status - **enable**, **disable**. Configured through the **interfaces admin** command.
Link Status	Operational status - **up**, **down**.

output definitions (continued)

Violations	Applications that have blocked the port due to a specific violation.
Recovery Time	The recovery time for the port. Configured through the **interfaces violation-recovery-time** command.
Recovery Max	The maximum recovery attempts for the port Configured through the **interfaces violation-recovery-maximum** command.
WTR (sec)	The wait-to-restore timer value, in seconds, for the port. The value of 0 indicates the timer is disabled. Configured through the **interfaces wait-to-restore** command.
Alias	Interface alias. Configured through the **interfaces alias** command.

Release History

Release 6.1; command was introduced.
Release 6.4.4; **Recovery Time**, **Recovery Max**, **WTR (sec)** fields were added.

Related Commands

show interfaces port	Displays interface port status (up or down) for non-combo ports.
show interfaces violation-recovery	Displays the globally configured recovery time, SNMP recovery trap enable/disable status and maximum recovery attempts.

MIB Objects

```
esmConfTable
   esmPortSlot
   esmPortIF
   esmPortViolationBitMap
   esmWaitToRestoreTimer
ifXTable
   ifAdminStatus
   ifOperStatus
   ifAlias
alaPortViolationRecoveryTable
   alaPortViolationRecoveryTime
   alaPortViolationRecoveryMaximum
```

show interfaces hybrid flood rate

Displays interface peak flood rate settings for combo ports.

show interfaces [*slot* | *slot*/*port***[-***port2***]] hybrid {fiber |copper} flood rate**

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
fiber	Specifies that the status of the SFP port(s) will be displayed.
copper	Specifies that the status of the copper 10/100/1000 RJ-45 port(s) will be displayed.

Defaults

By default, information is displayed for all ports on all modules.

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- Enter a slot number to display information for all interfaces on a specific port.
- Enter a slot and port number or a range of port numbers to display information for a specific interface or a range of interfaces.

Examples

```
-> show interfaces hybrid copper flood rate

 Slot/  Bcast    Bcast   Bcast   Ucast    Ucast   Ucast    Mcast   Mcast   Mcast
 Port   Value     Type  Status   Value     Type  Status    Value    Type  Status

-----+----------+-----+-------+----------+-----+-------+----------+-----+-------
 1/21        496  mbps  enable        496  mbps  enable        496  mbps disable
 1/22        496  mbps  enable        496  mbps  enable        496  mbps disable
 1/23        496  mbps  enable        496  mbps  enable        496  mbps disable
 1/24         49  mbps  enable         49  mbps  enable         49  mbps disable
```

output definitions

Slot/Port	Interface slot and port numbers.
Bcast Value	The broadcast storm value based on the type.
Bcast Type	The type of broadcast (**mbps**, **pps**, **percentage**).
Bcast Status	The status of brodcast, **enable** or **disable**.

output definitions (continued)

Ucast Value	The unknown-unicast storm value based on the type.
Ucast Type	The type of unknown-unicast (**mbps**, **pps**, **percentage**)
Ucast Status	The status of unicast, **enable** or **disable**.
Mcast Value	The multicast storm value based on the type.
Mcast Type	The type of multicast (**mbps**, **pps**, **percentage**)
Mcast Status	The status of multicast, **enable** or **disable**.

Release History

Release 6.1; command was introduced.

Related Commands

interfaces violation-recovery-trap	Configures the peak flood rate for an interface.
interfaces flood	Enables broadcast, multicast or unknown unicast traffic storm control on the specified interface.

MIB Objects

```
esmConfTable
   esmPortSlot
   esmPortIF
   esmPortMaxFloodRate
   esmPortFloodMcastEnable
```

show interfaces hybrid ifg

Displays interface inter-frame gap values for combo ports.

show interfaces [*slot* | *slot/port***[-***port2***]] hybrid {fiber |copper} ifg**

Syntax Definitions

slot	The slot number for a specific module.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).
fiber	Specifies that statistics for the SFP port(s) will be displayed.
copper	Specifies that statistics for the copper 10/100/1000 RJ-45 port(s) will be displayed.

Defaults

By default, information is displayed for all ports on all modules.

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- Enter a slot number to display information for all interfaces on a specific port.
- Enter a slot and port number or a range of port numbers to display information for a specific interface or a range of interfaces.

Examples

```
-> show interfaces hybrid fiber ifg
 Slot/Port   ifg(Bytes)
-----------+-------------
  1/45          12
  1/46          12
  1/47          12
  1/48          12
  2/45          12
  2/46          12
  2/47          12
  2/48          12
```

output definitions

Slot/Port	Interface slot and port numbers.
ifg	Inter-frame gap value (Gigabit Ethernet interface).

Release History

Release 6.1; command was introduced.

Related Commands

interfaces ifg	Configures the inter-frame gap value.

MIB Objects

```
esmConfTable
   esmPortSlot
   esmPortIF
   esmPortCfgIFG
```

show interfaces link-monitoring config

Displays configuration information for the Link Monitoring feature. This includes the link monitoring status on a specific slot, port or a range of specified ports, time window, link flap threshold, and link error threshold.

show interfaces {*slot* | *slot/port***[-***port2***]} link-monitoring config**

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Enter a slot number to display information for all interfaces on a specific port.
- Enter a slot and port number or a range of port numbers to display information for a specific interface or a range of interfaces.

Example

```
-> show interfaces 1 link-monitoring config

Slot/   Status   Time     Link-flap    Link-error
Port             Window   Threshold    Threshold
                 (sec)
------+--------+--------+------------+-----------
1/1    enabled     10        5           10
1/2    disabled    10        5           10
1/3    disabled   200        8           20
.
.
1/24   disabled   150        2           99


-> show interfaces 1/1-3 link-monitoring config

Slot/   Status   Time      Link-flap    Link-error
Port             Window    Threshold    Threshold
                 (sec)
------+--------+--------+------------+-------------
1/1    enabled     10         5            10
1/2    disabled    10         5            10
1/3    disabled   200         7            99
```

```
-> show interfaces 1/1 link-monitoring config

Slot/   Status    Time     Link-flap    Link-error
Port              Window   Threshold    Threshold
                  (sec)
------+--------+--------+------------+-------------
1/1    enabled     10          5           10

-> show interfaces 1/2 link-monitoring config

Slot/   Status    Time     Link-flap    Link-error
Port              Window   Threshold    Threshold
                  (sec)
------+--------+--------+------------+------------
1/2    disabled    10         5            10
```

Release History

output definitions

Slot/Port	Interface slot and port number.
Status	Link monitoring status (enable/disable).
Time Window	Time interval, in seconds, for which the link is monitored.
Link-flap threshold	Number of link flaps allowed on a specific slot, port, or a range of specified ports in the time interval before the port is shutdown.
Link-error threshold	Number of MAC errors allowed on a specific slot, port, or a range of specified ports in the time interval before the port is shutdown.

Release 6.4.4; command introduced.

Related Commands

show interfaces port	Displays information of the interface port status.
show interfaces link-monitoring statistics	Displays the Link Monitoring statistics.
interfaces link-monitoring admin-status	Enables or disables link monitoring.
interfaces link-monitoring time-window	Configures the monitoring of the time-window of the link.
interfaces link-monitoring link-flap-threshold	Configures the number of link flaps that are allowed before the port is shutdown.
interfaces link-monitoring link-error-threshold	Configures the number of MAC errors that are allowed before the port is shutdown.

MIB Objects

```
alaLinkMonStatsTable
   alaLinkMonStatus
   alaLinkMonTimeWindow
   alaLinkMonLinkFlapThreshold
   alaLinkMonLinkErrorThreshold
```

show interfaces link-monitoring statistics

Displays the Link Monitoring statistics for a specific slot, port, or a range of specified ports.

show interfaces {*slot* | *slot/port***[-***port2***]} link-monitoring statistics**

Syntax Definitions

slot	The slot number for a specific module.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Enter a slot number to display information for all interfaces on a specific port.
- Enter a slot and port number or a range of port numbers to display information for a specific interface or a range of interfaces.

Example

```
-> show interfaces 1 link-monitoring statistics
Slot/   State     Current  Current  Current   Current  Current  Total  Total
Port              Flap     Error    CRC       Lost     Align    Flap   Error
------+---------+--------+--------+--------+--------+--------+-------+-------+
1/1     shutdown    6       3         2         0         0       15      6
1/2     down        3       2         1         0         0       12      3
.
.
1/24     up         3       2         1          0        0       12      3

-> show interfaces 1/1-2 link-monitoring statistics
Slot/   State     Current  Current  Current   Current  Current  Total  Total
Port              Flap     Error    CRC       Lost     Align    Flap   Error
------+---------+--------+--------+--------+--------+--------+-------+-------+
1/1     shutdown    6       3         2         0         0       15      6
1/2     down        3       2         1         0         0       12      3

-> show interfaces 1/1 link-monitoring statistics
Slot/   State     Current  Current  Current   Current  Current  Total  Total
Port              Flap     Error    CRC       Lost     Align    Flap   Error
------+---------+--------+--------+--------+--------+--------+-------+-------+
1/1     shutdown    6       3         2         0         0       15      6
```

Release History

Release 6.4.4; command introduced.

Related Commands

show interfaces port	Displays the administrative, operational, violation, and recovery status and configuration for the specified port.
show interfaces link-monitoring config	Displays configuration information of the Link Monitoring.
interfaces link-monitoring admin-status	Enables or disables link monitoring.
interfaces clear-link-monitoring-stats	Clears the Link Monitoring statistics.
interfaces link-monitoring link-error-threshold	Configures the number of MAC errors that are allowed before the port is shutdown.

MIB Objects

```
alaLinkMonStatsTable
   alaLinkMonStatsPortStatus
   alaLinkMonStatsCurrentLinkFlaps
   alaLinkMonStatsCurrentErrorFrames
   alaLinkMonStatsCurrentCRCErrors
   alaLinkMonStatsCurrentLostFrames
   alaLinkMonStatsCurrentAlignErrors
   alaLinkMonStatsCurrentLinkErrors
   alaLinkMonStatsTotalLinkFlaps
   alaLinkMonStatsTotalLinkErrors
```

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.
enable	Enables fabric backpressure.
disable	Disables fabric backpressure.

Defaults

By default, the fabric backpressure is disabled.

Platforms Supported

OmniSwitch 6400

Usage Guidelines

If the slot number is not specified, then the switch back pressure feature will be enabled or disabled on the 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 6.1; command was introduced.

Related Commands

debug interfaces backpressure	Displays whether fabric back pressure is enabled or disabled on an NI or an entire chassis.

MIB Objects

N/A

debug interfaces backpressure

Displays whether fabric back pressure is enabled or disabled on a Network Interface (NI) or on the entire chassis.

debug interfaces [*slot*] backpressure

Syntax Definitions

slot	The slot number to display the fabric back pressure state.

Defaults

N/A

Platforms Supported

OmniSwitch 6400

Usage Guidelines

If the slot number is not specified, then the switch back pressure state is displayed for the 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 6.1; command was introduced.

Related Commands

debug interfaces backpressure	Enables and disables fabric back pressure on an NI or on the entire chassis.

MIB Objects

N/A

link-fault-propagation group

Configures a Link Fault Propagation (LFP) group to associate with source and destination ports.

link-fault-propagation group *group_id* **[admin-state {enable | disable}]**

no link-fault-propagation group {*group_id***[-***group_id2***]}**

Syntax Definitions

group_id	A group ID number. The valid range is 1–8.
*group_id***[-***group_id2***]**	A group ID number to remove. Use a hyphen to specify a range of existing group ID numbers (5-8). Specifying a range is only used to remove group IDs, not to create them.
enable	Enables LFP for the specified group.
disable	Disables LFP for the specified group.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a LFP group or a range of groups.
- Up to eight LFP groups per switch are allowed.
- Once a LFP group is created, assign source and destination ports to that group.

Example

```
-> link-fault-propagation group 1
-> no link-fault-propagation group 4
-> no link-fault-propagation group 4-7
```

Release History

Release 6.4.4; command introduced.

Related Commands

link-fault-propagation group source	Configures the source port assignments for the LFP group.
link-fault-propagation group destination	Configures the destination port assignments for the LFP group.
link-fault-propagation group wait-to-shutdown	Configures the amount of time LFP waits before shutting down the destination ports.
show link-fault-propagation group	Displays the LFP group configuration for the switch.

MIB Objects

```
alaLFPGroupTable
   alaLFPGroupId
   alaLFPGroupRowStatus
```

link-fault-propagation group source

Configures the source port assignments for a Link Fault Propagation (LFP) group.

link-fault-propagation group *group_id* **source {port** *slot/port***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]}**

no link-fault-propagation group *group_id* **source {port** *slot/port***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]}**

Syntax Definitions

group_id	An existing LFP group ID number. The valid range is 1–8.
*slot/port***[**-*port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports and/or a space to specify multiple port entries (3/1-10 4/1 4/5 5/10).
agg_i*d***[**-*agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs and/or a space to specify multiple ID entries (1-5 10 12).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a source port association with the specified LFP group.
- Make sure the LFP group specified with this command already exists in the switch configuration.
- Configuring the source ports and destinations ports for the specified LFP group is allowed within the same command (see the examples on this command page).
- A group can have a maximum of 48 source ports and 48 destination ports.
- A maximum of 48 link aggregates is supported, regardless of the number of ports in each aggregate in a group.
- A port/linkagg added as a source/destination port for a particular group cannot be added as a destination/source port for this group or for any other group.
- If a port is recovered due to the Interface Recovery Timer, then the port will revert to the shutdown state if the error persists.

Example

```
-> link-fault-propagation group 1 source port 1/2
-> link-fault-propagation group 1 source port 1/2-5 2/3
-> link-fault-propagation group 1 source linkagg 1
-> link-fault-propagation group 1 source linkagg 1-3
-> link-fault-propagation group 1 source port 2/3 destination port 1/6
-> link-fault-propagation group 1 source port 3/1-5 destination linkagg 6
-> no link-fault-propagation group 1 destination port 1/10
```

Release History

Release 6.4.4; command introduced.

Related Commands

link-fault-propagation group	Configures an LFP group, including the administrative status.
link-fault-propagation group destination	Configures the destination port assignments for the LFP group.
link-fault-propagation group wait-to-shutdown	Configures the amount of time LFP waits before shutting down the destination ports.
show link-fault-propagation group	Displays the LFP group configuration for the switch.

MIB Objects

```
alaLFPGroupTable
   alaLFPGroupId
   alaLFPGroupRowStatus
   alaLFPConfigTable
      alaLFPConfigPort
      alaLFPConfigPortType
      alaLFPConfigRowStatus
```

link-fault-propagation group destination

Configures the destination port assignments for a Link Fault Propagation (LFP) group.

link-fault-propagation group *group_id* **destination {port** *slot/port[-port2]* **| linkagg** *agg_id[-agg_id2]***}**

no link-fault-propagation group *group_id* **destination {port** *slot/port[-port2]* **| linkagg** *agg_id[-agg_id2]***}**

Syntax Definitions

group_id	An existing LFP group ID number. The valid range is 1–8.
slot/port[-port2]	The slot and port number (3/1). Use a hyphen to specify a range of ports and/or a space to specify multiple port entries (3/1-10 4/1 4/5 5/10).
agg_id[-agg_id2]	The link aggregate ID number. Use a hyphen to specify a range of IDs and/or a space to specify multiple ID entries (1-5 10 12).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a destination port association with the specified LFP group.
- Make sure the LFP group specified with this command already exists in the switch configuration.
- Configuring the source ports and destinations ports for the specified LFP group is allowed within the same command (see the examples on this command page).
- A group can have a maximum of 48 source ports and 48 destination ports.
- A maximum of 48 link aggregates is supported regardless of the number of ports in each aggregate in a group.
- A port or link aggregate that is configured as a source port cannot be configured as a destination port for any group. However, a source port can be associated with multiple LFP groups.
- A port or link aggregate that is configured as a destination port cannot be configured as a source port for any group. However, a destination port can be associated with multiple LFP groups.
- If port is recovered due to the Interface Recovery Timer, then the port will revert to the shutdown state if the error persists.

Example

```
-> link-fault-propagation group 1 destination port 1/4
-> link-fault-propagation group 1 destination port 1/5-8 2/3
-> link-fault-propagation group 1 destination linkagg 6
-> link-fault-propagation group 1 destination linkagg 6-10
-> link-fault-propagation group 1 source port 1/2 2/3 destination port 1/6
-> link-fault-propagation group 1 source port 1/2 2/3 destination linkagg 6
-> link-fault-propagation group 1 source linkagg 3 destination port 1/6 1/9
-> link-fault-propagation group 1 source linkagg 3 destination linkagg 1

-> no link-fault-propagation group 1 source port 1/9
-> no link-fault-propagation group 1 destination port 1/10
```

Release History

Release 6.4.4; command introduced.

Related Commands

link-fault-propagation group	Configures an LFP group, including the administrative status.
link-fault-propagation group source	Configures the source port assignments for the LFP group.
link-fault-propagation group wait-to-shutdown	Configures the amount of time LFP waits before shutting down the destination ports.
show link-fault-propagation group	Displays the LFP group configuration for the switch.

MIB Objects

```
alaLFPGroupTable
   alaLFPGroupId
   alaLFPGroupRowStatus
   alaLFPConfigTable
      alaLFPConfigPort
      alaLFPConfigPortType
      alaLFPConfigRowStatus
```

link-fault-propagation group wait-to-shutdown

Configures the wait-to-shutdown timer value for the Link Fault Propagation (LFP) group. This is the amount of time after all the source ports go down that LFP waits before shutting down the destination ports.

link-fault-propagation group *group_id* **wait-to-shutdown** *seconds*

Syntax Definitions

group_id	An existing LFP group ID number. The valid range is 1–8.
seconds	The number of seconds LFP waits before shutting down the destination ports. The valid range is 0-300 in multiples of 5.

Defaults

By default, the timer is set to zero (disabled).

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Set the wait-to-shutdown timer value to 0 to disable the timer.
- Make sure the LFP group specified with this command already exists in the switch configuration.

Example

```
-> link-fault-propagation group 1 wait-to-shutdown 40
-> link-fault-propagation group 3 wait-to-shutdown 70
-> link-fault-propagation group 5 wait-to-shutdown 0
```

Release History

Release 6.4.4; command introduced.

Related Commands

link-fault-propagation group	Configures an LFP group, including the administrative status.
show link-fault-propagation group	Displays the LFP group configuration for the switch.

MIB Objects

```
alaLFPGroupTable
   alaLFPGroupId
   alaLFPGroupWaitToShutdown
   alaLFPGroupRowStatus
```

show link-fault-propagation group

Displays information for the specified Link Fault Propagation (LFP) group.

show link-fault-propagation group [*group_id***]**

Syntax Definitions

group_id	An existing LFP group ID number. The valid range is 1–8.

Defaults

By default, information is displayed for all existing LFP groups.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Enter a LFP group ID number with this command to display information for a specific group.

Example

```
-> show link-fault-propagation group
Group Id : 2
  Source Port(s)          : 0/1-2 1/1-5 1/7,
  Destination Port(s)     : 0/3 1/10-13,
  Group-Src-Ports Status  : up,
  Admin Status            : enable,
  Wait To Shutdown        : 10

Group Id : 6
  Source Port(s)          : 1/2 1/6 1/9,
  Destination Port(s)     : 1/10-11 1/13,
  Group-Src-Ports Status  : down,
  Admin Status            : disable,
  Wait To Shutdown        : 5

Group Id : 7
  Source Port(s)          : 1/1 1/3,
  Destination Port(s)     : 0/3 1/5 1/7 1/11 1/13 1/15 1/17 1/19 1/21 1/23,
  Group-Src-Ports Status  : up,
  Admin Status            : enable,
  Wait To Shutdown        : 100

-> show link-fault-propagation group 2
Group Id : 2
  Source Port(s)          : 0/1-2 1/1-5 1/7,
  Destination Port(s)     : 0/3 1/10-13,
  Group-Src-Ports Status  : up,
  Admin Status            : enable,
  Wait To Shutdown        : 10
```

```
-> show link-fault-propagation group 6
Group Id : 6
  Source Port(s)          : 1/2 1/6 1/9,
  Destination Port(s)     : 1/10-11 1/13,
  Group-Src-Ports Status  : down,
  Admin Status            : enable,
  Wait To Shutdown        : 5
```

Release History

Release 6.4.4; command introduced.

Related Commands

link-fault-propagation group	Configures a LFP group, including the administrative status.
link-fault-propagation group wait-to-shutdown	Configures the amount of time LFP waits before shutting down the destination ports.

MIB Objects

```
alaLFPConfigTable
   alaLFPConfigPort
   alaLFPConfigPortType
alaLFPGroupTable
   alaLFPGroupId
      alaLFPGroupAdminStatus
      alaLFPGroupOperStatus
      alaLFPGroupWaitToShutdown
```

interfaces tdr-test-start

Initiates a Time Domain Reflectometry (TDR) cable diagnostics test on the specified port. The TDR feature sends a signal down a cable to determine the distance to a break or other discontinuity in the cable path. The length of time it takes for the signal to reach the break and return is used to estimate the distance to the discontinuity.

interfaces *slot/port* **tdr-test-start**

Syntax Definitions

slot/port	The slot and port number (3/1).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- TDR is an on-demand, out-of-service test. The test is not automatically triggered; data and protocol traffic is interrupted.
- Only one TDR test can be run at any given time.
- TDR is not supported on link aggregate ports, fiber ports, or stacking ports.
- TDR results are automatically cleared when a new test is started on the port or when the module for the port is reset.

Examples

```
-> interfaces 1/1 tdr-test-start
```

Release History

Release 6.4.4; command was introduced.

Related Commands

interfaces no tdr-statistics	Clears the statistics of the last test performed on the port
show interfaces tdr-statistics	Displays the results of the last TDR test performed on a port.

MIB Objects

```
esmTdrPortTable
   esmTdrPortTest
```

interfaces no tdr-statistics

Clears the statistics of the last TDR test performed on the port.

interfaces {*slot* | *slot/port***[-***port2***]} no tdr-statistics**

Syntax Definitions

slot	The slot number for a specific module.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

There is no global command to clear TDR statistics for all ports on all slots; statistics are cleared at the slot or the slot/port level.

Examples

```
-> interfaces 2/1 no tdr-statistics
-> interfaces 2 no tdr-statistics
-> interfaces 2/1-7 no tdr-statistics
```

Release History

Release 6.4.4; command was introduced.

Related Commands

interfaces tdr-test-start	Initiates the cable diagnostics on a port.
show interfaces tdr-statistics	Displays the results of the last TDR test performed on a port.

MIB Objects

```
esmTdrPortTable
   esmTdrPortClearResults
```

show interfaces tdr-statistics

Displays the results of the last TDR test performed on a port.

show interfaces [*slot* | *slot*/*port***[-***port2***]] tdr-statistics**

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-3/10).

Defaults

By default, TDR statistics are shown for all ports on all modules

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Enter a slot number to display information for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to display information for a specific interface or range of interfaces.

Examples

```
-> show interfaces 1/3 tdr-statistics
Legend: Pair 1 - orange and white
        Pair 2 - green and white
        Pair 3 - blue and white
        Pair 4 - brown and white

Slot/ No of Cable Fuzzy  Pair1 Pair1  Pair2 Pair2  Pair3 Pair3  Pair4 Pair4  Test
port  pairs State Length State Length State Length State Length State Length Result
-----+-----+------+-----+-----+-----+------+------+-----+------+-----+------+------
1/3    4     ok     0     ok     3     ok      3    ok      3     ok    3   success
```

output definitions

Legend	Eight-conductor data cable contains 4 pairs of twisted Pair Copper Cable wires. Each pair consists of a solid (or predominantly) colored wire and a white wire with a strip of the same color. The pairs are twisted together.
Slot/Port	The interface slot and port number.
No of pairs	The number of pairs in the cable for which the test results are valid.

output definitions (continued)

Cable State	State of a cable as returned by the TDR test. The state of the cable wire. (a) **OK** - Wire is working properly (b) **Open** - Wire is broken (c) S**hort** - Pairs of wire are in contact with each other (d) **Crosstalk** - Signal transmitted on one pair of wire creates an undesired effect in another wire. (e) **Unknown** - Cable diagnostic test unable to find the state of a cable.
Fuzzy Length	The error in the estimated length of the cable.
Pair1 State	The state of the Pair 1 cable wire (**OK**, **Open**, **Short**, **Crosstalk**, or **Unknown**)
Pair1 Length	The length of the Pair 1 cable at which the fault is detected, if the pair is faulty. Else, specifies the complete length of the cable.
Pair2 State	The state of the Pair 2 cable wire (**OK**, **Open**, **Short**, **Crosstalk**, or **Unknown**)
Pair2 Length	The length of the Pair 2 cable at which the fault is detected, if the pair is faulty. Else, specifies the complete length of the cable.
Pair3 State	The state of the Pair 3 cable wire (**OK**, **Open**, **Short**, **Crosstalk**, or **Unknown**)
Pair3 Length	The length of the Pair 3 cable at which the fault is detected, if the pair is faulty. Else, specifies the complete length of the cable.
Pair4 State	The state of the Pair 4 cable wire (**OK**, **Open**, **Short**, **Crosstalk**, or **Unknown**)
Pair4 Length	The length of the Pair 4 cable at which the fault is detected, if the pair is faulty. Else, specifies the complete length of the cable.
Test Result	The status of the TDR test performed, success or fail.

Release History

Release 6.4.4; command was introduced.

Related Commands

interfaces tdr-test-start	Initiates the cable diagnostics on a port.
interfaces no tdr-statistics	Clears the statistics of the last test performed on the port.

MIB Objects

```
esmTdrPortTable
   esmTdrPortCableState
   esmTdrPortValidPairs
   esmTdrPortPair1State
   esmTdrPortPair1Length
   esmTdrPortPair2State
   esmTdrPortPair2Length
   esmTdrPortPair3State
   esmTdrPortPair3Length
   esmTdrPortPair4State
   esmTdrPortPair4Length
   esmTdrPortFuzzLength
```

2 UDLD Commands

This chapter describes the CLI commands used to configure the UDLD (UniDirectional Link Detection) protocol. UDLD operates at Layer 2 in conjunction with IEEE 802.3 Layer 1 fault detection mechanism. It is a protocol used for detecting and disabling unidirectional Ethernet fiber or copper connections to avoid interface malfunctions, Spanning Tree loops, media faults, etc. It operates in two main modes normal and aggressive.

The two basic mechanisms that UDLD follows are:

- Advertises port's identity and learns about its neighbors. This information is maintained in a cache table.
- It sends continuous echo messages when fast notifications are required.

MIB information for the UDLD commands is as follows:

Filename: AlcatelIND1UDLD.mib
Module: ALCATEL-IND1-UDLD-MIB

A summary of available commands is listed here:

udld
udld port
udld mode
udld probe-timer
udld echo-wait-timer
clear udld statistics port
interfaces clear-violation-all
show udld configuration
show udld configuration port
show udld statistics port
show udld neighbor port
show udld status port

Configuration procedures for UDLD are explained in the “Configuring UDLD” chapter of the *OmniSwitch AOS Release 6 Network Configuration Guide*.

udld

Globally enables or disables UDLD protocol on the switch.

udld {enable | disable}

Syntax Definitions

enable	Globally enables UDLD on the switch.
disable	Globally disables UDLD on the switch.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

The port that is shutdown by this command can be reset by using the **interfaces admin** command.

Examples

```
-> udld enable
-> udld disable
```

Release History

Release 6.3.1; command was introduced.

Related Commands

udld port	Enables or disables UDLD status on a specific port or a range of ports.
show udld configuration	Displays the global status of UDLD configuration.
show udld configuration port	Displays the configuration information for all UDLD ports or for a particular UDLD port on the switch.

MIB Objects

```
alaUdldGlobalStatus
```

udld port

Enables or disables UDLD status on a specific port or a range of ports.

udld port *slot/port***[-***port2***] {enable | disable}**

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
port2	The last port number in a range of ports that you want to configure on the same slot (for example, 3/1-4 specifies ports 1-4 on slot 3).
enable	Enables UDLD status on a port.
disable	Disables UDLD status on a port.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- The UDLD protocol must be enabled before using this command.
- If the slot/port is a VFL member port, an error message is displayed indicating that the DLD configuration is not allowed on VFL member port.

Examples

```
-> udld port 1/3 enable
-> udld port 1/6-10 enable
-> udld port 2/4 disable
Error Message: UDLD configuration is not allowed on VFL member port.
```

Release History

Release 6.3.1; command was introduced.

Related Commands

udld	Globally enables or disables UDLD protocol on the switch.
show udld configuration port	Displays the configuration information for all UDLD ports or for a particular UDLD port on the switch.

MIB Objects

```
alaUdldPortConfigTable
   alaUdldConfigUdldStatus
```

udld mode

Configures the operational mode of UDLD on a specific port, a range of ports, or all the ports.

udld port [*slot/port***[-***port2***]] mode {normal | aggressive}**

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
port2	The last port number in a range of ports that you want to configure on the same slot (for example, 3/1-4 specifies ports 1-4 on slot 3).
normal	Specifies UDLD operation in the normal mode.
aggressive	Specifies UDLD operation in the aggressive mode.

Defaults

parameter	default
normal | aggressive	**normal**

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- The UDLD protocol must be enabled before using this command.
- The UDLD protocol is not supported on aggregate ports.
- When two UDLD enabled ports that are configured in aggressive mode gets the link-up asynchronously, then the UDLD port which gets the link-up indication first is considered to be in the shutdown state. In such case, the link should be configured manually after both the links are up to start UDLD detection.
- In case of faulty cable connection, the port which is configured in normal mode of operation is determined to be in the shutdown state.

Examples

```
-> udld mode aggressive
-> udld mode normal
-> udld port 1/3 mode aggressive
-> udld port 2/4 mode normal
-> udld port 2/9-18 mode aggressive
```

Release History

Release 6.3.1; command was introduced.

Related Commands

udld	Globally enables or disables UDLD protocol on the switch.
show udld configuration port	Displays the configuration information for all UDLD ports or for a particular UDLD port on the switch.

MIB Objects

```
alaUdldPortConfigTable
   alaUdldPortConfigUdldMode
```

udld probe-timer

Configures the probe-message advertisement timer on a specific port, a range of ports, or all the ports. Probe-messages are transmitted periodically after this timer expires.

udld port [*slot/port***[-***port2***]] probe-timer** *seconds*

no udld port [*slot/port***[-***port2***]] probe-timer**

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
port2	The last port number in a range of ports that you want to configure on the same slot (for example, 3/1-4 specifies ports 1-4 on slot 3).
seconds	The probe-message transmission interval. Valid range is 7 seconds to 90 seconds.

Defaults

parameter	default
seconds	15

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to reset the probe-message timer to the default value. Note that it is not necessary to specify the probe-message interval to reset it.
- The UDLD protocol must be enabled before using this command.
- Configure probe-advertisement timer with values varying in a range of 12 seconds to 18 seconds for better convergence time and to avoid burst of probe advertisements.

Examples

```
-> udld probe-timer 20
-> udld port 1/3 probe-timer 16
-> udld port 1/8-21 probe-timer 18
-> no udld probe-timer
-> no udld port 1/3 probe-timer
```

Release History

Release 6.3.1; command was introduced.

Related Commands

udld	Globally enables or disables UDLD protocol on the switch.
show udld configuration port	Displays the configuration information for all UDLD ports or for a particular UDLD port on the switch.

MIB Objects

```
alaUdldPortConfigTable
   alaUdldPortConfigUdldProbeIntervalTimer
```

udld echo-wait-timer

Configures the echo based detection timer on a specific port, a range of ports, or all the ports. This is known as link detection period.

udld port [*slot/port***[-***port2***]] echo-wait-timer** *seconds*

no udld port [*slot/port***[-***port2***]] echo-wait-timer**

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
port2	The last port number in a range of ports that you want to configure on the same slot (for example, 3/1-4 specifies ports 1-4 on slot 3).
seconds	The echo based detection period. Valid range is 4 seconds to 15 seconds.

Defaults

parameter	default
seconds	8

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to reset the echo based detection timer to the default value. Note that it is not necessary to specify the echo based timer to reset it.
- The UDLD protocol must be enabled before using this command.
- An echo message is expected in reply from the neighbor within this time duration, otherwise, the port is considered as faulty.

Examples

```
-> udld echo-wait-timer 9
-> udld port 1/5 echo-wait-timer 12
-> udld port 1/7-16 echo-wait-timer 12
-> no udld echo-wait-timer
-> no udld port 1/3 echo-wait-timer
```

Release History

Release 6.3.1; command was introduced.

Related Commands

udld	Globally enables or disables UDLD protocol on the switch.
show udld configuration port	Displays the configuration information for all UDLD ports or for a particular UDLD port on the switch.

MIB Objects

```
alaUdldPortConfigTable
   alaUdldPortConfigUdldDetectionPeriodTimer
```

clear udld statistics port

Clears the UDLD statistics for a specific port or for all the ports.

clear udld statistics [port *slot/port***]**

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

If the slot/port option is not specified, UDLD statistics for the switch is cleared.

Examples

```
-> clear udld statistics port 1/4
-> clear udld statistics
```

Release History

Release 6.3.1; command was introduced.

Related Commands

udld	Globally enables or disables UDLD protocol on the switch.
show udld statistics port	Displays the UDLD statistics for a specific port.

MIB Objects

```
alaUdldGlobalClearStats
```

interfaces clear-violation-all

Brings the port out of shutdown state.

interfaces *slot/port***[-***port2***] clear-violation-all**

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
port2	The last port number in a range of ports that you want to configure on the same slot (for example, 3/1-4 specifies ports 1-4 on slot 3).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- If any interface is in the admin down state because of UDLD, then the status of the interface can be confirmed using the **show interfaces port** command. The violation field indicates the reason of violation.
- The port may again go into shutdown state if the UDLD operation determine that UDLD violation is still not cleared.

Examples

```
-> interfaces 1/8 clear-violation-all
-> interfaces 1/10-14 clear-violation-all
```

Release History

Release 6.3.1; command was introduced.

Related Commands

show interfaces port	Displays interface port status (up or down).

MIB Objects

```
alaUdldPortStatsTable
   alaUdldPortStatsClear
```

show udld configuration

Displays the global status of UDLD configuration.

show udld configuration

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show udld configuration
Global UDLD Status : Disabled
```

output definitions

Global UDLD Status	Indicates the UDLD status on the switch. Options include **enabled** or **disabled**.

Release History

Release 6.3.1; command was introduced.

Related Commands

udld	Globally enables or disables UDLD protocol on the switch.
show udld configuration port	Displays the configuration information for all UDLD ports or for a particular UDLD port on the switch.

MIB Objects

```
alaUdldGlobalStatus
```

show udld configuration port

Displays the configuration information for all UDLD ports or for a particular UDLD port on the switch.

show udld configuration port [*slot/port***]**

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).

Defaults

By default, a list of all UDLD ports is displayed.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show udld configuration port
Slot/Port    Admin State    Oper Mode    Probe-Timer    Echo-Wait-Timer
-----------+--------------+------------+-------------+----------------
1/1           disabled       normal          15           10
1/2           disabled       normal          45           10
1/17          disabled       normal          33            8
1/18          disabled       normal          33            8
1/19          disabled       normal          33            8
1/20          disabled       aggresive       55            8
1/21          disabled       aggresive       55            8
1/22          disabled       aggresive       55            8
1/41          disabled       aggresive       77            8
1/42          enabled        aggresive       77            8
1/43          enabled        aggresive       77            8
1/44          enabled        aggresive       77            8
1/45          enabled        aggresive       77            8

 -> show udld configuration port 1/44
Global UDLD Status            : enabled,
Port UDLD Status              : enabled,
Port UDLD State               : bidirectional,
UDLD Op-Mode                  : aggresive,
Probe Timer (Sec)             : 77,
Echo-Wait Timer (sec)         : 8
```

output definitions

Slot/Port	Slot number for the module and physical port number on that module.
UDLD-State	Indicates the state of interface determined by UDLD operation, which can be **notapplicable, shutdown, undetermined,** or **bidirectional**.
Oper-Mode	Indicates the operational mode of UDLD protocol. Options include **normal** or **aggressive**.
Global UDLD Status	Indicates the UDLD status on the switch. Options include **enabled** or **disabled**.
Port UDLD Status	Indicates the UDLD status on a port. Options include **enable** or **disable**.
Probe Timer	The probe-message expected after this time period.
Echo-Wait Timer	The detection of neighbor is expected with in this time period.

Release History

Release 6.3.1; command was introduced.

Related Commands

udld mode	Configures the operational mode of UDLD on a specific port, a range of ports, or all the ports.
udld probe-timer	Configures the probe-message advertisement timer on a specific port, a range of ports, or all the ports.
udld echo-wait-timer	Configures the echo based detection timer on a specific port, a range of ports, or all the ports.

MIB Objects

```
   alaUdldGlobalStatus
alaUdldPortConfigTable
   alaUdldPortConfigUdldOperationalStatus
   alaUdldPortConfigUdldMode
   alaUdldPortConfigUdldStatus
   alaUdldPortConfigUdldProbeintervalTimer
   alaUdldPortConfigUdldDetectionPeriodTimer
alaUdldPortNeighborStatsTable
   alaUdldNeighborName
```

show udld statistics port

Displays the UDLD statistics for a specific port.

show udld statistics port *slot/port*

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show udld statistics port 1/42
UDLD Port Statistics
 Hello Packet Send        :8,
 Echo Packet Send         :8,
 Flush Packet Recvd       :0
UDLD Neighbor Statistics
 Neighbor ID    Hello Pkts Recv       Echo Pkts Recv
--------------+--------------------+--------------
      1              8              15
      2              8              15
      3              8              21
      4              8              14
      5              8              15
      6              8              20
```

output definitions

Hello Packet Send	The number of hello messages sent by a port.
Echo Packet Send	The number of echo messages sent by a port.
Flush Packet Recvd	The number of UDLD-Flush message received by a port.
Neighbor ID	The name of the neighbor.
Hello Pkts Recv	The number of hello messages received from the neighbor.
Echo Pkts Recv	The number of echo messages received from the neighbor.

Release History

Release 6.3.1; command was introduced.

Related Commands

udld probe-timer	Configures the probe-message advertisement timer on a specific port, a range of ports, or all the ports.
udld echo-wait-timer	Configures the echo based detection timer on a specific port, a range of ports, or all the ports.

MIB Objects

```
alaUdldPortNeighborStatsTable
   alaUdldNeighborName
   alaUdldNumHelloSent
   alaUdldNumHelloRcvd
   alaUdldNumEchoSent
   alaUdldNumEchoRcvd
   alaUdldNumFlushRcvd
```

show udld neighbor port

Displays the UDLD neighbor ports.

show udld neighbor port *slot/port*

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show udld neighbor port 1/42
 Neighbor ID           Device Id             Port Id
-----------------+--------------------+---------------
      1            00:d0:95:ea:b2:48         00:d0:95:ea:b2:78
      2            00:d0:95:ea:b2:48         00:d0:95:ea:b2:79
      3            00:d0:95:ea:b2:48         00:d0:95:ea:b2:74
      4            00:d0:95:ea:b2:48         00:d0:95:ea:b2:75
      5            00:d0:95:ea:b2:48         00:d0:95:ea:b2:76
      6            00:d0:95:ea:b2:48         00:d0:95:ea:b2:77
```

output definitions

Neighbor ID	The name of the neighbor.
Device ID	The device ID.
Port ID	The port ID.

Release History

Release 6.3.1; command was introduced.

Related Commands

udld echo-wait-timer	Configures the echo based detection timer on a specific port, a range of ports, or all the ports. This is known as link detection period.
show udld statistics port	Displays the UDLD statistics for a specific port.

MIB Objects

```
alaUdldPortNeighborStatsTable
   alaUdldNeighborName
```

show udld status port

Displays the UDLD status for all ports or for a specific port.

show udld status port [*slot/port***]**

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).

Defaults

By default, a list of all UDLD ports is displayed.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show udld status port
  Slot/Port        Admin State        Operational State
-------------+------------------+-----------------------
    1/1             disabled           not applicable
    1/2             disabled           not applicable
    1/3             disabled           not applicable
    1/21            disabled           not applicable
    1/40            disabled           not applicable
    1/41            disabled           not applicable
    1/42            enabled            bidirectional
    1/43            enabled            bidirectional
    1/44            enabled            bidirectional
    1/45            enabled            bidirectional
    1/46            enabled            bidirectional
    1/47            enabled            bidirectional
    1/48            enabled            bidirectional

-> show udld status port 1/44
Admin State              : enabled,
Operational State        : bidirectional
```

output definitions

Slot/Port	Slot number for the module and physical port number on that module.
Admin State	Indicates whether UDLD is administratively **enabled** or **disabled**.
Operational State	Indicates the state of interface determined by UDLD operation, which can be **notapplicable, shutdown, undetermined,** or **bidirectional**.

Release History

Release 6.3.1; command was introduced.

Related Commands

udld port	Enables or disables UDLD status on a specific port or a range of ports.
show udld configuration port	Displays the configuration information for all UDLD ports or for a particular UDLD port on the switch.

MIB Objects

```
   alaUdldGlobalStatus
alaUdldPortConfigTable
   alaUdldPortConfigUdldOperationalStatus
```

3 Power over Ethernet (PoE) Commands

The Power over Ethernet (PoE) feature is supported on OmniSwitch chassis-based switches using PoE-capable Ethernet modules and a peripheral power shelf as well as on OmniSwitch PoE capable switches. Refer to the *OmniSwitch Hardware Users Guide* for further 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 AOS Release 6 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 such as OmniSwitch chassis-based switches with PoE modules or OmniSwitch PoE capable switches.

PoE commands documented in this section comply with IEEE 802.3, 802.af, and pre-802.3at.

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 slot-priority
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***[-***port2***] |** *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.
port2	The last port number in a range of ports that you want to configure on the same slot (e.g, 3/1-4 specifies ports 1-4 on slot 3).
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 6400, 6855, 6850E, 9000E

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
-> lanpower start 5/11-14
```

Release History

Release 6.1; 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***[-***port2***] | *slot***}**

Syntax Definitions

slot/port	Disables inline power on the specified PoE port only.
port2	The last port number in a range of ports that you want to configure on the same slot (e.g, 3/1-4 specifies ports 1-4 on slot 3).
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 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> lanpower stop 5/22
-> lanpower stop 5
-> lanpower stop 5/22-27
```

Release History

Release 6.1; 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, available 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 configured.
milliwatts	The maximum amount of inline power, in milliwatts, being made available to the corresponding port. Refer to the *OmniSwitch Hardware Users Guide* PoE specifications.

Defaults

parameter	default	Range
milliwatts (OS6400)	15400	3000-18000
milliwatts (OS6855)	15400	3000-20000
milliwatts (OS6850E/OS9000E)	30000	3000-30000

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Using this command does not immediately allocate the power to the slot or port. Any unused power is still available and remains a part of the overall PoE budget.
- To globally specify the amount of inline power available to *all ports in a slot*, refer to the **lanpower maxpower** command on page 3-8.
- 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 6.1; command was introduced.

Related Commands

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

lanpower *slot* **maxpower** *watts*

Syntax Definitions

slot	The slot containing PoE ports on which the maximum amount of inline power allowed is being configured.
watts	The maximum amount of inline power, in watts, available to all PoE ports in the corresponding slot. Refer to the *OmniSwitch Hardware Users Guide* for additional PoE specifications.

Defaults

parameter	default
900W Power Supply	780W
510W Power Supply	390W
360W Power Supply	240W
OS6855-14/P14	66W/185W
OS6855-24	80W
OS9000E	720W

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- To specify the maximum amount of inline power available to a *single port*, refer to the **lanpower power** command on page 3-6.
- 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 6.1; command was introduced.

Related Commands

lanpower power	Specifies the maximum amount of inline power, in milli-watts, available 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 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

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

Release History

Release 6.1; 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 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 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 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

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

Release History

Release 6.1; 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 slot-priority

Configures an inline power priority level for a slot. If the power supply of the power shelf goes down, the order of a particular daughter module will be disabled based on priority, thus affecting the power budget available to the whole chassis. Levels include critical, high, and low.

lanpower *slot* **slot-priority {critical | high | low}**

Syntax Definitions

slot	The particular slot on which a priority level is being configured.
critical	Intended for slots 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 slots 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 slots 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 9000E

Usage Guidelines

- Note that if all the POE NI modules are all configured with the same priority level, then priority is determined based on the slot number of the module; the lower the slot number the higher the priority. For example, if slots 1, 2, 7, and 8 are powered by two POE power supplies and one of the power supplies goes down, power is cut to slots 7 and 8 because they have a lower priority than slots 1 and 2.

Examples

```
-> lanpower 1 slot-priority critical
-> lanpower 2 slot-priority high
-> lanpower 3 slot-priority low
```

Release History

Release 6.1.3; command was introduced.

Related Commands

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.

MIB Objects

```
alaPethMainPseTable
   alaPethMainPsePriority
```

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 9000E

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 Hardware Users Guide*.

Examples

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

Release History

Release 6.1.3; 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 the capacitor detection method.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

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 specifications. Please contact your Alcatel-Lucent sales engineer or Customer Support representative to find out which Alcatel-Lucent IP phones models need capacitive detection enabled.

Examples

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

Release History

Release 6.1; 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 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show lanpower 1
Port Maximum(mW) Actual Used(mW)   Status    Priority  On/Off   Class
----+-----------+---------------+-----------+---------+-------+-----------
 1     31000        7000         Powered On    Critical  ON        0
 2     31000        20000        Powered On    Critical  ON        4
 3     15400        7000         Powered On    Low       ON        3
 .....

 42     18000            0       Undefined      Low      OFF      -
 43     18000            0       Undefined      Low      OFF      -
 44     18000            0       Undefined      Low      OFF      -
 45     18000            0       Undefined      Low      OFF      -
 46     18000            0       Undefined      Low      OFF      -
 47     18000            0       Undefined      Low      OFF      -
 48     18000            0       Undefined      Low      OFF      -


Slot 1 Max Watts 380
380 Watts Total Power Budget Remaining
380 Watts Total Power Budget Available
1 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 available to the corresponding PoE port, in milliwatts. The default value is 15400. To change this setting, use the **lanpower power** command.

output definitions (continued)

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.
Class	PoE class detected on attached Powered Device.
Max Watts	The maximum watts available 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 for PoE modules. 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. **Only applicable on OS9000E.**
Total Power Budget Available	The total amount of power remaining, based upon the number of power supplies installed and operating in the power shelf. **Only applicable on OS9000E**
Power Shelf Power Supplies Available	The number of power supplies currently installed and operating in the switch's power shelf. The power shelf is also referred to as Power Source Equipment (PSE).

Release History

Release 6.1; command was introduced.
Release 6.4.4; Class parameter 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 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

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

Release History

Release 6.1; 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 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

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

Release History

Release 6.1; 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 inline power prioirty level for the specified slot number.

show lanpower slot-priority *slot*

Syntax Definitions

slot	The slot number for which to display the priority level.

Defaults

N/A

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

This command is not supported on the stackable PoE switches.

Examples

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

Release History

Release 6.1.3; command was introduced.

Related Commands

lanpower slot-priority	Configures an inline power priority level for a slot

MIB Objects

```
alaPethMainPseTable
   alaPethMainPsePriority
```

4 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 interfaces, 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 source-learning
vlan mtu-ip
vlan port default
show vlan
show vlan port
show vlan router mac status
show vlan gvrp
show vlan ipmvlan

vlan

Creates a new VLAN with the specified VLAN ID (VID) and an optional description.

vlan *vid1***[**-*vid2***] [enable | disable] [name** *description***]**

no vlan *vid1***[**-*vid2***]**

Syntax Definitions

vid1	An existing VLAN ID number (1–4094).
-*vid2*	The last VLAN ID number in a range of VLANs that you want to configure (for example, 10-12 specifies VLANs 10, 11, and 12).
description	Text string up to 32 characters. Use quotes around string if description contains multiple words with spaces between them (for example, “Alcatel-Lucent Marketing VLAN”).
enable	Enable VLAN administrative status.
disable	Disable VLAN administrative status.

Defaults

parameter	default
enable | disable	**enable**
description	VLAN ID

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

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.
- Note that specifying multiple VLAN IDs and/or a range of VLAN IDs on the same command line is allowed. Use a hyphen to indicate a contiguous range and a space to separate multiple VLAN ID entries (for example, vlan 10-15 500-510 850).
- 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 name “Marketing Admin”
-> vlan 200
-> vlan 720 disable
-> no vlan 1020
-> vlan 100-105 355 400-410 “Sales Admin”
-> vlan 10 250-260
-> vlan 250-260 disable
-> no vlan 10-15
-> no vlan 10 20 200-210
```

Release History

Release 6.1; command was introduced.
Release 6.1.2; support added for entering a range and/or multiple entries of VLAN IDs.

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 *vid1***[-***vid2***] [1x1 | flat] stp {enable | disable}**

Syntax Definitions

vid1	An existing VLAN ID number (1–4094).
-vid2	The last VLAN ID number in a range of VLANs that you want to configure (for example, 10-12 specifies VLANs 10, 11, and 12).
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, the Spanning Tree status is enabled in both the 1x1 and flat mode when the VLAN is created.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- STP is not active until at least one active port is assigned to the VLAN.
- If the *vid* specified is that of a VLAN that does not exist, the VLAN is automatically created.
- Note that specifying multiple VLAN ID entries and/or a range of VLAN IDs on the same command line is allowed. Use a hyphen to indicate a contiguous range and a space to separate multiple VLAN ID entries (for example, vlan 10-15 500-510 850 stp enable).
- 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 252 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 252 VLANs can have an active Spanning Tree instance at any given time.
- To create more than 252 VLANs in the 1x1 Spanning Tree mode, use the **vlan stp disable**, **vlan 1x1 stp disable**, or **vlan flat stp disable** command to create a VLAN with Spanning Tree disabled.

- When STP is disabled on a VLAN, it remains disabled even if the switch Spanning Tree 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 disable
-> vlan 500 flat stp enable
-> vlan 100-110 stp disable
-> vlan 500-510 600 720-725 stp enable
-> vlan 250 350 400-410 stp 1x1 enable
-> vlan 10 20 stp flat disable
```

Release History

Release 6.1; command was introduced.
Release 6.1.2; support added for entering a range and/or multiple entries of VLAN IDs.

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 *vid1***[-***vid2***] mobile-tag {enable | disable}**

Syntax Definitions

vid1	An existing VLAN ID number (1–4094).
-vid2	The last VLAN ID number in a range of VLANs that you want to configure (for example, 10-12 specifies VLANs 10, 11, and 12).
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 6400, 6855, 6850E, 9000E

Usage Guidelines

- Note that specifying multiple VLAN ID entries and/or a range of VLAN IDs on the same command line is allowed. Use a hyphen to indicate a contiguous range and a space to separate multiple VLAN ID entries (for example, vlan 10-15 500-510 850 mobile-tag enable).
- 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
-> vlan 500 410-420 mobile-tag enable
-> vlan 201-210 301-310 mobile-tag enable
-> vlan 450 550 mobile-tag disable
```

Release History

Release 6.1; command was introduced.
Release 6.1.2; support added for entering a range and/or multiple entries of VLAN IDs.

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 6400, 6855, 6850E, 9000E

Usage Guidelines

- Note that specifying multiple VLAN ID entries and/or a range of VLAN IDs on the same command line is allowed. Use a hyphen to indicate a contiguous range and a space to separate multiple VLAN ID entries (for example, vlan 10-15 500-510 850 authentication).
- A maximum of 128 authenticated VLANs per switch is supported. See Chapter 41, “AAA Commands,” for more information about configuring Layer 2 Authentication.

Examples

```
-> vlan 850 authentication enable
-> vlan 720 authentication enable
-> vlan 1020 authentication disable
-> vlan 900-905 authentication enable
-> vlan 2 10-15 450-455 authentication enable
-> vlan 420 1500 authentication disable
```

Release History

Release 6.1; command was introduced.
Release 6.1.2; support added for entering a range and/or multiple entries of VLAN IDs.

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 mtu-ip

Configures the maximum transmission unit (MTU) packet size allowed for all ports associated with a VLAN. This value is configured on a per VLAN basis, so all IP interfaces assigned to the VLAN apply the same MTU value to packets sent on VLAN ports.

vlan *vid* **mtu-ip** *size*

Syntax Definitions

vid	An existing VLAN ID number (1–4094).
size	Packet size value specified in bytes (1280–9198).

Defaults

By default, the MTU size is set to 1500 bytes (the standard Ethernet MTU size).

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- The MTU size applies to traffic sent on all switch ports that are associated with the specified VLAN regardless of the port speed (for example, 10/100 Ethernet, gigabit Ethernet). Therefore, assign only ports that are capable of handling the MTU size restriction to the VLAN. For example, if the VLAN MTU size is greater than 1500, do not assign 10/100 Ethernet ports to the VLAN.
- By default, packets that exceed the MTU size are dropped. To enable MTU discovery and fragmentation, use the **icmp type** command to enable the “frag needed but DF bit set” control (for example, **icmp type 3 code 4 enable**).

Examples

```
-> vlan 200 mtu-ip 1000
-> vlan 1503 mtu-ip 10222
```

Release History

Release 6.4.1; command was introduced.

Related Commands

show vlan	Displays the VLAN configuration for the switch.

MIB objects

```
vlanTable
   vlanMtu
```

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 (for example, 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 (for example, 3/1-16) and a space to specify multiple slots (for example, 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 7, "Link Aggregation Commands."

Defaults

VLAN 1 is the default VLAN for all ports.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

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.
- 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 6.1; 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
```

vlan source-learning

Configures the status of source learning on a VLAN, a range of VLANs, or on an IP Multicast VLAN (IMPVLAN).

vlan {*vid1***[-***vid2***] | impvlan** *ipmvlan-id***} source-learning {enable | disable}**

Syntax Definitions

vid1	The VLAN ID number (2–4094).
-vid2	The last VLAN ID number in a range of VLANs that you want to configure (e.g, 10-12 specifies VLANs 10, 11, and 12).
ipmvlan-id	Specifies the IP Multicast VLAN number. The valid range is 1–4094.
enable	Enables source MAC address learning.
disable	Disables source MAC address learning.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6400, 6855-U24X, 9000E

Usage Guidelines

- The **vlan ipmvlan source-learning** command does not accept multiple VLAN IDs.
- Disabling source learning on a VLAN or IMPVLAN clears all the dynamically learned MAC addresses associated with the VLAN or IMPVLAN from the MAC address table. It causes traffic to flood the VLAN.
- Static MAC addresses associated with a VLAN or IMPVLAN are *not* cleared when source learning is disabled for the VLAN or IMPVLAN.

Examples

```
-> vlan 10-15 source-learning disable
-> vlan ipmvlan 10 source-learning disable
```

Release History

Release 6.4.2; command introduced.

Related Commands

show vlan	Displays the VLAN configuration for the switch.
show vlan ipmvlan	Displays IPMVLAN information for a specific IPMVLAN, a range of IPMVLANs, or all the IPMVLANs.

MIB Objects

```
vlanTable
   vlanEntry
   vlanNumber
   vlanStatus
   vlanMacLearningControlStatus
```

show vlan

Displays a list of VLANs and their attributes configured on the switch.

show vlan [*vid1* **[-***vid2***]]**

Syntax Definitions

vid1	The VLAN ID number (2–4094).
-vid2	The last VLAN ID number in a range of VLANs that you want to configure (for example, 10-12 specifies VLANs 10, 11, and 12).

Defaults

By default, a list of all VLANs and their attributes are displayed.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Specify a VLAN ID with this command to display information about a specific VLAN.
- Note that specifying a range of VLAN IDs is also allowed. Use a hyphen to indicate a contiguous range (for example, show vlan 10-15). Note that only one VLAN entry—a single VLAN ID or a range of VLAN IDs— is allowed with this command. Multiple entries are not accepted.

Examples

```
-> show vlan
                            stree                        mble  src
vlan  type  admin  oper  1x1   flat auth   ip   ipx   tag   lrn     name
-----+-----+------+-----+----+-----+----+-----+-----+-----+-----+---------
 1    std   on     on     on    on   off   off   NA   off    on     VLAN 1
100   vstk  on    off     off   on   off   off   NA   off    off    VLAN 100

-> show vlan 1

Name                : VLAN 1,
Administrative State: enabled,
Operational State   : enabled,
1x1 Spanning Tree State : enabled,
Flat Spanning Tree State : enabled,
Authentication      : disabled,
IP Router Port      : off,
IPX Router Port     : none,
Mobile Tag          : off,
Source Learning     : enabled
```

```
-> show vlan 100

Name                : VLAN 100,
Administrative State: enabled,
Operational State   : disabled,
1x1 Spanning Tree State : disabled,
Flat Spanning Tree State : enabled,
Authentication      : disabled,
IP Router Port      : off,
IP MTU              : 1500,
IPX Router Port     : none,
Mobile Tag          : off,
Source Learning     : disabled,
Traffic-Type: ethernet-service Customer SVLAN,
Priority-Map: x->0
```

output definitions

vlan	The numerical VLAN ID. Use the **vlan** command to create or remove VLANs.
type	The type of VLAN (**std, vstk, gvrp**, or **ipmv**).
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.
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 (for exampl, router interfaces, 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 router interface status: **on** (IP interface exists for the VLAN) or **off** (no IP router interface exists for the VLAN). Use the **ip interface** command to define an IP router interface for a VLAN.
mble tag	Mobile tagging status: **on** (enabled); **off** (disabled). Configured through the **vlan mobile-tag** command.
src lrn	Source learning status: **on** (enabled); **off** (disabled). Configured through the **vlan source-learning** command. Note that disabling source learning is not supported on the OmniSwitch 6850E.

output definitions (continued)

name	The user-defined text description for the VLAN. By default, the VLAN ID is specified for the VLAN description.
Traffic-Type	Type of traffic passing through the VLAN port.
Priority-Map	Priority map value set for the VLAN.

Release History

Release 6.1; command was introduced.
Release 6.1.2; support added for entering a range and/or multiple entries of VLAN IDs.
Release 6.2.1; **type** field added.
Release 6.4.2; **src lrn** field added.

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 interface statistics.
show vlan gvrp	Displays a list of VLANs learned through GVRP and their details.
show vlan ipmvlan	Displays IPMVLAN information for a specific IPMVLAN, a range of IPMVLANs, or all the IPMVLANs.
show ip interface	Displays IP router information.

MIB Objects

```
vlanMgrVlan
vlanTable
   vlanNumber
   vlanDescription
   vlanAdmStatus
   vlanOperStatus
   vlanStatus
   vlanStpStatus
   vlanAuthentStatus
   vlanIpAddress
   vlanIpMask
   vlanIpEnacp
   vlanIpForward
   vlanIpStatus
   vlanIpxEncap
   vlanIpxRipSapMode
   vlanIpxDelayTicks
   vlanIpxStatus
   vlanMacLearningControlStatus
   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 [*vid1***[-***vid2***]] port [***slot/port* | *link_agg***]**

Syntax Definitions

vid1	VLAN ID number (1–4094).
-vid2	The last VLAN ID number in a range of VLANs that you want to configure (e.g, 10-12 specifies VLANs 10, 11, and 12).
slot/port	Enter the slot number for the module and the physical port number on that module (for example, 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

If no parameters are specified with this command, a list of all VLANs and their assigned ports is displayed by default.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- 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.
- Note that specifying a range of VLAN IDs is also allowed. Use a hyphen to indicate a contiguous range (for example, show vlan 10-15 port). Note that only one VLAN entry—a single VLAN ID or a range of VLAN IDs— is allowed with this command. Multiple entries are not accepted.

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
         2/5    dynamic   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
   5     dynamic   blocking
   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 (for example, 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), **mirror** (port is mirroring the VLAN assignment of another port), or **dynamic** (VPAs that are learnt through GVRP).
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 (for example, router interfaces, Spanning Tree) are applied to ports and traffic flow. A VLAN must have an enabled administrative status before it can become operationally enabled.

output definitions

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 6.1; command was introduced.
Release 6.1.2; support added for entering a range and/or multiple entries of VLAN IDs.

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 interface statistics.
show vlan gvrp	Displays a list of VLANs learned through GVRP and their details.
show vlan ipmvlan	Displays IPMVLAN information for a specific IPMVLAN, a range of IPMVLANs, or all the IPMVLANs.
show ip interface	Displays IP router 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 interfaces and the number of IP router interfaces configured.

show vlan router mac status

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Only single MAC router mode is supported at this time, so multiple MAC router mode always displays as disabled.
- In single MAC router mode, a maximum of 4094 VLANs can have IP router interfaces defined. Note that these limits are subject to the availability of switch resources.

Examples

```
-> show vlan router mac status
  router-mac-multiple   total vlans   router vlans   ip vlans   ipx vlans
----------------------+-------------+--------------+----------+------------
       disabled               7              6           4           NA
```

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.
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 interface defined. Use the **ip interface** command to define an IP router interface for a VLAN.
ip vlans	The total number of VLANs configured on the switch that have an IP router interface defined. Use the **ip interface** command to define an IP router for a VLAN.

Release History

Release 6.1; 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 interface information.

MIB Objects

```
vlanMgrVlanSet
   vlanSetMultiRtrMacStatus
   vlanSetVlanCount
   vlanSetVlanRouterCount
   vlanSetIpRouterCount
   vlanSetIpxRouterCount
```

show vlan gvrp

Displays a list of VLANs learned through GVRP.

show vlan gvrp [*vid1***[-***vid2***]]**

Syntax Definitions

vid1	The VLAN ID number (2–4094).
-vid2	The last VLAN ID number in a range of VLANs that you want to configure (for example, 10-12 specifies VLANs 10, 11, and 12).

Defaults

By default, all VLANs learned through GVRP are displayed.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

Use the *vid* parameter with this command to display information for a specific VLAN or for a specific range of VLANs.

Examples

```
-> show vlan gvrp
                              stree                          mble
vlan  type  admin oper  1x1    flat    auth   ip   ipx   tag     name
----+-----+-----+----+-----+--------+------+------+-----+-----+-------------
 5   gvrp   on    on    on      on      off   NA   off   off    GVRP1
 6   gvrp   on    on    off     off     off   NA   off   off    GVRP12
```

output definitions

vlan	The VLAN ID. Use the **vlan** command to create or remove VLANs.
type	The type of VLAN (**std, vstk, gvrp**, or **ipmv**)
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.
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 (for example, router interfaces, Spanning Tree) are applied to ports and traffic flow. A VLAN must have an enabled administrative status before it can become operationally enabled.

output definitions (continued)

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 router interface status: **on** (IP interface exists for the VLAN) or **off** (no IP router interface exists for the VLAN). Use the **ip interface** command to define an IP router interface for a VLAN.
mble tag	Mobile tagging status: **on** (enabled); **off** (disabled). Configured through the **vlan mobile-tag** command.
name	The user-defined text description for the VLAN. By default, the VLAN ID is specified for the VLAN description.

Release History

Release 6.2.1; command was introduced.

Related Commands

show vlan	Displays a list of VLANs configured on the switch.
show vlan port	Displays VLAN port assignments.

MIB Objects

```
vlanMgrVlan
vlanTable
   vlanNumber
   vlanDescription
   vlanAdmStatus
   vlanOperStatus
   vlanStatus
   vlanStpStatus
   vlanAuthentStatus
   vlanIpAddress
   vlanIpMask
   vlanIpEnacp
   vlanIpForward
   vlanIpStatus
   vlanIpxEncap
   vlanIpxRipSapMode
   vlanIpxDelayTicks
   vlanIpxStatus
   vlanTagMobilePortStatus
```

show vlan ipmvlan

Displays IPMVLAN information for a specific IPMVLAN, a range of IPMVLANs, or all the IPMVLANs.

show vlan ipmvlan [*ipmvlan-id1***[-***ipmvlan-id2***]]**

Syntax Definitions

ipmvlan-id1	The IPMVLAN ID number (1–4094).
-ipmvlan-id2	The last IPMVLAN ID number in a range of IPMVLANs that you want to display (for example, 10-12 specifies VLANs 10, 11, and 12).

Defaults

By default, the configuration for all IPMVLANs is displayed.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

Use the *ipmvlan-id* parameter with this command to display information for a specific IPMVLAN or a range of IPMVLANs.

Examples

```
-> show vlan ipmvlan
                                        stree
vlan      type      admin    oper    1x1    flat      name
------+------------+-------+--------+-------------+--------------
 1201   Vstk ipmtv    on       on     on      on     VLAN 1201
 1202   Vstk ipmtv    on       on     off     off    VLAN 1202
 1203   Entp ipmtv    on       on     off     off    VLAN 1203
 1204   Vstk ipmtv    on       on     on      on     VLAN 1204
 1205   Entp ipmtv    on      off     on      off    VLAN 1205

-> show vlan ipmvlan 1201-1203
                                        stree
vlan      type      admin    oper    1x1    flat      name
------+------------+-------+--------+-------------+--------------
 1201   Vstk ipmtv    on       on     on      on     VLAN 1201
 1202   Vstk ipmtv    on       on     off     off    VLAN 1202
 1203   Entp ipmtv    on       on     off     off    VLAN 1203

-> show vlan ipmvlan 50

Name                : VLAN 50,
IPMV Mode           : Enterprise IPMVLAN
Administrative State: enabled,
Operational State   : disabled,
1x1 Spanning Tree State : disabled,
Flat Spanning Tree State: disabled,
```

```
-> show vlan ipmvlan 51

Name                     : VLAN 51,
IPMV Mode                : Vlan Stacking IPMVLAN
Administrative State     : enabled,
Operational State        : disabled,
1x1 Spanning Tree State  : enabled,
Flat Spanning Tree State: enabled,
```

output definitions

vlan	The IPMVLAN ID.
type	Indicates if the IPMVLAN is in Enterprise mode (**Entp ipmtv**) or VLAN Stacking mode (**Vstk ipmtv**).
admin	Indicates IPMVLAN administrative status: **on** (enables IPMVLAN functions to operate) or **off (**disables IPMVLAN functions without deleting the IPMVLAN).
oper	IPMVLAN operational status: **on** (enabled) or **off** (disabled). Operational status remains disabled until an active port is assigned to the IPMVLAN. When operational status is enabled, IPMVLAN properties (for example, router interfaces, Spanning Tree) are applied to ports and traffic flow. An IPMVLAN must have an enabled administrative status before it can become operationally enabled.
Name	The user-defined text description for the IPMVLAN. By default, the IPMVLAN ID is specified for the IPMVLAN description.
IPMV mode	Indicates the mode (**Enterprise IPMVLAN** or **Vlan Stacking IPMVLAN**) of the IPMVLAN.
Administrative State	Indicates the administrative status of the IPMVLAN, which can be **enabled** or **disabled**.
Operational State	Indicates the operational status of the IPMVLAN, which can be **enabled** or **disabled**.
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.

Release History

Release 6.2.1; command was introduced.

Related Commands

vlan ipmvlan	Creates an IP Multicast VLAN.
show vlan	Displays a list of VLANs configured on the switch.
show vlan port	Displays VLAN port assignments.

MIB Objects

```
vlanTable
   vlanNumber
   vlanDescription
   vlanTrafficType
   alavlanOperStatus
   alavlanAdmStatus
   alavlanStpStatus
   alavlan1x1StpStatus
   alavlanflatStpStatus
```

5 802.1Q Commands

Alcatel-Lucent'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-Lucent'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
show 802.1q

Note. Before using 802.1Q, the VLAN for 802.1Q must be created using the commands described in Chapter 4, "VLAN Management Commands."

Configuration procedures for 802.1Q are explained in "Configuring 802.1Q," *OmniSwitch AOS Release 6 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.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to delete 802.1Q tagging on a port or an aggregate of ports.
- The VLAN specified for the port or aggregate link before 802.1Q tagging can be specified. See Chapter 4, “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 7, “Link Aggregation Commands” for more information on link aggregation.
- The port’s default VLAN can never be configured to accepted tagged frames.

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 6.1; command was introduced.

Related Commands

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
   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 6400, 6855, 6850E, 9000E

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 6.1; command was introduced.

Related Commands

vlan 802.1q	Creates, modifies, or deletes 802.1Q tagging on a single port or an aggregate of ports.
show 802.1q	Displays 802.1Q tagging status and configuration.

MIB Objects

```
DOT1QPORTVLANTABLE
   dot1dBasePort
   dot1qPortAcceptableFrameTypes
```

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 7, "Link Aggregation Commands" for more information on link aggregation.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

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 5-2.

Release History

Release 6.1; 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.

MIB Objects

```
QPORTVLANTABLE
   qPortVlanSlot
   qPortVlanPort
   qPortVLanStatus
   qPortVlanTagValue
   qPortVlanDescription
   qAggregateVlanTagValue
   qAggregateVlanAggregateId
   qAggregateVlanStatus
   qAggregateVlanDescription
```

6 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-Lucent 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 four Spanning Tree protocols: 802.1D (STP), 802.1W (RSTP), 802.1Q 2005 (MSTP), and RRSTP.
- A *flat* Spanning Tree operating mode. If STP or RSTP is used, this mode applies a single STP instance across all VLANs. If MSTP is used, this mode applies a single STP instance to each Multiple Spanning Tree Instance (MSTI), which identifies a set of VLANs.
- Support for maximum MSTIs per switch. In addition, there is always one Common and Internal Spanning Tree (CIST) instance 0 on each switch.
- Ring Rapid Spanning Tree Protocol (RRSTP) supports up to a maximum range supported per switch. Note that there can be no alternate connections for the same instance between any two switches within an RRSTP ring topology.
- 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 port loop-guard** **bridge hello time** **bridge max age** **bridge forward delay** **bridge bpdu-switching** **bridge path cost mode** **bridge auto-vlan-containment** **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** **bridge priority** **bridge path cost** **bridge mode** **bridge connection** **show spantree ports**

Explicit port commands	**bridge cist** **bridge 1x1** **bridge cist priority** **bridge msti priority** **bridge 1x1 priority** **bridge cist path cost** **bridge msti path cost** **bridge 1x1 path cost** **bridge cist mode** **bridge 1x1 mode** **bridge cist connection** **bridge 1x1 connection** **bridge cist admin-edge** **bridge 1x1 admin-edge** **bridge cist auto-edge** **bridge 1x1 auto-edge** **bridge cist restricted-role** **bridge 1x1 restricted-role** **bridge cist restricted-tcn** **bridge 1x1 restricted-tcn** **bridge cist txholdcount** **bridge 1x1 txholdcount** **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**
RRSTP commands	**bridge rrstp** **bridge rrstp ring** **bridge rrstp ring vlan-tag** **bridge rrstp ring status** **show bridge rrstp configuration** **show bridge rrstp ring**
PVST+ commands	**bridge port pvst+** **bridge mode 1x1 pvst+**

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 6400, 6850E, 6855, 9000E

Usage Guidelines

- The Multiple Spanning Tree Protocol (MSTP), as defined in the IEEE 802.1Q 2005 standard, is only supported on switches operating in the flat Spanning Tree mode.
- If standard STP or RSTP 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 blocks one of these ports.
- If MSTP 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 that has 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 4, “VLAN Management Commands”).

Note. Active ports associated with VLANs that have Spanning Tree disabled on them are excluded from any Spanning Tree calculations. These VLANs remain in a forwarding state.

Examples

```
-> bridge mode flat
-> bridge mode 1x1
```

Release History

Release 6.1; command 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
```

spantree mode

Selects the flat Spanning Tree or per-VLAN Spanning Tree operating mode for the switch. These modes are exclusive; however, it is not necessary to reboot the switch when the STP modes are changed.

spantree mode {**flat | per-vlan}**

Syntax Definitions

flat	One Spanning Tree instance per switch.
per-vlan	One Spanning Tree instance for each VLAN configured on a switch.

Defaults

By default, the Spanning Tree mode for the switch is set to per-VLAN.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The Multiple Spanning Tree Protocol (MSTP), as defined in the IEEE 802.1Q 2005 standard, is only supported on switches operating in the flat Spanning Tree mode.
- If standard STP or RSTP 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 connect to the same switch together, then STP blocks one of these ports.
- If MSTP 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 the per-VLAN 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 that has its own bridge ID and configurable STP parameters, such as protocol, priority, hello time, max-age, and forward delay.
- When operating in per-VLAN 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 can 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 per-VLAN 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 4, “VLAN Management Commands”).

Note. Active ports associated with such a VLAN are excluded from any Spanning Tree calculations and remain in a forwarding state.

Examples

```
-> spantree mode flat
-> spantree mode per-vlan
```

Release History

Release 6.4.5; command 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 (1–4094).
stp	IEEE 802.1D standard Spanning Tree Algorithm and Protocol.
rstp	IEEE 802.1W Rapid Spanning Tree Protocol.
mstp	IEEE 802.1Q 2005 Multiple Spanning Tree Protocol.

Defaults

RSTP is the default protocol for the flat mode CIST instance and for the 1x1 mode VLAN instance.

parameter	default
instance	flat mode instance

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 or RSTP is the active protocol, entering 1 to specify the CIST instance is optional. If MSTP is the active protocol, however, entering 1 for the instance number is not accepted.
- Selecting MSTP is the only option for the flat mode CIST instance and is required to configure 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.
- Delete all existing MSTIs before changing the protocol from MSTP to STP or RSTP.

Note. When changing the protocol to MSTP or from MSTP, 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
WARNING: Changing to MSTP(802.1s) resets flat bridge priority and path
-> bridge protocol rstp
WARNING: Changing from MSTP(802.1s) resets flat bridge priority and path
```

Release History

Release 6.1; command introduced.
Release 6.1.2; default protocol changed to RSTP.

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 802.1Q 2005 Multiple Spanning Tree Protocol.

Defaults

RSTP is the default protocol for the flat mode CIST instance and for the 1x1 mode VLAN instance.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- 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.
- Use this command to select STP, RSTP, or MSTP as the protocol for the flat mode CIST instance.
- Selecting MSTP is only an option for the flat mode CIST instance and is required to configure 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.
- You can also use bridge instance 1 instead of **cist** keyword to specify the CIST instance.
- 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.
When changing the protocol to MSTP or from MSTP, 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.

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

-> bridge mode 1x1
-> bridge cist protocol mstp
WARNING: Changing to MSTP(802.1s) resets flat bridge priority and path
```

Release History

Release 6.1; command introduced.
Release 6.1.2; default protocol changed to RSTP.

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 port loop-guard

Enables or disables the STP loop-guard on a port or link aggregate.

bridge port {*slot/port* **| linkagg** *linkagg_id* **} loop-guard {enable | disable}**

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
linkagg_id	The number corresponding to the link aggregate group. Valid range is a unique integer in the range 0–31.
enable	Enables STP loop-guard.
disable	Disables STP loop-guard.

Defaults

STP loop-guard is disabled by default.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- When you enable loop-guard on a port, it is automatically applied to all the active instances or VLANs associated to the port.
- Loop-guard cannot be enabled on a port if root-guard is already enabled on the port or link aggregate related to the port. Root-guard must be disabled before configuring loop-guard. Similarly, when loop-guard configuration is enabled on a port or chassis, root-guard cannot be configured on the port/s.
- Loop-guard can be enabled on all types of ports including designated (forwarding), non-designated (alternate, secondary, or root) ports. However, STP loop-guard configuration does not affect designated ports. Hence, loop-guard is not effective when applied on designated ports.
- When loop-guard is enabled on root ports, they change to blocking mode when a loop-guard error occurs. In such an instance the alternate or secondary ports takeover until the root port recovers from the error state.
- If a set of ports that are already blocked by loop-guard are grouped together to form a link aggregate, the new link aggregate gets a new designated role. The link aggregate can also obtain a forwarding state depending on the STP state.
- If a spanning tree channel is blocked by loop-guard and spanning tree loses all the state information. The individual physical ports obtain the designated role, even if one or more of the links that formed the channel are unidirectional. New link aggregate might obtain a forwarding state but new port state is defined.
- The ports that are configured as fast-forwarding or edge-ports do not receive BPDUs. Loop-guard is not effective on such ports.

- Loop-guard error state is recovered when the administrative state of the port is enabled or disabled.
- When a VLAN is disabled, all the VLAN port associations recover from the error state.
- The loop-guard feature can be enabled on the ports that have STP (RSTP, MRSTP or MSTP) enabled.
- STP loop-guard on link aggregate protects all ports that are members of the link aggregation group.

Examples

```
-> bridge port 1/2 loop-guard enable
-> bridge port linkagg 1 loop-guard enable
-> bridge port 1/2 loop-guard disable
-> bridge port linkagg 1 loop-guard disable
```

Release History

Release 6.4.4; command introduced.

Related Commands

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.

MIB Objects

```
vStpPortConfigTable
       vStpPortConfigIfIndex
       vStpPortConfigLoopGuard
```

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 (1–4096).
stp	IEEE 802.1D standard Spanning Tree Algorithm and Protocol.
rstp	IEEE 802.1w Rapid Spanning Tree Protocol.

Defaults

RSTP is the default protocol for the flat mode CIST instance and for the 1x1 mode VLAN instance.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- This command is an explicit Spanning Tree command that applies only 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 stp
-> bridge 1x1 455 protocol rstp
```

Release History

Release 6.1; command introduced.
Release 6.1.2; default protocol changed to RSTP.

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 802.1Q 2005 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 (for example “Alcatel-Lucent Marketing”).

Defaults

By default, the MST region name is left blank.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 MSTP.

Examples

```
-> bridge mst region name SalesRegion
-> bridge mst region name “Alcatel-Lucent Marketing”
-> bridge mst region no name
```

Release History

Release 6.1; command 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 802.1Q 2005 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 6400, 6850E, 6855, 9000E

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 MSTP.

Examples

```
-> bridge mst region revision level 1000
-> bridge mst region revision level 2000
```

Release History

Release 6.1; command 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 6400, 6850E, 6855, 9000E

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 MSTP.

Examples

```
-> bridge mst region max hops 40
-> bridge mst region max hops 10
```

Release History

Release 6.1; command 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 (for example “Alcatel-Lucent 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 6400, 6850E, 6855, 9000E

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 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 6.1; command 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 802.1Q 2005 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 (for example 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 6400, 6850E, 6855, 9000E

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 is the selected flat mode protocol. However, the MSTI configuration 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 6.1; command 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 6400, 6850E, 6855, 9000E

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 or RSTP is the active protocol, entering 1 to specify the CIST instance is optional. If MSTP 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 MSTP or from MSTP, 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 6.1; command 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 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 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 6400, 6850E, 6855, 9000E

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 MSTP or from MSTP, 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 6.1; command 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 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 Multiple Spanning Tree Instance (MSTI). Bridge priority is used to determine which bridge the Spanning Tree algorithm designates as the root bridge.

bridge msti *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 6400, 6850E, 6855, 9000E

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 MSTI regardless of which operating mode (flat or 1x1) is active on the switch. If MSTP 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 MSTP or from MSTP, 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 6.1; command 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 6400, 6850E, 6855, 9000E

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 6.1; command 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 MSTP 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 6400, 6850E, 6855, 9000E

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 or RSTP is the active protocol, entering 1 to specify the CIST instance is optional. If MSTP is the active protocol, however, entering 1 for the instance number is not accepted.
- Note that for 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 6.1; command 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 6400, 6850E, 6855, 9000E

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 6.1; command 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 6400, 6850E, 6855, 9000E

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 6.1; command 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 6400, 6850E, 6855, 9000E

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 or RSTP is the active protocol, entering 1 to specify the CIST instance is optional. If MSTP is the active protocol, however, entering 1 for the instance number is not accepted.
- Note that for 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 6.1; command 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 6400, 6850E, 6855, 9000E

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 6.1; command 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 6400, 6850E, 6855, 9000E

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 6.1; command 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 6400, 6850E, 6855, 9000E

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 or RSTP is the active protocol, entering 1 to specify the CIST instance is optional. If MSTP is the active protocol, however, entering 1 for the instance number is not accepted.
- Note that for 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 6.1; command 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 6400, 6850E, 6855, 9000E

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 6.1; command 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 6400, 6850E, 6855, 9000E

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 6.1; command 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 mode 1x1 pvst+

Enables or disables PVST+ mode on the switch, enabling it to operate with Cisco switches.

bridge mode 1x1 pvst+ {enable | disable}

Syntax Definitions

enable	Enables the pvst+ mode.
disable	Disables the pvst+ mode.

Defaults

PVST+ is disabled by default.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- In order to handle PVST+ mode, the ports must be configured in 1x1 mode.
- This command enables the ports to handle PVST+ BPDUs.
- In this mode, the bridge priority field of the bridge ID can only be changed by a multiple of 4096.

Examples

```
-> bridge mode 1x1 pvst+ enable
-> bridge mode 1x1 pvst+ disable
```

Release History

Release 6.3.1; command introduced.

Related Commands

bridge port pvst+	Configures the type of BPDU to be used on a port when PVST+ mode is enabled.

MIB Objects

```
vStpTable
   vStpMode
   vStpModePVST
```

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.

parameter	default
instance	CIST (flat mode)

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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.
- If an *instance* is not specified with this command, the BPDU switching status is configured for the flat mode CIST instance by default regardless of which mode (flat or 1x1) is active on the switch.
- Note that if the switch is running in the flat mode, specifying a value greater than 1 for the *instance* returns 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
```

Release History

Release 6.1; command introduced.

Related Commands

vlan stp	Enables or disables Spanning Tree instance for the specified VLAN.
show spantree	Displays VLAN 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 6400, 6850E, 6855, 9000E

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 has 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, 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 6.1; command introduced.

Related Commands

bridge 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 auto-vlan-containment

Enables or disables Auto VLAN Containment (AVC). When enabled, AVC prevents a port that has no VLANs mapped to an Multiple Spanning Tree Instance (MSTI) from becoming the root port for that instance. Such ports are automatically assigned an infinite path cost value to make them an inferior choice for root port.

bridge [msti *msti_id***] auto-vlan-containment {enable | disable}**

Syntax Definitions

msti_id	An existing MSTI ID number (0–4094).
enable	Enables automatic VLAN containment.
disable	Disables automatic VLAN containment.

Defaults

By default, automatic VLAN containment is disabled.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The AVC feature is not active for any MSTI until it is globally enabled. To globally enable this feature, use the **bridge auto-vlan-containment** command but do not specify an *msti_ id*.
- When AVC is globally enabled, it is active for all MSTIs. To disable AVC for a single instance, use the **disable** form of this command and specify the *msti_id* for the instance.
- Use the **enable** form of this command and specify an *msti_id* to enable AVC for an instance that was previously disabled.
- An administratively set port path cost takes precedence and prevents AVC configuration of the path cost. The exception to this is if the port path cost is administratively set to zero, which resets the path cost to the default value.
- Note that when AVC is disabled that a port assigned to a VLAN not mapped to a specific instance can become the root port for that instance and cause a loss of connectivity between other VLANs.
- AVC does not have any effect on root bridges.

Examples

```
-> bridge auto-vlan-containment enable
-> bridge auto-vlan-containment disable
-> bridge msti 1 auto-vlan-containment disable
-> bridge msti 1 auto-vlan containment enable
```

Release History

Release 6.1.1; command introduced.

Related Commands

bridge path cost	Defines a Spanning Tree path cost for a port.
show spantree msti ports	Displays Spanning Tree port information for a flat mode Multiple Spanning Tree Instance (MSTI).

MIB Objects

```
vStpInsTable
   vStpInsAutoVlanContainment
vStpBridge
   vStpBridgeAutoVlanContainment
```

bridge port pvst+

Configures the type of BPDU to be used on a port when PVST+ mode is enabled.

bridge port {*slot/port* **|** *agg_num***} pvst+ {auto | enable | disable}**

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
agg_num	Specifies the aggregate group.
auto	IEEE BPDUs are used until a PVST+ BPDU is detected.
enable	Specifies that PVST+ BPDUs can be used.
disable	Specifies that IEEE BPDUs can be used.

Defaults

parameters	default
auto | enable | disable	**auto**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- In order to handle PVST+ mode, the ports must be configured in 1x1 mode.
- Initially, a port sends or receive IEEE BPDUs. Once a PVST+ BPDU is received, the port sends and receives only PVST+ BPDUs for tagged VLANs and IEEE BPDUs for default VLANs.

Examples

```
-> bridge port 1/3 pvst+ enable
-> bridge port 2/2 pvst+ auto
```

Release History

Release 6.3.1; command introduced.

Related Commands

bridge mode 1x1 pvst+	Enables or disables PVST+ mode on the switch.

MIB Objects

```
vStpPortConfigTable
   vStpPortConfigIfIndex
   vStpPortConfigPVST
```

bridge

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 (for example, 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 6400, 6850E, 6855, 9000E

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 or RSTP is the active protocol, enter 1 to specify the CIST instance. If MSTP is the active protocol, however, entering 1 for the instance number is not accepted. In this case, use the **bridge cist** command instead.
- Note that for 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.

Examples

```
-> bridge mode flat
-> bridge 1 4/1 disable
-> bridge 1 1/24 enable

-> bridge mode 1x1
-> bridge 255 5/10 enable
-> bridge 455 16 enable
```

Release History

Release 6.1; command introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge cist	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	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

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***} {enable | disable}**

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (for example, 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 6400, 6850E, 6855, 9000E

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.

Examples

```
-> bridge mode flat
-> bridge cist 4/1 enable
-> bridge cist 16 enable

-> bridge mode 1x1
-> bridge cist 5/10 enable
-> bridge cist 22 enable
```

Release History

Release 6.1; command introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge	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	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

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***} {enable | disable}**

Syntax Definitions

vid	An existing VLAN ID number (1–4096).
slot/port	The slot number for the module and the physical port number on that module (for example, 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 6400, 6850E, 6855, 9000E

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.

Examples

```
-> bridge mode flat
-> bridge 1x1 2 4/1 enable
-> bridge 1x1 3 16 disable

-> bridge mode 1x1
-> bridge 1x1 2 5/10 enable
-> bridge 1x1 3 22 disable
```

Release History

Release 6.1; command introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge	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	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 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 (1–4095).
slot/port	Enter the slot number for the module and the physical port number on that module (for example, 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 6400, 6850E, 6855, 9000E

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 or RSTP is the active protocol, enter 1 to specify the CIST instance. If MSTP is the active protocol, however, entering 1 for the instance number is not accepted. In this case, use the **bridge cist priority** command instead.

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 6.1; command introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge cist 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 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 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 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 (for example, 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 6400, 6850E, 6855, 9000E

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.

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 6.1; command introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge 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 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 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 priority

Configures the Spanning Tree priority value for a port or an aggregate of ports for the specified flat mode 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 (for example, 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 6400, 6850E, 6855, 9000E

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 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.

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 6.1; command introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge 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 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 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 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 (1–4096).
slot/port	Enter the slot number for the module and the physical port number on that module (for example, 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 6400, 6850E, 6855, 9000E

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.

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 6.1; command introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge 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 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 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 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 (0–4095).
slot/port	Enter the slot number for the module and the physical port number on that module (for example, 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 6400, 6850E, 6855, 9000E

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 is the active protocol, however, entering 1 for the instance number is not accepted. In this case, use the **bridge cist path cost** command instead.
- Note that when the Spanning Tree protocol is changed to/from MSTP, 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.
- If a 32-bit path cost value is in use and the *path_cost* is set to zero, the following 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
100 MB	2	120,000
	4	80,000
	8	60,000
1 GB	2	12,000
	4	8,000
	8	6,000
10 GB	2	1,200
	4	800
	8	600

- 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
100 Mbps	2	12
	4	9
	8	7
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 6.1; command 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 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 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 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 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 (for example, 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 6400, 6850E, 6855, 9000E

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, 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.
- If a 32-bit path cost value is in use and the *path_cost* is set to zero, the following 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
100 MB	2	120,000
	4	80,000
	8	60,000
1 GB	2	12,000
	4	8,000
	8	6,000
10 GB	2	1,200
	4	800
	8	600

- 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
100 Mbps	2	12
	4	9
	8	7
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 6.1; command 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 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 path cost	Explicit command for configuring the Spanning Tree path cost 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 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 path cost

Configures the Spanning Tree path cost value for a port or an aggregate of ports for the specified flat mode 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 (for example, 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 6400, 6850E, 6855, 9000E

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 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, 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.
- When MSTP is the active protocol on the switch, only a 32-bit path cost value is used. You cannot use a 16-bit path cost value is option when the MSTP protocol is active on the switch.

- If zero is entered for the *path_cost* value, then the following default path cost values are used based on the link speed:

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 are used based on link speed and link aggregate size:

Link Speed	Aggregate Size (number of links)	Default Path Cost Value
10 MB	2	1,200,000
	4	800,000
	8	600,000
100 MB	2	120,000
	4	80,000
	8	60,000
1 GB	2	12,000
	4	8,000
	8	6,000
10 GB	2	1,200
	4	800
	8	600

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 6.1; command introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge 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 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 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 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 (for example, 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 6400, 6850E, 6855, 9000E

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, 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.
- All Spanning Tree commands are saved in their explicit format when a configuration snapshot is taken of the switch.
- 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 are used based on link speed:

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 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 are used based on the link speed:

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 are used based on the link speed and link aggregate size:

Link Speed	Aggregate Size (number of links)	Default Path Cost Value
10 MB	2	1,200,000
	4	800,000
	8	600,000
100 MB	2	120,000
	4	80,000
	8	60,000
1 GB	2	12,000
	4	8,000
	8	6,000
10 GB	2	1,200
	4	800
	8	600

- 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 are used based on the link speed and link aggregate size:

Link Speed	Aggregate Size (number of links)	Default Path Cost Value
10 Mbps	2	60
	4	40
	8	30
100 Mbps	2	12
	4	9
	8	7
1 Gbps	N/A	3
10 Gbps	N/A	1

Note. The aggregate size is not applicable for Gigabit ports when a 16-bit path cost value is set.

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 6.1; command introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge 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 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 path cost	Explicit command for configuring the Spanning Tree path cost value for a port or an aggregate of ports for an MSTI when the switch is operating in either the 1x1 or flat Spanning Tree mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortPathCost
```

bridge 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 (for example, 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 6400, 6850E, 6855, 9000E

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 is the active protocol, however, entering 1 for the instance number is not accepted. In this case, use the **bridge cist mode** command instead.
- For Multiple Spanning Tree Instances (MSTI), the port Spanning Tree mode is inherited from the CIST instance. The spanning tree mode cannot be configured explicitly when the CIST instance is active.
- When a 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.

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 6.1; command introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge cist 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 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 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 (for example, 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 6400, 6850E, 6855, 9000E

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.

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 6.1; command introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge 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 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 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 (for example, 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 6400, 6850E, 6855, 9000E

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.

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 6.1; command introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge 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 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 connection

Configures the 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.

bridge *instance* **{***slot/port* | *logical_port***} connection {noptp | ptp | autoptp}**

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 (for example, 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31). *This parameter is not available on OmniSwitch 6855 switches.*
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 automatically defines connection type as point-to-point or no point-to-point.

Defaults

By default the link connection type is set to auto point-to-point.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 or RSTP is the active protocol, enter 1 to specify the CIST instance. If MSTP is the active protocol, however, entering 1 for the instance number is not accepted. In this case, use the **bridge cist connection** command instead.
- Note that for 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 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.

Examples

```
-> bridge mode flat
-> bridge 1 1/24 connection noptp

-> bridge mode 1x1
-> bridge 200 8/2 connection ptp
-> bridge 300 10 connection autoptp
```

Release History

Release 6.1; command introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge cist 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 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.
bridge cist admin-edge	Configures the administrative edge port status for a port or aggregate of ports for the CIST instance.
bridge cist auto-edge	Configures whether or not Spanning Tree automatically determines the operational edge status of a port or an aggregate of ports for the CIST instance.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortAdminConnectionType
   vStpInsPortOperConnectionType
```

bridge cist connection

Configures the connection type for a port or an aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST).

bridge cist {*slot/port* **|** *logical_port***} connection {noptp | ptp | autoptp}**

Syntax Definitions

slot/port	Enter the slot number for the module and the physical port number on that module (for example, 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 automatically defines connection type as point-to-point or no point-to-point.

Defaults

By default, the link connection type is set to auto point-to-point.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 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.

Examples

```
-> bridge mode flat
-> bridge cist 7/24 connection noptp

-> bridge mode 1x1
-> bridge cist 2/2 connection noptp
```

Release History

Release 6.1; command introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge 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 admin-edge	Configures the administrative edge port status for a port or aggregate of ports for the CIST instance.
bridge cist auto-edge	Configures whether or not Spanning Tree automatically determines the operational edge status of a port or an aggregate of ports for the CIST instance.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortAdminConnectionType
   vStpInsPortOperConnectionType
```

bridge 1x1 connection

Configures the connection type for a port or an aggregate of ports for a 1x1 mode VLAN instance.

bridge 1x1 *vid* **{***slot/port* | *logical_port***} connection {noptp | ptp | autoptp }**

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 (for example, 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 automatically defines connection type as point-to-point or no point-to-point *and* whether or not the port is an edge port.

Defaults

By default, the link connection type is set to auto point-to-point.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 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.

Examples

```
-> bridge mode flat
```

```
-> bridge 1x1 255 7/24 connection noptp

-> bridge mode 1x1
-> bridge 1x1 200 2/2 connection noptp
```

Release History

Release 6.1; command introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch
bridge 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 admin-edge	Configures the administrative edge port status for a port or aggregate of ports for the CIST instance.
bridge cist auto-edge	Configures whether or not Spanning Tree automatically determines the operational edge status of a port or an aggregate of ports for the CIST instance.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortAdminConnectionType
   vStpInsPortOperConnectionType
```

bridge cist admin-edge

Configures the administrative edge port status for a port or an aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST).

bridge cist {*slot/port* | *logical_port***} admin-edge {on | off | enable | disable}**

Syntax Definitions

slot/port	Enter the slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31).
on	Turns on the administrative edge port status for the specified port-CIST instance.
off	Turns off the administrative edge port status for the specified port-CIST instance.
enable	Enables the administrative edge port status for the specified port-CIST instance.
disable	Disables the administrative edge port status for the specified port-CIST instance.

Defaults

By default, the administrative edge port status is disabled (off).

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 the 1x1 mode when this command is used, the specified edge port status is not active for the CIST instance until the switch is configured to run in the flat Spanning Tree mode.
- Note that when a configuration snapshot is taken of the switch, all Spanning Tree commands are saved in their explicit format.
- The administrative edge port status is used to determine if a port is an edge or non-edge port when automatic edge port configuration (**auto-edge**) is disabled for the port. However, if **auto-edge** is enabled for the port, then the administrative status is overridden.
- Rapid transition of a designated port to forwarding can only occur if the port 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 connect to a host (PC, workstation, server, and so on) as edge ports to avoid unnecessary topology changes when these ports go active. This also prevents 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 operationally reverts back to a no point-to-point connection type.

Examples

```
-> bridge mode flat
-> bridge cist 15 admin-edge enable
-> bridge cist 8/23 admin-edge disable

-> bridge mode 1x1
-> bridge cist 2/2 admin-edge enable
-> bridge cist 8/23 admin-edge off
```

Release History

Release 6.1.3; command introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch
bridge 1x1 admin-edge	Configures the administrative edge port status for a port or an aggregate of ports for a specific VLAN instance.
bridge cist auto-edge	Configures whether or not Spanning Tree automatically determines the operational edge status of a port or an aggregate of ports for the flat mode CIST instance.
bridge 1x1 auto-edge	Configures whether or not Spanning Tree determines the operational edge port status for a port or an aggregate of ports for the specified 1x1 mode VLAN instance.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortAdminEdge
```

bridge 1x1 admin-edge

Configures the administrative edge port status for a port or an aggregate of ports for a 1x1 mode VLAN instance.

bridge 1x1 *vid* **{***slot/port* **|** *logical_port***} admin-edge {on | off | enable | disable}**

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 (for example, 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31).
on	Turns on the administrative edge port status for the specified port-VLAN instance.
off	Turns off the administrative edge port status for the specified port-VLAN instance.
enable	Enables the administrative edge port status for the specified port-VLAN instance.
disable	Disables the administrative edge port status for the specified port-VLAN instance.

Defaults

By default, the administrative edge port status is disabled (off).

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 edge port status for the port is not active for the VLAN instance until the switch is configured to run in the 1x1 Spanning Tree mode.
- Note that when a configuration snapshot is taken of the switch, all Spanning Tree commands are saved in their explicit format.
- The administrative edge port status is used to determine if a port is an edge or non-edge port when automatic edge port configuration (**auto-edge**) is disabled for the port. However, if **auto-edge** is enabled for the port, then the administrative status is overridden.
- Rapid transition of a designated port to forwarding can only occur if the port connection type is defined as 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 connect to a host (PC, workstation, server, and so on) as edge ports to avoid unnecessary topology changes when these ports go active. This also prevents 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 operationally reverts back to a no point-to-point connection type.

Examples

```
-> bridge mode flat
-> bridge 1x1 4 15 admin-edge on
-> bridge 1x1 255 8/23 admin-edge disable

-> bridge mode 1x1
-> bridge 1x1 3 2/2 admin-edge enable
-> bridge 1x1 255 10 admin-edge off
```

Release History

Release 6.1.3; command introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch
bridge cist admin-edge	Configures the administrative edge port status for a port or aggregate of ports for the CIST instance.
bridge cist auto-edge	Configures whether or not Spanning Tree automatically determines the operational edge status of a port or an aggregate of ports for the CIST instance.
bridge 1x1 auto-edge	Configures whether or not Spanning Tree determines the operational edge port status for a port or an aggregate of ports for the specified 1x1 mode VLAN instance.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortAdminEdge
```

bridge cist auto-edge

Configures whether or not Spanning Tree automatically determines the operational edge port status of a port or an aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST).

bridge cist {*slot/port* | *logical_port***} auto-edge {on | off | enable | disable}**

Syntax Definitions

slot/port	Enter the slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31).
on	Spanning Tree automatically determines edge port status.
off	Spanning Tree does not automatically determine edge port status.
enable	Spanning Tree automatically determines edge port status.
disable	Spanning Tree does not automatically determine edge port status.

Defaults

By default, automatic edge port status configuration is enabled (on).

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- This command is an explicit Spanning Tree command that only applies to the CIST instance regardless of which operating mode (flat or 1x1) is active on the switch.
- If the switch is running in the 1x1 mode when this command is used, the specified edge port status for the port is not active for the CIST instance until the switch is running in the flat Spanning Tree mode.
- Note that when a configuration snapshot is taken of the switch, all Spanning Tree commands are saved in their explicit format.
- The administrative edge port status is used to determine if a port is an edge or non-edge port when automatic edge port configuration (**auto-edge**) is disabled for the port. However, if **auto-edge** is enabled for the port, then the administrative status is overridden.
- Rapid transition of a designated port to forwarding can only occur if the port connection type is defined as 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 connect to a host (PC, workstation, server, and so on) as edge ports to avoid unnecessary topology changes when these ports go active. This also prevents 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 operationally reverts back to a no point-to-point connection type.

Examples

```
-> bridge mode flat
-> bridge cist 15 auto-edge on
-> bridge cist 8/23 auto-edge disable

-> bridge mode 1x1
-> bridge cist 2/2 auto-edge enable
-> bridge cist 10 auto-edge off
```

Release History

Release 6.1.3; command introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch
bridge 1x1 auto-edge	Configures whether or not Spanning Tree determines the operational edge port status for a port or an aggregate of ports for the specified 1x1 mode VLAN instance.
bridge cist admin-edge	Configures the administrative edge port status for a port or aggregate of ports for the CIST instance.
bridge 1x1 admin-edge	Configures the administrative edge port status for a port or an aggregate of ports for a specific VLAN instance.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortAutoEdge
```

bridge 1x1 auto-edge

Configures whether or not Spanning Tree determines the operational edge port status for a port or an aggregate of ports for the specified 1x1 mode VLAN instance.

bridge 1x1 *vid* **{***slot/port* | *logical_port***} auto-edge {on | off | enable | disable}**

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 (for example, 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31).
on	Spanning Tree automatically determines edge port status.
off	Spanning Tree does not automatically determine edge port status.
enable	Spanning Tree automatically determines edge port status.
disable	Spanning Tree does not automatically determine edge port status.

Defaults

By default, automatic edge port status configuration is enabled (on).

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 edge port status for the port is not active for the VLAN instance until the switch is running in the 1x1 Spanning Tree mode.
- Note that when a configuration snapshot is taken of the switch, all Spanning Tree commands are saved in their explicit format.
- The administrative edge port status is used to determine if a port is an edge or non-edge port when automatic edge port configuration (**auto-edge**) is disabled for the port. However, if **auto-edge** is enabled for the port, then the administrative status is overridden.
- Rapid transition of a designated port to forwarding can only occur if the port connection type is defined as 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 connect to a host (PC, workstation, server, and so on) as edge ports to avoid unnecessary topology changes when these ports go active. This also prevents 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 operationally reverts back to a no point-to-point connection type.

Examples

```
-> bridge mode flat
-> bridge 1x1 3 15 auto-edge on
-> bridge 1x1 255 8/23 auto-edge disable

-> bridge mode 1x1
-> bridge 1x1 4 2/2 auto-edge enable
-> bridge 1x1 255 10 auto-edge off
```

Release History

Release 6.1.3; command introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge cist auto-edge	Configures whether or not Spanning Tree automatically determines the operational edge status of a port or an aggregate of ports for the CIST instance.
bridge cist admin-edge	Configures the administrative edge port status for a port or aggregate of ports for the CIST instance.
bridge 1x1 admin-edge	Configures the administrative edge port status for a port or an aggregate of ports for a specific VLAN instance.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortAutoEdge
```

bridge cist restricted-role

Configures whether or not to prevent a port (or an aggregate of ports) from becoming the root port. When this parameter is enabled, the port does not become the root even if the port is the most likely candidate for the root. Once another port is selected as the root port, the restricted port becomes the Alternate Port.

bridge cist {*slot/port* **|** *logical_port***} {restricted-role | root-guard} {on | off | enable | disable}**

Syntax Definitions

slot/port	Enter the slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31).
root-guard	Optional command syntax. Enter **root-guard** instead of **restricted-role**; both parameters specify the same functionality for this command.
on	Turns on (enables) the restricted role status for the specified port.
off	Turns off (disables) the restricted role status for the specified port.
enable	Enables the restricted role status for the specified port.
disable	Disables the restricted role status for the specified port.

Defaults

By default, the port is not restricted from becoming the root port.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- When running in flat mode, this is a per-port setting and is applicable to any CIST or MSTI instances configured on that port.
- Note that preventing an eligible root port from becoming the root may impact connectivity within the network.
- Network administrators exclude certain ports from becoming the root to prevent bridges external to the core region of the network from influencing the Spanning Tree topology.
- 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 15 restricted-role on
-> bridge cist 8/23 root-guard disable

-> bridge mode 1x1
-> bridge cist 2/2 root-guard enable
-> bridge cist 10 restricted-role off
```

Release History

Release 6.1.3; command introduced.
Release 6.3.3; **root-guard** parameter was added.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge 1x1 restricted-role	Configures the restricted role status for a port or an aggregate of ports for the 1x1 mode VLAN instance.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortRestrictedRole
```

bridge 1x1 restricted-role

Configures whether or not to prevent a port (or an aggregate of ports) for the specified 1x1 mode VLAN instance from becoming the root port. When this parameter is enabled, the port does not become the root even if the port is the most likely candidate for the root. Once another port is selected as the root port, the restricted port becomes the Alternate Port.

bridge 1x1 *vid* **{***slot/port* | *logical_port***} {restricted-role | root-guard} {on | off | enable | disable}**

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 (for example, 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31).
root-guard	Optional command syntax. Enter **root-guard** instead of **restricted-role**; both parameters specify the same functionality for this command.
on	Turns on (enables) the restricted role status for the specified port-VLAN instance.
off	Turns off (disables) the restricted role status for the specified port-VLAN instance.
enable	Enables the restricted role status for the specified port-VLAN instance.
disable	Disables the restricted role status for the specified port-VLAN instance.

Defaults

By default, the port is not restricted from becoming the root port.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Note that preventing an eligible port from becoming the root may impact connectivity within the network.
- Network administrators exclude certain ports from becoming the root to prevent bridges external to the core region of the network from influencing the Spanning Tree topology.
- This command is an explicit Spanning Tree command that only applies to the 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 restricted status of the port is not active for the VLAN instance until the switch is running in the 1x1 Spanning Tree 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 3 15 restricted-role on
-> bridge 1x1 255 8/23 root-guard disable

-> bridge mode 1x1
-> bridge 1x1 4 2/2 root-guard enable
-> bridge 1x1 255 10 restricted-role off
```

Release History

Release 6.1.3; command introduced.
Release 6.3.3; **root-guard** parameter was added.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge cist restricted-role	Configures the restricted role status for a port or an aggregate of ports for the flat mode CIST instance.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortRestrictedRole
```

bridge cist restricted-tcn

Configures the restricted TCN status for a port or an aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST). When this parameter is enabled, the port does not propagate topology changes and notifications to/from other ports.

bridge cist {*slot/port* **|** *logical_port***} restricted-tcn {on | off | enable | disable}**

Syntax Definitions

slot/port	Enter the slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31).
on	Turns on (enables) the restricted TCN status for the specified port-CIST instance.
off	Turns off (disables) the restricted TCN status for the specified port-CIST instance.
enable	Enables the restricted TCN status for the specified port-CIST instance.
disable	Disables the restricted TCN status for the specified port-CIST instance.

Defaults

By default, the restricted TCN status for the port is disabled.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Enabling the restricted TCN status is used by network administrators to prevent bridges external to the core region of the network from causing unnecessary MAC address flushing in that region.
- Note that enabling the restricted TCN status for a port may impact Spanning Tree connectivity.
- This command is an explicit Spanning Tree command that only applies to the CIST instance regardless of which operating mode (flat or 1x1) is active on the switch.
- If the switch is running in the 1x1 mode when this command is used, the specified restricted TCN status for the port is not active for the CIST instance until the switch is running in the flat Spanning Tree 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 15 restricted-tcn on
-> bridge cist 8/23 restricted-tcn disable


-> bridge mode 1x1
-> bridge cist 2/2 restricted-tcn enable
-> bridge cist 10 restricted-tcn off
```

Release History

Release 6.1.3; command introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge 1x1 restricted-tcn	Configures the restricted TCN status for a port or an aggregate of ports for the specified 1x1 mode VLAN instance.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortRestrictedTcn
```

bridge 1x1 restricted-tcn

Configures the restricted TCN status for a port or an aggregate of ports for the specified 1x1 mode VLAN instance. When this parameter is enabled, the port does not propagate topology changes and notifications to/from other ports.

bridge 1x1 *vid* **{***slot/port* | *logical_port***} restricted-tcn {on | off | enable | disable}**

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 (for example, 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31).
on	Turns on (enables) the restricted TCN status for the specified port-VLAN instance.
off	Turns off (disables) the restricted TCN status for the specified port-VLAN instance.
enable	Enables the restricted TCN status for the specified port-VLAN instance.
disable	Disables the restricted TCN status for the specified port-VLAN instance.

Defaults

By default, the restricted TCN is set to disable.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Enabling the restricted TCN status is used by network administrators to prevent bridges external to the core region of the network from causing unnecessary MAC address flushing in that region.
- Note that enabling the restricted TCN status for a port may impact Spanning Tree connectivity.
- 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 restricted TCN status for the port is not active for the VLAN instance until the switch is running in the 1x1 Spanning Tree 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 15 restricted-tcn on
-> bridge 1x1 255 8/23 restricted-tcn disable

-> bridge mode 1x1
-> bridge 1x1 5 2/2 restricted-tcn enable
-> bridge 1x1 255 10 restricted-tcn off
```

Release History

Release 6.1.3; command introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge cist restricted-tcn	Configures the restricted TCN status for a port or an aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST).

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortRestrictedTcn
```

bridge cist txholdcount

This command is used to rate limit the transmission of BPDU through a given port for the flat mode Common and Internal Spanning Tree (CIST) instance.

bridge cist txholdcount *value*

Syntax Definitions

value	A numeric value (1–10) that controls the transmission of BPDU through the port.

Defaults

By default, the **txholdcount** value is set to 3.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- This command is an explicit Spanning Tree command that only applies to the CIST instance regardless of which operating mode (flat or 1x1) is active on the switch.
- If the switch is running in the 1x1 mode when this command is used, the specified **txholdcount** status for the port is not active for the CIST instance until the switch is running in the flat Spanning Tree 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 txholdcount 3
```

Release History

Release 6.1.3; command introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge 1x1 txholdcount	Explicit command used to rate limit the transmission of BPDU for the specified VLAN instance when the switch is operating in either the 1x1 or flat Spanning Tree mode.

MIB Objects

```
vStpInsTable
   vStpInsBridgeTxHoldCount
```

bridge 1x1 txholdcount

Configures a rate limit value that controls the transmission of BPDU through a given port for the 1x1 mode VLAN instance.

bridge 1x1 *vid* **txholdcount {***value***}**

Syntax Definitions

value	A numeric value (1–10) that controls the transmission of BPDU through the port.

Defaults

By default, the **txholdcount** value is set to 3.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 **txholdcount** status for the port is not active for the VLAN instance until the switch is running in the 1x1 Spanning Tree mode.
- Note that when a configuration snapshot is taken of the switch, all Spanning Tree commands are saved in their explicit format.

Examples

```
-> bridge 1x1 3 txholdcount 3
```

Release History

Release 6.1.3; command introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge cist txholdcount	Explicit command used to rate limit the transmission of BPDU for the CIST instance when the switch is operating in either the 1x1 or flat Spanning Tree mode.

MIB Objects

```
vStpInsTable
   vStpInsBridgeTxHoldCount
```

bridge rrstp

Enables or disables RRSTP on a switch.

bridge rrstp

no bridge rrstp

Syntax Definitions

N/A

Defaults

By default, RRSTP is disabled on the switch.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to disable RRSTP on the switch.
- RRSTP can be enabled on the switch only when the **flat** mode is active. If you try to enable RRSTP in 1x1 mode, you get an error message: “Failed to enable RRSTP because STP Mode is 1x1”.

Examples

```
-> bridge mode flat
-> bridge rrstp
-> no bridge rrstp

-> bridge mode 1x1
-> bridge rrstp
ERROR: Failed to enable Rrstp because STP Mode is 1x1
```

Release History

Release 6.2.1; command introduced.

Related Commands

bridge rrstp ring	Creates a RRSTP ring consisting of two ports.
show bridge rrstp configuration	Displays the current RRSTP status for the switch.

MIB Objects

```
vStpInfo
   VStpRrstpGlobalState
```

bridge rrstp ring

Creates a RRSTP ring consisting of two ports.

bridge rrstp ring *ring_id* **port1 {***slot/port* **| linkagg** *agg_num***} port2 {***slot/port* **| linkagg** *agg_num***} vlan-tag** *vlan_id* **[status {enable | disable}]**

no bridge rrstp ring [*ring_id***]**

Syntax Definitions

ring_id	A numeric value (1–128) that identifies the RRSTP ring.
slot/port	The slot number of the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
agg_num	The number corresponding to the static aggregate group. Must be a unique integer in the range 0–31.
vlan_id	VLAN identifier with which ring ports should be 802.1q tagged before ring creation.
enable	Enables the RRSTP ring.
disable	Disables the RRSTP ring**.**

Defaults

Parameters	Defaults
enable | disable	**disable**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a specific RRSTP ring.
- This command is used to create a ring or modify ports in an existing ring or modify the ring status.
- The ring ports must be 802.1q tagged with the VLAN before using this command.
- Note that there can be no alternate connections for the same instance between any two switches within an RRSTP ring topology.
- If RRSTP ring consists of NNI ports then they must be tagged with SVLAN (VLAN stacking) and not with standard VLAN before ring creation. For tagged RRSTP frame generation same SVLAN must be specified as ring vlan-tag. Also RRSTP ring ports must be of same type (both ring ports should be NNI ports or both should be conventional ports).
- RRSTP ring cannot be created on UNI ports.

Examples

```
-> bridge rrstp ring 1 port1 1/1 port2 1/3 vlan-tag 10 status enable
-> no bridge rrstp ring 1
```

Release History

Release 6.2.1; command introduced.

Related Commands

bridge rrstp	Enables or disables RRSTP on a switch.
show bridge rrstp ring	Displays information for all the rings or a specific ring present in the system.

MIB Objects

```
vStpRrstpRingConfigTable
   vStpRrstpRingId
   vStpRrstpRingPort1
   vStpRrstpRingPort2
   vStpRrstpRingVlanTag
   vStpRrstpRingState
   vStpRrstpRingRowStatus
```

bridge rrstp ring vlan-tag

Modifies the unique VLAN tag associated with the ring. The previous ring VLAN tag is replaced when this command is used.

bridge rrstp ring *ring_id* **vlan-tag** *vid*

Syntax Definitions

ring_id	A numeric value (1–128) that identifies the RRSTP ring.
vid	The VLAN identification number of an existing VLAN with which ring ports are 802.1Q tagged. The RRSTP ring frames shall be 802.1Q tagged with this VLAN.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The RRSTP ring can have only one VLAN tag associated with it.
- Untagged RRSTP frames shall be generated if the specified **vlan-tag** is the default VLAN of the ports.
- The ring ports must be 802.1Q tagged with the new **vlan-tag** before modifying the ring **vlan-tag**.
- RRSTP frames have 802.1Q priority similar to STP BPDUs. In order to retain this priority, use the **qos trust ports** command.

Examples

```
-> bridge rrstp ring 1 vlan-tag 10
-> bridge rrstp ring 5 vlan-tag 20
-> bridge rrstp ring 11 vlan-tag 11
```

Release History

Release 6.3.1; command introduced.

Related Commands

bridge rrstp ring	Creates a RRSTP ring consisting of two ports.
show bridge rrstp ring	Displays information for all the rings or a specific ring present in the system.

MIB Objects

```
vStpRrstpRingConfigTable
   vStpRrstpRingId
   vStpRrstpRingVlanTag
```

bridge rrstp ring status

Modifies the RRSTP status of an existing ring.

bridge rrstp ring *ring_id* **status {enable | disable}**

Syntax Definitions

ring_id	A numeric value (1–128) that identifies the RRSTP ring.
enable	Enables the RRSTP ring.
disable	Disables the RRSTP ring**.**

Defaults

Parameters	Defaults
enable | disable	**disable**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

The RRSTP status can also be modified by using the **bridge rrstp ring** command.

Examples

```
-> bridge rrstp ring 1 status enable
```

Release History

Release 6.3.1; command introduced.

Related Commands

bridge rrstp ring	Creates a RRSTP ring consisting of two ports.
show bridge rrstp ring	Displays information for all the rings or a specific ring present in the system.

MIB Objects

```
vStpRrstpRingConfigTable
   vStpRrstpRingId
   vStpRrstpRingState
   vStpRrstpRingRowStatus
```

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 (1–4095).

Defaults

parameter	default
instance	all instances

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 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
 Vlan STP Status Protocol Priority
-----+----------+--------+--------------
    1      ON       RSTP   32768 (0x8000)
  400      ON       RSTP   32768 (0x8000)
 4044      ON       RSTP   32768 (0x8000)
```

```
-> bridge protocol mstp
WARNING: Changing to MSTP(802.1s) resets flat bridge priority and path

-> 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)

-> show spantree 1

Spanning Tree Parameters
  Spanning Tree Status :                   ON,
  Protocol             :       IEEE MSTP,
  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,
  Tx Hold Count        :                    6,
  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.
VLAN	The VLAN ID when RSTP or STP mode is configured.
MSTI	The MSTI ID when MSTP mode is configured.
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.
STP Status / Spanning Tree Status	The Spanning Tree state for the CIST instance (**ON** or **OFF**).
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.
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.
Tx Hold Count	The count to limit the transmission of BPDU through the port.
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 remains 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.

output definitions (continued)

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 1x1
-> show spantree
  Spanning Tree Path Cost Mode : AUTO
  Spanning Tree PVST+ Mode     : Enable
 Vlan STP Status Protocol Priority
-----+----------+--------+--------------
    1      ON        STP   32768 (0x8000)
    2      ON        STP   32768 (0x8000)
    3      ON        STP   32768 (0x8000)

-> show spantree 2
Spanning Tree Parameters for Vlan 2
  Spanning Tree Status :                   ON,
  Protocol             :       IEEE STP,
  mode                 :   PVST+ 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,
  Tx Hold Count        :                    6,
  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.
Spanning Tree PVST+ Mode	Indicates whether the PVST + status is enabled or disabled. Configured through the **bridge mode 1x1 pvst+** 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 this instance (**STP** or **RSTP**). Configured through the **bridge protocol** command.
Mode	The Spanning Tree operating mode for the switch (**PVST+, 1x1** or **flat**). Configured through **bridge mode** command.

output definitions (continued)

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.
Tx Hold Count	The count to limit the transmission of BPDU through the port.
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 remains 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.

```
-> show spantree 1

Spanning Tree Parameters
  Spanning Tree Status :                  ON,
  Protocol             :      IEEE Rapid STP,
  mode                 :    FLAT (Single STP),
  Auto-Vlan-Containment:           Enabled   ,
  Priority             :      32768 (0x8000),
  Bridge ID            :   8000-00:e0:b1:77:78:3a,
  Designated Root      :   0000-00:e0:b1:7d:da:0e,
  Cost to Root Bridge  :                  19,
  Root Port            :   Slot 1 Interface 24,
  Next Best Root Cost  :                   0,
```

```
Next Best Root Port  :                None,
TxHoldCount          :                   3,
Topology Changes     :                   1,
Topology age         :            00:18:55,
  Current Parameters (seconds)
    Max Age              =    20,
    Forward Delay        =    20,
    Hello Time           =     2
  Parameters system uses when attempting to become root
    System Max Age       =    20,
    System Forward Delay =    15,
    System Hello Time    =     2
```

Release History

Release 6.1; command introduced.
Release 6.1.3; **Tx Hold Count** field added.

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
   vStpInsBridgeTxHoldCount
   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 6400, 6850E, 6855, 9000E

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,
  Tx Hold Count        :                    6,
  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 MSTP 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 MSTP 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 MSTP 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.
Tx Hold Count	The count to limit the transmission of BPDU through the port.
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 remains 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 6.1; command introduced.
Release 6.1.3; **Tx Hold Count** field added.

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 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
- vStpInsBridgeTxHoldCount
- vStpInsForwardDelay
- vStpInsBridgeMaxAge
- vStpInsBridgeHelloTime
- vStpInsBridgeForwardDelay
- vStpInsCistRegionalRootId
- vStpInsCistPathCost

show spantree msti

Displays Spanning Tree bridge information for a 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 6400, 6850E, 6855, 9000E

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 fails if MSTP 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,
  TxHoldCount          :                    6,
  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,
  TxHoldCount          :                    6,
  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 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 MSTP 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 MSTP 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 MSTP 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.

output definitions (continued)

Next Best Root Port	The port that offers the next best (second lowest) cost path to the root bridge for this Spanning Tree instance.
TxHoldCount	The count to limit the transmission of BPDU through the port.
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 remains 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 6.1; command introduced.
Release 6.1.3; **Tx Hold Count** field added.

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
- vStpInsBridgeTxHoldCount
- 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
vid	all VLAN instances

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- If a *vid* number is *not* specified, this command displays the Spanning Tree status, protocol, and priority values for all VLAN instances.
- Specify a *vid* number with this command to display Spanning Tree bridge information for a specific VLAN instance.
- Specifying a range of VLAN IDs is also allowed. Use a hyphen to indicate a contiguous range (for example, **show spantree 1x1 10-15**). Note that only one VLAN entry—a single VLAN ID or a range of VLAN IDs— is allowed with this command. Multiple entries are not accepted.
- 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

```
-> show spantree

  Spanning Tree Path Cost Mode : AUTO
Bridge STP Status Protocol Priority(Prio:SysID)
------+----------+--------+--------------------
    1      ON      RSTP   32768 (0x8000:0x0000)

-> show spantree 1x1
  Spanning Tree Path Cost Mode : AUTO
 Vlan STP Status Protocol Priority
-----+----------+--------+--------------
    1      ON       RSTP   32768 (0x8000)
    2      ON       RSTP   32768 (0x8000)
    3      ON       RSTP   32768 (0x8000)
```

```
-> show spantree 1x1 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,
  Tx Hold Count        :                    6,
  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
BPDU Switching Enabled

-> show spantree 1x1 10-15
  Spanning Tree Path Cost Mode : AUTO
 Vlan STP Status Protocol Priority
-----+----------+--------+--------------
   10      ON       RSTP   32768 (0x8000)
   11      ON       RSTP   32768 (0x8000)
   12      ON       RSTP   32768 (0x8000)
   13      ON       RSTP   32768 (0x8000)
   14      ON       RSTP   32768 (0x8000)
   15      ON       RSTP   32768 (0x8000)
```

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 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.
Tx Hold Count	The count to limit the transmission of BPDU through the port.
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 remains 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 6.1; command introduced.
Release 6.1.2; support added for entering a range and/or multiple entries of VLAN IDs.
Release 6.1.3; **Tx Hold Count** field added.
Release 6.4.4; **Loop Guard** and **Note** fields added.

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 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
   vStpInsBridgeTxHoldCount
   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 6400, 6850E, 6855, 9000E

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 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

```
-> show spantree 1x1

  Spanning Tree Path Cost Mode : AUTO
 ** Inactive 1x1 mode instances: **
 Vlan STP Status Protocol Priority
-----+----------+--------+-------------
    1      ON       RSTP   32768 (0x8000)
    2      ON       RSTP   32768 (0x8000)
    3      ON       RSTP   32768 (0x8000)

-> bridge mode flat
-> show spantree ports

Vlan  Port  Oper Status  Path Cost  Role   Loop Guard   Note
-----+-----+------------+---------+------+-----------+-----
    1  1/3        DIS           0    DIS         DIS
    1  1/4        DIS           0    DIS         DIS
    1  1/6        DIS           0    DIS         DIS
    1  1/7        DIS           0    DIS         DIS

-> show spantree 1 ports

Spanning Tree Port Summary for Vlan 2
       Oper  Path    Desig        Prim. Op  Op  Loop
Port   St    Cost    Cost   Role  Port  Cnx Edg Guard  Desig Bridge ID        Note
------+----+-------+-------+----+------+---+---+-----+----------------------+-----
 1/1  FORW      19      52 ROOT  1/1  PTP EDG    DIS   8000-00:30:f1:5b:37:73
 1/2   DIS       0       0  DIS  1/2   NS  NO    ENA   0000-00:00:00:00:00:00
 1/3   DIS       0       0  DIS  1/3   NS  NO    ENA   0000-00:00:00:00:00:00
 1/4   DIS       0       0  DIS  1/4   NS  NO    ENA   0000-00:00:00:00:00:00
 1/5   DIS       0       0  DIS  1/5   NS  NO    DIS   0000-00:00:00:00:00:00
 1/6   DIS       0       0  DIS  1/6   NS  NO    DIS   0000-00:00:00:00:00:00
 1/7   DIS       0       0  DIS  1/7   NS  NO    DIS   0000-00:00:00:00:00:00
 1/8   DIS       0       0  DIS  1/8   NS  NO    DIS   0000-00:00:00:00:00:00
 1/9   DIS       0       0  DIS  1/9   NS  NO    DIS   0000-00:00:00:00:00:00
 1/10  DIS       0       0  DIS  1/10  NS  NO    DIS   0000-00:00:00:00:00:00
 1/11  DIS       0       0  DIS  1/11  NS  NO    DIS   0000-00:00:00:00:00:00
 1/12  DIS       0      0  DIS  1/12  NS  NO    DIS  0000-00:00:00:00:00:00

-> show spantree 2 ports active
Spanning Tree Port Summary for Vlan 2
       Oper  Path    Desig        Prim. Op  Op  Loop
Port   St    Cost    Cost   Role  Port  Cnx Edg Guard  Desig Bridge ID       Note
------+----+-------+-------+----+------+---+---+-----+---------------------+-----
 2/2  FORW      19    0    ROOT    1/2  PTP  NO  DIS  8000-00:d0:95:f9:c4:7e
```

```
-> show spantree 1 ports active

Spanning Tree Port Summary for Vlan 1
       Oper  Path    Desig        Prim. Op  Op  Loop
Port   St    Cost    Cost   Role  Port  Cnx Edg Guard  Desig Bridge ID       Note
------+----+-------+-------+----+------+---+---+-----+---------------------+------
  1/1  FORW      19      52 ROOT   1/1  PTP EDG  DIS  8000-00:d0:95:f3:96:76
```

output definitions

Vlan	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 (for example, 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 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** - root, **DIS** - disable, **DESG** - designated, **ALT** - alternate**, MSTR** - master (valid only when MSTP mode is active), and **BKP** - backup.
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**, or **NS** (nonsignificant)**.** Shows the current operational state of the port connection type. See the **bridge connection** command for more information.
Op Edg	Operational connection type: **EDG.** Shows the current operational state of the port connection type. See the **bridge connection** command on page 6-95 for more information.
Loop Guard	Operational status of the loop-guard on a particular port or link aggregate (**ENA** or **DIS**)
Desig Bridge ID	The bridge identifier for the designated bridge for this port segment.
Note	Specifies if an Error has occured on the particular loop-guard enabled port. (**ERR**)

```
-> show spantree msti 1 ports configured

Spanning Tree Port Admin Configuration
      Port  Adm Man. Config  Adm  Adm  Aut  Rstr Rstr  10G       PVST+
Port  Pri   St. Mode   Cost  Cnx  Edg  Edg  Tcn  Role  Opt.    Cfg   Stat
-----+----+----+----+-------+----+----+----+----+----+-------+-------------
 1/1     7  ENA  No        0  AUT   No  Yes   No   No   DIS    AUT   Off
 1/2     7  ENA  No        0  AUT   No  Yes   No   No   DIS    AUT   Off
```

```
1/3     7  ENA  No        0  AUT   No  Yes   No   No   DIS    AUT   Off
1/4     7  ENA  No        0  AUT   No  Yes   No   No   DIS    AUT   Off
1/5     7  ENA  No        0  AUT   No  Yes   No   No   DIS    AUT   Off
1/6     7  ENA  No        0  AUT   No  Yes   No   No   DIS    AUT   Off
1/7     7  ENA  No        0  AUT   No  Yes   No   No   DIS    AUT   Off
1/8     7  ENA  No        0  AUT   No  Yes   No   No   DIS    AUT   Off
1/9     7  ENA  No        0  AUT   No  Yes   No   No   DIS    AUT   Off
1/10    7  ENA  No        0  AUT   No  Yes   No   No   DIS    AUT   Off
1/11    7  ENA  No        0  AUT   No  Yes   No   No   DIS    AUT   Off
1/12    7  ENA  No        0  AUT   No  Yes   No   No   DIS    AUT   Off
```

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 (for example, 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 priority** command.
Adm St	The Spanning Tree administrative status of the port: **enabled** or **disabled**. Configured through the **bridge** 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 mode** command.
Config Cost	The configured path cost value for this port. Configured through the **bridge path cost** command.
Adm Cnx	The administrative connection type: **PTP, NPT,** or **AUT**. Configured through the **bridge connection** command.
Adm Edg	The edge port administrative status: **yes** indicates that the port is an admin edge port; **no** indicates that the port is not an admin edge port. Configured through the **bridge connection** command.
Aut Edg	The edge port automatic status: **yes** indicates that the port is an automatic edge port; **no** indicates that the port is not an automatic edge port. Configured through the **bridge cist auto-edge** or **bridge 1x1 auto-edge** command.
Rstr Tcn	The restricted TCN capability: **yes** indicates that the port supports the restricted TCN capability; **no** indicates that the port does not support the restricted TCN capability. Configured through the **bridge cist restricted-tcn** or **bridge 1x1 restricted-tcn** command.
Rstr Role	The restricted role port status: **yes** indicates that the port is a restricted role port; **no** indicates that the port is not a restricted role port. Configured through the **bridge cist restricted-role** or **bridge 1x1 restricted-role** command.
10G Opt.	Indicates whether the 10 GB port interoperability status is enabled (**ENA**) or disabled (**DIS**).

output definitions

PVST+ Cfg	Indicates the current PVST+ port configuration (**auto, enable** or **disable)**.
PVST+ Stat	Indicates the current status of the PVST+ port (**On** or **Off**).

```
-> bridge mode flat
-> bridge protocol mstp
-> show spantree ports

 Msti  Port Oper Status  Path Cost  Role   Loop Guard   Note
-----+-----+------------+---------+------+------------+----------
    0  1/1      FORW       200000   ROOT    DIS
    0  1/2       DIS           0    DIS     ENA
    0  1/3       DIS           0    DIS     ENA
    0  1/4       DIS           0    DIS     ENA
    0  1/5       DIS           0    DIS     DIS
    0  1/6       DIS           0    DIS     DIS
    0  1/7       DIS           0    DIS     DIS
    0  1/8       DIS           0    DIS     DIS
    0  1/9       DIS           0    DIS     DIS
    0  1/10      DIS           0    DIS     DIS
    0  5/1       DIS           0    DIS     DIS
    0  5/2       DIS           0    DIS     DIS

-> show spantree ports active

 Msti  Port  Oper Status  Path Cost  Role   Loop Guard   Note
-----+------+------------+---------+-------+-----------+---------
    0  1/1      FORW        200000   ROOT         DIS

-> bridge mode 1x1
-> bridge protocol rstp
-> show spantree ports active

Brdge  Port  Oper Status  Path Cost  Role
-----+------+------------+---------+-------
    1  1/15      LIST          19   DESG
    1  1/21      FORW          19   DESG
    1  1/24      FORW          19   ROOT
```

output definitions

Msti	The Multiple Spanning Tree Instance (MSTI) instance number. Configured through the **bridge msti** command. **Note.** 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 (for example, 0/31).
Oper Status	The port operational state as defined by application of the Spanning Tree Protocol. Possible port operational states include: **DIS** - disabled, **BLOCK** - blocking, **LIST** - listening, **LEARN** - learning, and **FORW** - 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 path cost** command.
Role	The role of the port for this Spanning Tree instance. Possible port roles are: **ROOT -** root, **DIS -** disable, **DESG -** designated, **ALT -** alternate**, MSTR -** master (valid only when MSTP mode is active), and **BKP** - backup.
Loop Guard	Operational status of the loop-guard on a particular port or link aggregate (**ENA** or **DIS**).
Note	Indicates whether a loop-guard error (**ERR**) has occured on the MSTI instance.

```
-> bridge mode 1x1
-> show spantree ports

 Vlan  Port Oper Status  Path Cost  Role    Loop Guard    Note
-----+-----+------------+---------+-------+------------+--------
    1  1/1       DIS           0    DIS      ENA
    1  1/2       DIS           0    DIS      ENA
    1  1/3       DIS           0    DIS      ENA
    1  1/4       DIS           0    DIS      DIS
    1  1/5       DIS           0    DIS      DIS
    1  1/6       DIS           0    DIS      DIS
    1  1/7       DIS           0    DIS      DIS
    1  1/8       DIS           0    DIS      DIS
    1  1/9       DIS           0    DIS      DIS
    1  1/10      DIS           0    DIS      DIS
    1  1/11      DIS           0    DIS      DIS
    1  1/12     FORW          19    ROOT     DIS

-> show spantree 1 ports

Spanning Tree Port Summary for Vlan 1
      Oper  Path   Desig        Prim. Op  Op  Loop
Port   St   Cost    Cost   Role Port  Cnx Edg Guard    Desig Bridge ID      Note
------+----+------+------+----+------+---+---+-----+----------------------+------
 1/1   DIS       0       0  DIS 1/1   NS EDG   DIS   0000-00:00:00:00:00:00
 1/2   DIS       0       0  DIS 1/2   NS  NO   DIS   0000-00:00:00:00:00:00
```

```
 1/3   DIS       0       0  DIS 1/3   NS  NO   DIS   0000-00:00:00:00:00:00
 1/4   DIS       0       0  DIS 1/4   NS  NO   DIS   0000-00:00:00:00:00:00
 1/5   DIS       0       0  DIS 1/5   NS  NO   ENA   0000-00:00:00:00:00:00
 1/6   DIS       0       0  DIS 1/6   NS  NO   ENA   0000-00:00:00:00:00:00
 1/7   DIS       0       0  DIS 1/7   NS  NO   DIS   0000-00:00:00:00:00:00
 1/8   DIS       0       0  DIS 1/8   NS  NO   DIS   0000-00:00:00:00:00:00
 1/9   DIS       0       0  DIS 1/9   NS  NO   DIS   0000-00:00:00:00:00:00
 1/10  DIS       0       0  DIS 1/10  NS  NO   DIS   0000-00:00:00:00:00:00
 1/11  BLK      19       0 DESG 1/11  NS EDG   ENA   0000-00:00:00:00:00:00  ERR
 1/12 FORW      20       0 ROOT 1/12 PTP EDG   ENA   0001-00:d0:95:6a:79:50

 -> show spantree 1 ports active

    Spanning Tree Port Summary for Vlan 1

     Oper  Path  Desig        Prim. Op  Op  Loop
Port   St  Cost  Cost   Role  Port  Cnx Edg Guard  Desig Bridge ID         Note
----+----+------+------+----+------+---+---+-----+-----------------------+--------
1/12 FORW     0       0  DIS   1/5   NS  EDG  ENA   0000-00:00:00:00:00:00

 -> show spantree ports blocking

 Vlan  Port  Oper Status  Path Cost  Role   Loop Guard   Note
-----+------+-----------+---------+-------+-----------+-------
   1   1/11        BLK           19   DESG         ENA   ERR
```

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 (for example, 0/31).
Oper Status	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 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** - root, **DIS** - disable, **DESG** - designated, **ALT** - alternate**, MSTR** - master (valid only when MSTP mode is active), and **BKP** - backup.
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**, or **NS** (nonsignificant)**.** Shows the current operational state of the port connection type. See the **bridge connection** command for more information.

output definitions (continued)

Op Edg	Operational connection type: **EDG.** Shows the current operational state of the port connection type. See the **bridge connection** command on page 6-95 for more information.
Desig Bridge ID	The bridge identifier for the designated bridge for the port segment.
Loop Guard	Operational status of the loop-guard on a particular port or link aggregate (**ENA** or **DIS**)
Note	Specifies if an Error has occured on the particular loop-guard enabled port. (**ERR**)

```
-> show spantree 2 ports configured

Spanning Tree Port Admin Configuration for Vlan 2
      Port  Adm Man. Config  Adm  Adm  Aut  Rstr Rstr OS8800     PVST+
Port  Pri   St. Mode   Cost  Cnx  Edg  Edg  Tcn  Role 10G Opt.  Cfg Stat
-----+----+----+----+-------+----+----+----+----+----+---------+---------
 3/1     7  ENA  No        0  AUT   No  Yes   No   No   DIS     AUT ON
 3/3     7  ENA  No        0  AUT   No  Yes   No   No   DIS     AUT OFF
 0/9     7  ENA  No        0  AUT   No  Yes   No   No   DIS     AUT ON
```

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 (for example, 0/31).
Port Pri	The Spanning Tree priority for the port. The lower the number, the higher the priority. Configured through the **bridge priority** command.
Adm St	The Spanning Tree administrative status of the port: **enabled** or **disabled**. Configured through the **bridge** 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 mode** command.
Config Cost	The configured path cost value for this port. Configured through the **bridge path cost** command.
Adm Cnx	The administrative connection type: **PTP, NPT,** or **AUT.** Configured through the **bridge connection** command.
Adm Edg	The edge port administrative status: **yes** indicates that the port is an admin edge port; **no** indicates that the port is not an admin edge port. Configured through the **bridge connection** command.
Aut Edg	The edge port automatic status: **yes** indicates that the port is an automatic edge port; **no** indicates that the port is not an automatic edge port. Configured through the **bridge cist auto-edge** or **bridge 1x1 auto-edge** command.
Rstr Tcn	The restricted TCN capability: **yes** indicates that the port supports the restricted TCN capability; **no** indicates that the port does not support the restricted TCN capability. Configured through the **bridge cist restricted-tcn** or **bridge 1x1 restricted-tcn** command.

output definitions (continued)

Rstr Role	The restricted role port status: **yes** indicates that the port is a restricted role port; **no** indicates that the port is not a restricted role port. Configured through the **bridge cist restricted-role** or **bridge 1x1 restricted-role** command.
OS8800 10G Opt.	Indicates whether the 10 GB port interoperability status is enabled (**ENA**) or disabled (**DIS**).
PVST+ Cfg	Indicates the current PVST+ port configuration (**auto, enable** or **disable)**.
PVST+ Stat	Indicates the current status of the PVST+ port (**On** or **Off**).

Release History

Release 6.1; command introduced.
Release 6.3.1; **PVST+** field added.
Release 6.4.4;**Loop Guard** and **Note** fields added.

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 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
   vStpInsPortAdminConnectionType
   vStpInsPortOperConnectionType
   vStpInsPortAdminEdge
   vStpInsPortAutoEdge
   vStpInsPortRestrictedRole
   vStpInsPortRestrictedTcn
   vStpInsPortPrimaryPortNumber
   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 6400, 6850E, 6855, 9000E

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

       Oper  Path    Desig        Prim. Op  Op  Loop
Port   St    Cost    Cost   Role  Port  Cnx Edg Guard  Desig Bridge ID       Note
------+----+-------+-------+----+------+---+---+-----+----------------------+------
 1/1    DIS       0       0  DIS  1/1    NS EDG  DIS  0000-00:00:00:00:00:00
 1/2    DIS       0       0  DIS  1/2    NS EDG  DIS  0000-00:00:00:00:00:00
```

```
-> show spantree cist ports active

Spanning Tree Port Summary

       Oper  Path    Desig        Prim. Op  Op  Loop
Port   St    Cost    Cost   Role  Port  Cnx Edg Guard  Desig Bridge ID        Note

------+----+-------+-------+----+------+---+---+-----+----------------------+-----
1/19   FORW       4       8 DESG  1/19  PTP  NO  DIS   8000-00:d0:95:d5:e5:a2
1/23   FORW       4       4 ROOT  1/23  PTP  NO  DIS   8000-00:d0:95:ea:b2:48
```

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 (for example, 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 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** - root, **DIS** - disable, **DESG** - designated, **ALT** - alternate**,** **MSTR** - master (valid only when MSTP mode is active), and **BKP** - backup.
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**, or **NS** (nonsignificant). Shows the current operational state of the port connection type. See the **bridge connection** command for more information.
Op Edg	Operational connection type: **EDG.** Shows the current operational state of the port connection type. See the **bridge connection** command on page 6-95 for more information.
Loop Guard	Operational status of the loop-guard on a particular port or link aggregate (**ENA** or **DIS**).
Desig Bridge ID	The bridge identifier for the designated bridge for this port segment.
Note	Indicates whether a loop-guard error (**ERR**) has occured on the MSTI instance.

```
-> show spantree cist ports configured

Spanning Tree Port Admin Configuration for Vlan 1
      Port  Adm  Man. Config  Adm  Adm  Aut  Rstr  Rstr Role/  OS8800   PVST+
Port  Pri   St.  Mode Cost    Cnx  Edg  Edg  Tcn   Root Guard  10G Opt  Cfg Stat
-----+----+----+-----+-------+----+----+----+----+------------+--------+--------
 1/1   7    ENA   No    0     AUT   No  Yes   No    No   DIS   AUT      Off
 1/2   7    ENA   No    0     AUT   No  Yes   No    No   DIS   AUT      Off
 1/3   7    ENA   No    0     AUT   No  Yes   No    No   DIS   AUT      Off
 1/4   7    ENA   No    0     AUT   No  Yes   No    No   DIS   AUT      Off
```

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 (for example, 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 priority** command.
Adm St.	The Spanning Tree administrative status of the port: **enabled** or **disabled**. Configured through the **bridge** 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 mode** command.
Config Cost	The configured path cost value for this port. Configured through the **bridge path cost** command.
Adm Cnx	The administrative connection type: **PTP, NPT,** or **AUT.** Configured through the **bridge connection** command.
Adm Edg	The edge port administrative status: **yes** indicates that the port is an admin edge port; **no** indicates that the port is not an admin edge port**.** Configured through the **bridge connection** command.
Aut Edg	The edge port automatic status: **yes** indicates that the port is an automatic edge port; **no** indicates that the port is not an automatic edge port. Configured through the **bridge cist auto-edge** or **bridge 1x1 auto-edge** command.
Rstr Tcn	The restricted TCN capability: **yes** indicates that the port supports the restricted TCN capability; **no** indicates that the port does not support the restricted TCN capability. Configured through the **bridge cist restricted-tcn** or **bridge 1x1 restricted-tcn** command.
Rstr Role/Root Guard	The restricted status of the port: **Yes** indicates that the port is restricted from becoming the root; **No** indicates that the port is not restricted from becoming the root. Configured through the **bridge cist restricted-role** or **bridge 1x1 restricted-role** command.
OS8800 10G Opt.	Indicates whether the 10 GB port interoperability status is enabled (**ENA**) or disabled (**DIS**).

output definitions (continued)

PVST+ Cfg Stat	The PVST+ status on the switch: **enabled** or **disabled**. Configured through the command to enable or disable PVST+ mode on the switch.
PVST+ Stat	Indicates whether or not the PVST+ interoperability status is enabled (**ENA**) or disabled (**DIS**) for the port. Configured throught the command.

Release History

Release 6.1; command introduced.
Release 6.3.3; **PVST+** fields added.
Releas 6.4.4; **Loop Guard** and **Note** fields added.

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 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
   vStpInsPortAdminEdge
   vStpInsPortAutoEdge
   vStpInsPortRestrictedRole
   vStpInsPortRestrictedTcn
   vStpInsPortManualMode
   vStpInsPortRole
   vStpInsPrimaryPortNumber
   vStpInsPortAdminConnectionType
   vStpInsPortOperConnectionType
```

show spantree msti ports

Displays Spanning Tree port information for a flat mode 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 6400, 6850E, 6855, 9000E

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.
- 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.

- 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 is not the selected flat mode protocol, this command fails.
- 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   Loop Guard   Note
-----+------+------------+-----------+-----+------------+---------
0      1/1     DIS          0           DIS     DIS
0      1/2     DIS          0           DIS     DIS
2      1/5     FORW         10          MSTR    ENA
2      1/6     DIS          0           DIS     DIS

-> show spantree msti 2 ports

Spanning Tree Port Summary for Msti 2
       Oper Path  Desig Prim. Op     Op   Op   Loop
Port   St   Cost  Cost  Role  Port   Cnx  Edg  Guard Desig Bridge ID        Note
------+----+-----+----+------+------+---+----+------+---------------------+-------
1/5    FORW  0      0    MSTR   1/1   NS  EDG   ENA  0000-00:00:00:00:00:00
1/6    DIS   0      0    DIS    1/2   NS  EDG   DIS  0000-00:00:00:00:00:00

-> show spantree msti 2 ports active

Spanning Tree Port Summary for Msti 2
      Oper  Path   Desig       Prim. Op  Op  Loop
Port   St   Cost    Cost  Role Port  Cnx Edg Guard Desig Bridge ID         Note
-----+----+-------+------+----+-----+---+---+-----+----------------------+-------
 1/1  FORW  200000    0   DESG  1/1  PTP EDG   DIS 8002-00:d0:95:57:3a:9e
```

output definitions

Msti	The 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 (for example, 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 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 -** root, **DIS -** disable, **DESG -** designated, **ALT -** alternate**, MSTR -** master (valid only when MSTP mode is active), and **BKP** - backup.
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**, or **NS** (nonsignificant). Shows the current operational state of the port connection type. See the **bridge connection** command for more information.
Op Edg	Operational connection type: **EDG.** Shows the current operational state of the port connection type. See the **bridge connection** command on page 6-95 for more information.
Loop Guard	Operational status of the loop-guard on a particular port or link aggregate (**ENA** or **DIS**).
Desig Bridge ID	The bridge identifier for the designated bridge for this port segment.
Note	Indicates whether a loop-guard error (**ERR**) has occured on the MSTI instance.

```
-> show spantree msti 2 ports configured

Spanning Tree Port Admin Configuration for Msti 2
      Port  Adm Man. Config  Adm  Adm  Aut  Rstr Rstr OS8800
Port  Pri   St. Mode   Cost  Cnx  Edg  Edg  Tcn  Role 10G Opt.
-----+----+----+----+-------+----+----+----+----+----+--------
 1/1     7  ENA  No        0  AUT   No  Yes   No   No   DIS
 1/2     7  ENA  No        0  AUT   No  Yes   No   No   DIS
 1/3     7  ENA  No        0  AUT   No  Yes   No   No   DIS
 1/4     7  ENA  No        0  AUT   No  Yes   No   No   DIS
 1/5     7  ENA  No        0  AUT   No  Yes   No   No   DIS
 1/6     7  ENA  No        0  AUT   No  Yes   No   No   DIS
 1/7     7  ENA  No        0  AUT   No  Yes   No   No   DIS
 1/8     7  ENA  No        0  AUT   No  Yes   No   No   DIS
 1/9     7  ENA  No        0  AUT   No  Yes   No   No   DIS
 1/10    7  ENA  No        0  AUT   No  Yes   No   No   DIS
 1/11    7  ENA  No        0  AUT   No  Yes   No   No   DIS
 1/12    7  ENA  No        0  AUT   No  Yes   No   No   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 (for example, 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 priority** command.

output definitions (continued)

Adm St	The Spanning Tree administrative status of the port: **enabled** or **disabled**. Configured through the **bridge** 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 mode** command.
Config Cost	The configured path cost value for this port. Configured through the **bridge msti path cost** command.
Adm Cnx	The administrative connection type: **PTP, NPT,** or **AUT.** Configured through the **bridge connection** command.
Adm Edg	The edge port administrative status: **yes** indicates that the port is an admin edge port; **no** indicates that the port is not an admin edge port**.** Configured through the **bridge connection** command.
Aut Edg	The edge port automatic status: **yes** indicates that the port is an automatic edge port; **no** indicates that the port is not an automatic edge port. Configured through the **bridge cist auto-edge** or **bridge 1x1 auto-edge** command.
Rstr Tcn	The restricted TCN capability: **yes** indicates that the port supports the restricted TCN capability; **no** indicates that the port does not support the restricted TCN capability. Configured through the **bridge cist restricted-tcn** or **bridge 1x1 restricted-tcn** command.
Rstr Role	The restricted role port status: **yes** indicates that the port is a restricted role port; **no** indicates that the port is not a restricted role port. Configured through the **bridge cist restricted-role** or **bridge 1x1 restricted-role** command.
OS8800 10G Opt.	Indicates whether the 10 GB port interoperability status is enabled (**ENA**) or disabled (**DIS**).

Release History

Release 6.1; command introduced.
Release 6.1.3; fields added.
Release 6.4.4; **Loop Guard** and **Note** fields added.

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
- vStpInsPortAdminEdge
- vStpInsPortAutoEdge
- vStpInsPortRestrictedRole
- vStpInsPortRestrictedTcn
- 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 6400, 6850E, 6855, 9000E

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.
- Specifying a range of VLAN IDs is also allowed. Use a hyphen to indicate a contiguous range (for example, **show spantree 1x1 10-15 ports**). Note that only one VLAN entry—a single VLAN ID or a range of VLAN IDs— is allowed with this command. Multiple entries are not accepted.
- 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   Loop Guard   Note
-----+------+------------+---------+-------+-----------+-----
    1  1/1        ROOT            0    DIS         DIS
    1  1/2        FORW           20    DIS         ENA
    1  1/3        ALT             0    DIS         DIS
    1  1/4        ALT             0    DIS         DIS
    1  1/5        ALT             0    DIS         DIS
    1  1/6        ALT             0    DIS         DIS
   10  1/7       FORW            19   DESG         ENA
   10  1/8        ALT             0    DIS         DIS
   11  1/9        ALT             0    DIS         DIS
   11  1/10       ALT             0    DIS         DIS
  172  1/11       FORW           19   ROOT         DIS
  400  1/12       BLK             0    ALT         ENA   ERR
 1001  2/1       FORW            19   DESG         ENA
 1001  2/3        DIS             0    DIS         DIS
 2000  2/2        DIS             0    DIS         DIS
 2000  2/5        DIS             0    DIS         DIS

-> show spantree 1x1 1 ports

      Oper  Path    Desig        Prim. Op  Op  Loop
Port  St    Cost    Cost   Role  Port  Cnx Edg Guard  Desig Bridge ID     Note

-----+-----+-------+-------+----+------+---+---+----+--------------------+----
 1/1   ROOT      0       0  DIS  1/1    NS EDG  DIS  0000-00:00:00:00:00:00
 1/2   FORW     20       0  DIS  1/2    NS EDG  ENA  0000-00:00:00:00:00:00
 1/3   ALT       0       0  DIS  1/3    NS EDG  DIS  0000-00:00:00:00:00:00
 1/4   ALT       0       0  DIS  1/4    NS EDG  DIS  0000-00:00:00:00:00:00
 1/5   ALT       0       0  DIS  1/5    NS EDG  DIS  0000-00:00:00:00:00:00
 1/6   ALT       0       0  DIS  1/6    NS EDG  DIS  0000-00:00:00:00:00:00


-> show spantree 1x1 1 ports active

Spanning Tree Port Summary for Vlan 1
      Oper  Path   Desig        Prim.Op  Op   Loop
Port   St   Cost    Cost   Role Port Cnx Edg  Guard  Desig Bridge ID        Note
-----+----+-------+-------+----+----+---+----+------+--------------------+-------
 1/2  FORW     20       0  DIS  1/2  NS  EDG  ENA    0001-00:d0:95:6a:79:50


-> show spantree 1x1 10-11 ports

Spanning Tree Port Summary for Vlan 10

      Oper Path Desig Prim. Op   Op   Op   Loop
Port  St   Cost Cost  Role  Port Cnx  Edg  Guard  Desig Bridge ID        Note
-----+----+----+----+------+----+----+----+-----+--------------------+--------
1/7   DIS   0   0     DIS   1/7  NS   EDG   DIS  0000-00:00:00:00:00:00
1/8   DIS   0   0     DIS   1/8  NS   EDG   DIS  0000-00:00:00:00:00:00
```

```
Spanning Tree Port Summary for Vlan 11

Oper  Path Desig Prim. Op   Op    Op    Op   Loop
Port  St   Cost Cost  Role  Port Cnx    Edg  Guard  Desig Bridge ID        Note
-----+----+-----+----+------+----+----+----+------+----------------------+--------
 1/9  DIS   0     0  DIS    1/36  NS   EDG  DIS   0000-00:00:00:00:00:00
 1/10 DIS   0     0  DIS    1/42  NS   EDG  DIS   0000-00:00:00:00:00:00
```

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 (for example, 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 1x1 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 -** root, **DIS -** disable, **DESG -** designated, **ALT -** alternate**, MSTR -** master (valid only when MSTP mode is active), and **BKP** - backup.
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**, or **NS** (nonsignificant). Shows the current operational state of the port connection type. See the **bridge connection** command for more information.
Op Edg	Operational connection type: **EDG.** Shows the current operational state of the port connection type. See the **bridge connection** command on page 6-95 for more information.
Loop Guard	Operational status of the loop-guard on a particular port or link aggregate (**ENA** or **DIS**).
Desig Bridge ID	The bridge identifier for the designated bridge for the segment related to this port.
Note	Indicates whether a loop-guard error (**ERR**) has occured on the MSTI instance.

```
-> show spantree 1x1 1 ports configured

Spanning Tree Port Admin Configuration for Vlan 1
      Port  Adm Man. Config  Adm  Adm  Aut  Rstr Rstr Role/  OS8800    PVST+
Port  Pri   St. Mode   Cost  Cnx  Edg  Edg  Tcn  Root Guard  10G Opt  Cfg Stat
-----+----+----+----+-------+----+----+-----+----+---------+--------+---------
 1/1     7  ENA  No        0  AUT   No  Yes   No    No        DIS     AUT OFF
 1/2     7  ENA  No        0  AUT   No  Yes   No    No        DIS     AUT OFF
 1/3     7  ENA  No        0  AUT   No  Yes   No    No        DIS     AUT OFF
 1/4     7  ENA  No        0  AUT   No  Yes   No    No        DIS     AUT OFF
 1/5     7  ENA  No        0  AUT   No  Yes   No    No        DIS     AUT OFF
 1/6     7  ENA  No        0  AUT   No  Yes   No    No        DIS     AUT OFF

-> show spantree 1x1 10-11 ports configured
Spanning Tree Port Admin Configuration for Vlan 10
      Port  Adm Man. Config  Adm  Adm  Aut  Rstr Rstr Role/  OS8800    PVST+
Port  Pri   St. Mode   Cost  Cnx  Edg  Edg  Tcn  Root Guard  10G Opt  Cfg Stat
-----+----+----+----+-------+----+----+-----+----+---------+--------+---------
 1/7    7  ENA  No        0  AUT   No  Yes   No    No        DIS     AUT OFF
 1/8    7   ENA  No        0  AUT   No  Yes   No    No        DIS     AUT OFF

Spanning Tree Port Admin Configuration for Vlan 11
      Port  Adm Man. Config  Adm  Adm  Aut  Rstr Rstr Role/  OS8800    PVST+
Port  Pri   St. Mode   Cost  Cnx  Edg  Edg  Tcn  Root Guard  10G Opt  Cfg Stat
-----+----+----+----+-------+----+----+-----+----+---------+--------+---------
 1/9    7  ENA  No        0  AUT   No  Yes   No    No        DIS      AUT OFF
 1/10   7  ENA  No       0  AUT   No Yes    No    No        DIS     AUT OFF
```

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 (for example, 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 priority** command.
Adm St	The Spanning Tree administrative status of the port: **enabled** or **disabled**. Configured through the **bridge** 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 mode** command.
Config Cost	The configured path cost value for this port. Configured through the **bridge 1x1 path cost** command.
Adm Cnx	The administrative connection type: **PTP, NPT,** or **AUT**. Configured through the **bridge connection** command.
Adm Edg	The edge port administrative status: **yes** indicates that the port is an admin edge port; **no** indicates that the port is not an admin edge port**.** Configured through the **bridge connection** command.

output definitions (continued)

Aut Edg	The edge port automatic status: **yes** indicates that the port is an automatic edge port; **no** indicates that the port is not an automatic edge port. Configured through the **bridge cist auto-edge** or **bridge 1x1 auto-edge** command.
Rstr Tcn	The restricted TCN capability: **yes** indicates that the port supports the restricted TCN capability; **no** indicates that the port does not support the restricted TCN capability. Configured through the **bridge cist restricted-tcn** or **bridge 1x1 restricted-tcn** command.
Rstr Role/Root Guard	The restricted status of the port: **Yes** indicates that the port is restricted from becoming the root; **No** indicates that the port is not restricted from becoming the root. Configured through the **bridge cist restricted-role** or **bridge 1x1 restricted-role** command.
10G Opt.	Indicates whether the 10 GB port interoperability status is enabled (**ENA**) or disabled (**DIS**).
PVST+ Cfg	The type of BPDU used on the port: **AUTO** indicates that IEEE BPDUs are used until a PVST+ BPDU is detected; **ENA** indicates that PVST+ BPDUs are used; **DIS** indicates that IEEE BPDUs are used. Configured through the **bridge port pvst+** command.
PVST+ Stat	Indicates whether or not the PVST+ interoperability status is enabled (**ENA**) or disabled (**DIS**) for the port. Configured throught the command.

Release History

Release 6.1; command introduced.
Release 6.1.2; support added for entering a range and/or multiple entries of VLAN IDs.
Release 6.1.3; fields added.
Release 6.3.3; fields added.
Release 6.4.4; **Loop Guard** and **Note** output fields added.

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
vStpInsPortAdminConnectionType
vStpInsPortOperConnectionType
vStpInsPortAdminEdge
vStpInsPortAutoEdge
vStpInsPortRestrictedRole
vStpInsPortRestrictedTcn
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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Three MST region attributes (configuration name, revision level, and configuration digest) define an MST region as required by the IEEE 802.1Q 2005 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       = ,
 Revision Level           = 0,
 Configuration Digest     = 0xac36177f 50283cd4 b83821d8 ab26de62,
 Revision Max hops        = 20,
 Cist Instance Number     = 0
```

output definitions

Configuration Name	An alphanumeric string that identifies the name of the MST region. Use the **bridge mst region name** command to define this value.
Revision Level	A numeric value 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 802.1Q 2005 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:** This instance is known as the flat mode instance and is known as bridge 1 when using STP or RSTP.

Release History

Release 6.1; command 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 6400, 6850E, 6855, 9000E

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

 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 6.1; command 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 6400, 6850E, 6855, 9000E

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

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 6.1; command 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 6400, 6850E, 6855, 9000E

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 6.1; command 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 (for example, 3/1 specifies port 1 on slot 3).
logical_port	The link aggregate ID number (0–31).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Note. MST 0 also represents the flat mode CIST instance, that all ports are associated with when the switch is running in the flat Spanning Tree mode.

Examples

```
-> bridge mode flat
-> show spantree mst port 1/2

MST   Role   State Pth Cst  Edge Boundary Op Cnx Loop Guard  Note  Vlans
-----+------+-----+--------+----+--------+------+----------+------+-----
    0   DIS    DIS      0    YES    YES     NS         DIS           1

-> bridge mode 1x1
-> show spantree mst port 1/10
MST   Role   State Pth Cst  Edge Boundary Op Cnx Loop Guard  Note  Vlans
-----+------+-----+--------+----+--------+------+----------+------+-----
    0   ROOT  ENA        0   YES    YES     NS         DIS           1
    2   DIS   DIS        0   YES    YES     NS         DIS
```

output definitions

MST	Indicates the MSTI ID.
Role	The role of the port for this Spanning Tree instance. Possible port roles are: **ROOT -** root, **DIS -** disable, **DESG -** designated, **ALT -** alternate**, MSTR -** master (valid only when MSTP mode is active), and **BKP -** backup.

output definitions

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.
Edge	Indicates whether or not the port is an **edge port** (**YES** or **NO**).
Boundary	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.
Op Cnx	Operational connection type: **PTP, NPT**, or **NS** (nonsignificant)**.** Shows the current operational state of the port connection type. See the **bridge connection** command for more information.
Loop Guard	Operational status of the loop-guard on a particular port or link aggregate (**ENA** or **DIS**)
Note	Indicates whether a loop-guard error (**ERR**) has occured on the MSTI instance.
Vlans	The VLAN ID of the default VLAN for the port.

Release History

Release 6.1; command introduced.

Related Commands

show spantree cist ports	Displays Spanning Tree port information for the flat mode Common and Internal Spanning Tree (CIST) instance.
show spantree msti ports	Displays Spanning Tree port information for a flat mode Multiple Spanning Tree Instance (MSTI).
show spantree 1x1 ports	Displays Spanning Tree port information for a 1x1 mode VLAN instance.

MIB Objects

```
vStpPortConfigTable
   vStpPortConfigIfIndex
   vStpPortConfigLoopGuard

vStpInsTable
   vStpIns1x1VlanNumber

vStpPortTable
   vStpPortState
   vStpPortPathCost
   vStpPortRole
```

show bridge rrstp configuration

Displays the current RRSTP status for the switch.

show bridge rrstp configuration

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show bridge rrstp configuration
RRSTP Global state is Enabled
```

Release History

Release 6.2.1; command introduced.

Related Commands

bridge rrstp	Enables or disables RRSTP on a switch.
show bridge rrstp ring	Displays information for all the rings or a specific ring present in the system.

MIB Objects

```
vStpInfo
   VStpRrstpGlobalState
```

show bridge rrstp ring

Displays information for all the rings or for a specific ring that exists in the switch configuration.

show bridge rrstp ring [*ring_id***]**

Syntax Definitions

ring_id	An existing ring ID number (1–128).

Defaults

By default displays information for all rings.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the *ring_id* parameter with this command to display information for a specific ring.

Examples

```
-> show bridge rrstp ring

      RingId     Vlan-Tag     Ring-Port1     Ring-Port2     Ring Status
  -----------+------------+---------------+--------------+---------------
       2          1000          1/19           1/10         enabled
       6            20           1/1            1/8        disabled
     128             1           0/1           0/31         enabled
```

output definitions

RingId	The numeric ID of the RRSTP ring.
Vlan-Tag	The VLAN to which the RRSTP ring frames are tagged.
Ring-Port-1	The first port in the RRSTP ring.
Ring-Port-2	The second port in the RRSTP ring.
Ring Status	The current state of the RRSTP ring (**Enabled** or **Disabled**).

Release History

Release 6.2.1; command introduced.
Release 6.3.1; **ring** parameter and **Vlan-Tag** field added.

Related Commands

bridge rrstp ring	Creates a RRSTP ring consists of two ports.
show bridge rrstp configuration	Displays the current RRSTP status for the switch.

MIB Objects

```
vStpRrstpRingConfigTable
   vStpRrstpRingId
   vStpRrstpRingPort1
   vStpRrstpRingPort2
   vStpRrstpRingVlanTag
   vStpRrstpRingState
   vStpRrstpRingRowStatus
```

7 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 is compatible only 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** **lacp linkagg wait-to-restore-timer**
Dual Home Link (DHL) Active-Standby	**lacp agg standby** **lacp linkagg pre-empt** **lacp linkagg pre-empt timer**
Dual Home Link (DHL) Active-Active	**dhl num** **dhl num linka linkb** **dhl num admin-state** **dhl num vlan-map linkb** **dhl num pre-emption-time** **dhl num mac-flushing** **show dhl** **show dhl num** **show dhl num link**
Static and dynamic	**show linkagg** **show linkagg port** **linkagg range** **show linkagg range**

static linkagg size

Creates a static aggregate group between two switches. A static aggregate group contains static links. Creates a static linkagg, where size, admin state and name are local to the chassis links.

static linkagg *agg_num* **size** *size* **[name** *name***] [admin state {enable | disable}] [multi-chassis active] min-size** *num***]**

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 (stackable products) or 0–127 (chassis-based products).
size	The maximum number of links allowed in the aggregate group. Values may be 2, 4, or 8.
name	The name of the static aggregate group. May be any alphanumeric string up to 255 characters long. Spaces must be contained within quotes. For example, “Static Group 1”.
on	Specifies that the static aggregate group is active and is able to aggregate links.
off	Specifies that the static aggregate group is inactive and not able to aggregate links.
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.
multi-chassis active	Specifies that the aggregate qualifies as MC-LAG.

Defaults

parameter	default
enable | disable	enable

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a static aggregate group from the configuration.
- The maximum number of link aggregate groups allowed on the switch (static and dynamic combined) is 32 for stackable products and 128 for chassis-based products.

- Note that a maximum of 256 link aggregation ports are supported. The number of link aggregation ports per group will determine the maximum number of groups that can be configured. The table below provides some example configurations:

Number of Ports in Group	Maximum Number of Groups
2	128
4	64
8	32

- If the static aggregate has any attached ports you must delete the attached ports with the **static agg agg num** command before you can remove the static link aggregate ID.
- Use the **lacp linkagg size** command to create a dynamic aggregation (that is, LACP) group. See page 4-197 for more information about this command.
- The **multi-chassis active** parameter must be specified at aggregate creation time. It must not be changeable while the aggregate exists after its creation.
- The **multi-chassis active** parameter should be set on both the chassis if it is a MC-LAG.

Examples

```
-> static linkagg 3 size 8 multi-chassis active
-> static linkagg 4 size 2 admin state disable
-> no static linkagg 3
```

Release History

Release 6.1; command was introduced.
Release 6.4.5; **multi-chassis active** parameter added.

Related Commands

show linkagg	Displays information about static and dynamic (LACP) link aggregate groups.

MIB Objects

```
alclnkaggAggTable
   alclnkaggAggNumber
   alclnkaggAggSize
   alclnkaggAggLacpType
   alclnkaggAggMcLagType
   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 (for example, “Static Group 1”).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the **no** form of this command to remove a name from a static aggregate.

Examples

```
-> static linkagg 2 name accounting
-> static linkagg 2 no name
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this 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. For example, all 10 Mbps, all 100 Mbps, all 1 Gigabit, or all 10 Gigabit).
- 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.
- The **ethernet**, **fastethernet**, and **gigaethernet** keywords do not modify a port's configuration. See Chapter 1, "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 6.1; 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***]**
[multi-chassis active]

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 (stackable products) or 0–127 (chassis-based products).
size	The maximum number of links that may belong to the aggregate. Values may be 2, 4, or 8.
name	The name of the dynamic aggregate group. May be any alphanumeric string up to 255 characters long. Spaces must be contained within quotes (for example, “Dynamic Group 1”).
multi-chassis active	Specifies that the aggregate qualifies as MC-LAG.
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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a dynamic aggregate group from the configuration.
- The maximum number of link aggregate groups allowed on the switch (static and dynamic combined) is 32 for stackable products and 128 for chassis-based products.
- Note that a maximum of 256 link aggregation ports are supported. The number of link aggregation ports per group will determine the maximum number of groups that can be configured. The table below provides some example configurations:

Number of Ports in Group	Maximum Number of Groups
2	**128**
4	**64**
8	**32**

- 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 4-191 for more information about this command.

Examples

```
-> lacp linkagg 2 size 4 multi-chassis active
-> lacp linkagg 3 size 2 admin state disable actor system priority 65535
```

Release History

Release 6.1; command was introduced.

Related Commands

show linkagg	Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

`alclnkaggAggTable`

```
alclnkaggAggNumber
alclnkaggAggSize
alclnkaggAggLacpType
alclnkaggAggName
alclnkaggAggMcLagType
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 (for example, “Dynamic Group 1”).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the **no** form of this command to remove a name from a dynamic aggregate group.

Examples

```
-> lacp linkagg 2 name finance
-> lacp linkagg 2 no name
```

Release History

Release 6.1; 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 is 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the **no** form of this 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 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this 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 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the **no** form of this 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 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this 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 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the **no** form of this 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 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the **no** form of this 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 6.1; 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 a port, which allows the 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 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 4-213.
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 4-219.
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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this 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 in the same speed (for example, all 100 Mbps. 1 Gigabit. or all 10 Gigabit).
- Ports that belong to the same dynamic aggregate group do not have to be configured sequentially and can be on any Network Interface (NI).
- The **ethernet**, **fastethernet**, and **gigaethernet** keywords do not modify a port's configuration. See Chapter 1, "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 6.1; 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
   alclnkaggAggPortMcLagType
   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 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 that 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 that 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 that 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 that 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 the defaulted partner information administratively configured for the partner.
expire	Specifying that 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to restore the 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 1, "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 6.1; 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 (that is, 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 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this 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 1, "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 6.1; 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 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this 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 1, "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 6.1; 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 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 that 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 that 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 the defaulted actor information administratively configured for the actor.
expire	Specifying that 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to restore the 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 1, "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 6.1; 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 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 hexadecimal format *xx:xx:xx:xx:xx:xx*.

Defaults

parameter	default
partner_admin_system_id	0

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this 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 1, "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 6.1; 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 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this 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 1, "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 6.1; 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
   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 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this 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 1, "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 6.1; 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 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this 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 1, "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 6.1; 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 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a *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 1, "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 6.1; 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 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

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a *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 1, "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 6.1; 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
```

lacp linkagg wait-to-restore-timer

Configures the wait-to-restore (WTR) timer value on the dynamic linkagg. It is disabled by default. When enabled, if the port joining the Linkagg is not the first one, the port attach in Linkagg is delayed by the WTR Timer for the required minutes.

lacp linkagg wait-to-restore timer *num*

Syntax Definitions

num	The number of minutes to delay LACP sync up to coincide with L3 convergence time. The valid range is 1-12 minutes.

Defaults

parameter	default
num	0

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- When WTR is enabled on dynamic Linkagg and if the port joining the Linkagg is not the first one, the port attach in Linkagg is delayed by the WTR Timer. Assuming that there was a first port attached in the Linkagg and another port was waiting in WTR, if the earlier port goes down then second port stops its WTR timer and joins the LACP Linkagg.
- **lacp linkagg wait-to-restore timer** is not supported on Static Linkagg.

Examples

```
-> lacp linkagg 1 wait-to-restore timer 5
-> lacp linkagg 1 wait-to-restore timer 100
ERROR: Allowed range for WTR Timer is from 1 to 12 minutes
```

Release History

Release 6.4.5; command introduced.

Related Commands

show linkagg	Displays information about static and dynamic (LACP) aggregate groups.
show linkagg port	Displays information about ports associated with a particular aggregate group or all aggregate groups.

MIB Objects

```
alclnkaggAggWTRTimer
   alclnkaggAggEntry
```

lacp agg standby

Configures the standby status for a switch port. When this status is enabled, the port is eligible to participate in a dual-home link aggregate as a standby port.

lacp agg [ethernet | fastethernet | gigaethernet] *slot*/*port* **standby {enable | disable}**

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 Gigabit Ethernet.
slot	The slot number for the standby port.
port	The port number for the standby port.

Defaults

By default, the standby functionality is disabled on a switch port.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- A dual home link aggregate consists of one active primary port and one standby port. Enabling the standby status makes a port eligible to serve as the standby port in this type of aggregate. Use this command to enable the standby status before the port is associated with the link aggregate.
- The **ethernet**, **fastethernet**, and **gigaethernet** keywords do not modify a port's configuration. See Chapter 1, "Ethernet Port Commands," for information on CLI commands to configure Ethernet ports.

Examples

```
-> lacp agg 2/1 standby enable
-> lacp agg 2/1 standby disable
```

Release History

Release 6.4.3; 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
   alclnkaggAggPortStandbyState
```

lacp linkagg pre-empt

Configures the pre-emption status for a dynamic dual-home link aggregate. When the pre-emption status is enabled, the switch will restore a downed primary port as the primary link when the port comes back up and after a configurable period of time (pre-emption delay time).

lacp linkagg *agg_num* **pre-empt {enable | disable}**

Syntax Definitions

agg_num	The number corresponding to the dynamic aggregate group.
enable	Enables the pre-emption status for the aggregate group.
disable	Disables the pre-emption status for the aggregate group.

Defaults

By default, the pre-emption status is disabled.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The dynamic aggregate group number specified with this command must already exist in the switch configuration. In addition, the aggregate should have Spanning Tree disabled.
- The amount of time the switch waits to restore a port as the primary link is determined by the value of a pre-emption delay timer. This timer value is configurable using the **lacp linkagg pre-empt timer** command.
- If the primary port fails again before the length of the pre-emption timer has elapsed, the timer value is reset and will start again when the port comes back up.
- If the pre-emption status is disabled, the standby port retains the primary status even when the original primary port comes back up. The original primary port then becomes the standby link.

Examples

```
-> lacp linkagg 2 pre-empt enable
-> lacp linkagg 2 pre-empt disable
```

Release History

Release 6.4.3; command was introduced.

Related Commands

lacp linkagg size	Creates a dynamic aggregate group.
lacp agg standby	Configures the standby status for a port. A standby port is required to configure a dual-home link aggregate.
lacp linkagg pre-empt timer	Configures the pre-emption delay timer value for the dynamic dual-home link aggregate group.
show linkagg	Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

```
alclnkaggAggTable
   alclnkaggAggNumber
   alcLnkAggPreemptState
```

lacp linkagg pre-empt timer

Configures the pre-emption delay timer value for a dynamic dual-home link aggregate. This value is the length of time the switch will wait before restoring a port to primary link status.

lacp linkagg *agg_num* **pre-empt timer** *seconds*

Syntax Definitions

agg_num	The number corresponding to the dynamic aggregate group.
seconds	The pre-emption delay timer value, in seconds. The range is 30–300.

Defaults

By default, the timer value is set to 30 seconds.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- When the primary port for a dual-home link aggregate fails and then comes back up, the switch will wait the length of the pre-emption timer value before restoring the port as the primary link for the aggregate.
- The pre-emption delay timer is only used when the pre-emption status for the specified aggregate group is enabled. The timer starts when a failed primary port comes back up.
- If the primary port goes down before the timer runs out, the timer is reset and then started again the next time the port comes back up.

Examples

```
-> lacp linkagg 2 pre-empt timer 120
-> lacp linkagg 3 pre-empt timer 300
```

Release History

Release 6.4.3; command was introduced.

Related Commands

lacp linkagg size	Creates a dynamic aggregate group.
lacp agg standby	Configures the standby status for a port. A standby port is required to configure a dual-home link aggregate.
lacp linkagg pre-empt timer	Configures the pre-emption delay timer value for the dynamic dual-home link aggregate group.
show linkagg	Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

```
alclnkaggAggTable
   alclnkaggAggNumber
   alcLnkAggPreemptValue
```

dhl num

Configures a Dual-homed Link (DHL) session associated with the specified session ID number.

dhl num *dhl_num* **[name** *name***]**

no dhl num *dhl_num*

Syntax Definitions

dhl_num	The DHL session ID number. Valid range is 1–1000.
name	The name of the DHL session.

Defaults

By default, if a name is not assigned to a DHL session, the session is configured as DHL-1.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a DHL session ID from the switch configuration.
- Use the optional **name** parameter to specify a name for the DHL session.
- Only one DHL session can be configured per switch.
- Once the DHL session ID is created, assign a link A port and a link B port to the session. This is required before administratively enabling the DHL session is allowed.

Examples

```
-> dhl num 1 name dhl_session1
-> no dhl num 1
```

Release History

Release 6.4.4; command was introduced.

Related Commands

dhl num linka linkb	Associates a pair of links (port or linkagg) with the DHL session.
dhl num admin-state	Configures the administrative status of the DHL session.
show dhl num	Displays information about a specific DHL session.

MIB Objects

```
alaDHLSessionTable
   alaDHLSessionIndex
   alaDHLSessionDescr
```

dhl num linka linkb

Configures two ports or two link aggregates or a combination of both as linkA and linkB for the specified DHL session. Only two links are allowed per DHL session; only one DHL session per switch is allowed.

dhl num *dhl_num* **linka {port** *slot/port* **| linkagg** *agg_id***} linkb {port** *slot/port* **| linkagg** *agg_id***}**

no dhl num *dhl_num* **linka {port** *slot/port* **| linkagg** *agg_id***} linkb {port** *slot/port* **| linkagg** *agg_id***}**

Syntax Definitions

dhl_num	An existing DHL session ID number.
slot	The slot number number to designate as a link for the DHL session.
port	The physical port number to designate as a link for the DHL session.
agg_id	The link aggregate ID number to designate as a link for the DHL session.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove the linkA and linkB ports from the specified session ID. Before attempting to remove the links, administratively disable the DHL session.
- Make sure that DHL linkA *and* linkB are associated with each VLAN that the DHL session will protect. Any VLAN not associated with either link or only associated with one of the links is unprotected.
- DHL linkA *and* linkB should belong to the same default VLAN. In addition, select a default VLAN that is one of the VLANs that the DHL session will protect. For example, if the session is going to protect VLANs 10-20, then assign one of those VLANs as the default VLAN for linkA and linkB.
- Only one DHL session per switch is allowed. Each session can have only two links (linkA and linkB). Specify a physical switch port or a link aggregate (linkagg) ID as a DHL link. The same port or link aggregate is not configurable as both linkA or linkB.
- DHL is not supported on mobile, 802.1x-enabled, GVRP, or UNI ports. DHL is also not supported on a port that is a member of a link aggregate or a port the is enabled for transparent bridging.
- The administrative state of a DHL session is not configurable until a linkA port and a linkB port are associated with the specified DHL session ID number.
- Changing the port designations for linkA and linkB is not recommended while the DHL session is enabled.
- Removing a link aggregate from the switch configuration is not allowed if the aggregate is configured as a link for a DHL session.

Examples

```
-> dhl num 1 linka port 1/1 linkb port 1/2
-> dhl num 1 linka  linkagg 1  linkb port 1/2
-> dhl num 1 linka port 1/1 linkb linkagg 1
-> dhl num 1 linka  linkagg 1  linkb linkagg 2
-> no dhl num 1 linka port 1/1 linkb port 1/2
```

Release History

Release 6.4.4; command was introduced.

Related Commands

dhl num	Configures a session ID for the DHL session.
dhl num admin-state	Configures the administrative status for the DHL session.
show dhl	Displays the global status of the DHL configuration.
show dhl num	Displays information about a specific DHL session.
show dhl num link	Displays information about a specific link.

MIB Objects

```
AlaDHLLinksTable
   alaDHLLinksSessionIndex
   alaDHLLinkslinkA
   alaDHLLinkslinkB
```

dhl num admin-state

Enables or disables the administrative state of a DHL session.

dhl num *dhl_num* **admin-state {enable | disable}**

Syntax Definitions

dhl_num	An existing DHL session ID number.
enable	Enables the DHL session.
disable	Disables the DHL session.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The DHL session ID specified with this command must already exist in the switch configuration.
- The administrative state is not configurable until a linkA port and a linkB port are associated with the specified DHL session ID number.

Examples

```
-> dhl num 1 admin-state enable
-> dhl num 1 admin-state disable
```

Release History

Release 6.4.4; command was introduced.

Related Commands

dhl num	Configures a session ID for the DHL session.
dhl num admin-state	Configures the administrative status for the DHL session.
show dhl	Displays the global status of the DHL configuration.
show dhl num	Displays information about a specific DHL session.

MIB Objects

```
alaDHLSessionTable
   alaDHLSessionAdminStatus
```

dhl num vlan-map linkb

Configures a VLAN-MAP (a single VLAN or a range of VLANs) from a common pool of VLANs to operate on DHL link B.

dhl num *dhl_num* **vlan-map linkb {***vlan_id***[-***vlan_id***]}**

no dhl num *dhl_num* **vlan-map linkb {***vlan_id***[-***vlan_id***]}**

Syntax Definitions

dhl_num	Specifies the DHL session ID number.
*vlan_id***[-***vlan_id***]**	A VLAN ID number or a range of VLAN IDs to map to linkB. The valid range is 1- 4094.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- A DHL session has to be created before a VLAN-MAP can be configured.
- When the DHL session is active, the common VLAN that both the dual homed links belong to is treated as a protected VLAN. The VLAN containing only one dual homed link is treated as an unprotected VLAN. Traffic is forwarded only on the dual homed links belonging to the protected VLAN.
- If a VLAN is removed globally and if the VLAN belongs to a particular dual homed link, then the VLAN will automatically be removed from the dual homed link.
- If one dual homed link, for example linkA, is moved out of a protected VLAN, then the VLAN becomes unprotected and the VPA is removed from the second dual homed link, for example linkB.
- If the admin state of a VLAN is changed to disabled, and if the VLAN is part of a protected VLAN, then the disabled VLAN is removed from the operational DHL VLAN list but will be present in the protected VLAN list.
- If the admin state of a dual homed link, for example linkA, is changed to disabled, then the protected VLANs of the disabled linkA is moved to the other link, for example linkB. When linkA is re-enabled, then the VLANs are moved back to linkA.
- If the VLAN-MAP of linkB is removed, then the VPAs for the linkB will also be removed and the VLANs configured on linkB is moved to linkA.
- If a VLAN is configured as default on one dual homed link, for example linkA, then the same VLAN cannot be configured as tagged on the other link, for example linkB.

Examples

```
-> vlan 10-30
-> vlan 10-20 802.1q 1/1
-> vlan 4
-> vlan port default 1/1-2
-> dhl num 1 name dhl_session1
-> dhl num 1 linka port 1/1 linkb port 1/2
-> dhl num 1 vlan-map linkb 18-20
-> no dhl num 1 vlan-map linkb 18-20
```

Release History

Release 6.4.4; command was introduced.

Related Commands

dhl num	Configures a session ID for the DHL session.
dhl num admin-state	Configures the administrative status for the DHL session.
show dhl	Displays the global status of the DHL configuration.
show dhl num	Displays information about a specific DHL session.
show dhl num link	Displays information about a specific link.

MIB Objects

```
alaDHLVlanMapTable
   alaDHLVlanMapSessionIndex
   alaDHLVlanMapVlanStart
   alaDHLVlanMapVlanEnd
   alaDHLVlanMapRowStatus
```

dhl num pre-emption-time

Configures the pre-emption timer for the DHL session. A pre-emption timer is a recovery-delay timer that is used to delay the switchover of VLANs to their primary links. It is the delay in the resumption of traffic when a link that is down is brought up.

dhl num *dhl_num* **pre-emption-time** *num*

Syntax Definitions

dhl_num	Specifies the number of the DHL session.
num	Specifies the number of seconds for the delay in the switchover of VLANs to their primary links. The valid range is 0 - 600.

Defaults

parameter	default
num	30 seconds

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Pre-emption timer is applicable only when a failed port is brought up. If both ports are down, the pre-emption timer is activated only when the second port is brought up.
- If the pre-emption value is set to 0, then there will be no delay in the VLANs being moved back to their primary link.
- If a link fails when the pre-emption value is active, that is when the pre-emption value is not equal to 0, then the time will be halted.
- When the pre-emption timer is active for a particular link and port and if the other port goes down, then the VLANs of the port that is down is automatically moved to the port for which the pre-emption timer is active.
- When DHL ports spanned across the NIs or DHC ports are on the same NI but data port is on different NI, it is advised to configure mac-flush mechanism (either Raw/MVRP) for faster convergence.

Examples

```
-> dhl num 1 pre-emption-time 40sec
```

Release History

Release 6.4.4; command was introduced.

Related Commands

dhl num	Configures a session ID for the DHL session.
show dhl	Displays the global status of the DHL configuration.
show dhl num	Displays information about a specific DHL session.
show dhl num link	Displays information about a specific link.

MIB Objects

```
alaDHLSessionTable
   alaDHLSessionPreemptionTime
```

dhl num mac-flushing

Configures the MAC-flushing technique for the DHL session. The MAC-flushing technique is used to correct any stale MAC entries that are caused when a dual homed link goes down.

dhl num *dhl_num* **mac-flushing {none | raw | mvrp}**

Syntax Definitions

dhl_num	Specifies the number of the DHL session.
none	Flushing of the MAC address tables does not occur.
raw	Method of flushing when VPAs of the links moved across them due to link up/down or configuration change (VLAN-map). The switch determines the MAC addresses within the affected VLANs
mvrp	Method of flushing when one link fails, and the other link issues 'join' declarations to establish connectivity. These new joins are flagged as 'new' and they are forwarded by the core devices causing flushing on the core network for the active VLANs.

Defaults

parameter	default
none | raw | mvrp	**none**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Before enabling MVRP on dual homed links, the Registrar Mode should be set to 'forbidden', failing which an error message is displayed when configuring DHL. If the Registrar Mode is set to 'not forbidden, then changes cannot be made to the MVRP configuration on the dual homed links.
- If the mac-flushing technique is set to MVRP and if MVRP is not enabled on the dual homed links, then the **show dhl** command displays the active mac-flushing technique as **none**. When MVRP is enabled on the dual homed links, then the mac-flushing technique changes to **MVRP** and the Registrar Mode of the links is automatically set to ‘forbidden’.
- If VLANs are moved across the dual homed links as a result of configuration changes, then mac-flushing is automatically enabled, if configured, excepting dual homed links that are changed on the fly.

Examples

```
-> dhl num 1 mac-flushing none
-> dhl num 1 mac-flushing raw
```

Release History

Release 6.4.4; command was introduced.

Related Commands

dhl num	Configures a session ID for the DHL session.
show dhl	Displays the global status of the DHL configuration.
show dhl num	Displays information about a specific DHL session.
show dhl num link	Displays information about a specific link.

MIB Objects

```
alaDHLSessionTable
   alaDHLSessionMacFlushingtech
```

show dhl

Displays the global status of the DHL configuration.

show dhl

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show DHL
 Number  Name    Admin    Oper     Pre-emption    Mac-flushing   Active Mac-flushing
                 state    state    time
-------+------+--------+-------+-----------+-----------------+--------------------
  1      DHL-1   UP       UP      30sec          Raw                 Raw
```

output definitions

Number	Number of the DHL session.
Name	The user-defined text description of the DHL session.
Admin state	The administrative status of the DHL session.
Oper state	The operational status of the DHL session.
Pre-emption time	The pre-emption time in seconds of the DHL session.
Mac-flushing	Mac-flushing technique on the DHL session.
Active Mac-flushing	Mac-flushing technique that is currently active on the DHL session.

Release History

Release 6.4.4; command was introduced.

Related Commands

dhl num	Configures a session ID for the DHL session.
show dhl num	Displays information about a specific DHL session.
show dhl num link	Displays information about a specific link.

MIB Objects

```
alaDHLSessionTable
   alaDHLSessionIndex
   alaDHLSessionDesc
   alaDHLSessionAdminStatus
   alaDHLSessionOperStatus
   alaDHLSessionPreemptionTime
   alaDHLSessionMacFlushingtech
```

show dhl num

Displays information about a specific DHL session.

show dhl num *dhl_num*

Syntax Definitions

dhl_num	Specifies the number of the DHL session.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show dhl num 1
DHL session name              : Arice,
Admin state                   : Up,
Operational state             : Up,
Pre-emption time              : 40 sec,
Mac-flushing                  : Raw-Flushing,
Active Mac-flushing           : Raw-Flushing,

Protected VLANs               : 10-20,23,25,30-100,600,700,800,

linkA:
  Port                        : 1/2,
  Operational state           : Up

  Un protected VLANs           : 900,1980,1987,234,
  Active VLAN                 : 10-20,23,25,30-100,600,700,800,

linkB:
  Port                        : 1/1,
  Operational state           : Down,
  Un protected VLANs          : 1730-1800,
  Vlan-map                    : 30-100,600,
  Active Vlans                :  none,
```

output definitions

DHL session Name	The user-defined text description of the DHL session.
Admin state	The current administrative status of the DHL session.
Operational state	The operational state of the DHL session.

output definitions

Pre-emption time	The delay-interval in seconds to move the VLANs back to their original links.
Mac-flushing	Mac-flushing technique on the DHL session.
Active Mac-flushing	The active Mac-flushing technique that is enabled on the specified DHL session.
Protected VLANs	The common VLANs that contain both the dual homed links, for example linkA and linkB.
LinkA	A dual homed link that is part of a pair of DHL links that can be configured per switch.
Port	The port number of linkA.
Operational state	The operational state of the port. The operational states are UP or DOWN.
Un protected VLANs	The VLANs containing only one dual homed link.
Active VLANs	The VLANs that are in an active state.
LinkB	A dual homed link that is part of a pair of DHL links that can be configured per switch.
Port	The port number of linkB.
Operational state	The operational state of the port. The operational states are UP or DOWN.
Un protected VLANs	The VLANs containing only one dual homed link.
VLAN-map	The DHL VLAN map for linkB. This specifies the VLANs that are operational on DHL linkB from the common pool of VLANs between DHL linkA and linkB.
Operational VLANs	The VLANs that are in an operational state.

Release History

Release 6.4.4; command was introduced.

Related Commands

dhl num	Configures a session ID for the DHL session.
show dhl num link	Displays information about a specific link.

MIB Objects

```
alaDHLSessionTable
   alaDHLSessionIndex
   alaDHLSessionDescr
   alaDHLSessionAdminStatus
   alaDHLSessionOperStatus
   alaDHLSessionPreemptionTime
   alaDHLSessionMacFlushingtech
alaDHLLinksTable
   alaDHLLinksSessionIndex
   alaDHLLinkslinkA
```

```
   alaDHLLinkslinkAOperStatus
   alaDHLLinkslinkB
   alaDHLLinkslinkBOperStatus
alaDHLVlanMapTable
   alaDHLVlanMapSessionIndex
   alaDHLVlanMapVlanStart
   alaDHLVlanMapVlanEnd
alaDHLVpaTable
   alaDHLVpalink
   alaDHLVpaVlan
   alaDHLVpaVlanType
   alaDHLVpaOperationalLink
```

show dhl num link

Displays information about a specific DHL link, for example linkA or linkB and the VLAN details of the specified link.

show dhl num *dhl_num* **[linkA | linkB]**

Syntax Definitions

dhl_num	Specifies the number of the DHL session.
linkA	The dual homed link that is part of a pair of DHL links that can be configured per switch.
linkB	The dual homed link that is part of a pair of DHL links that can be configured per switch.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show dhl num 1 linkA

linkA:
  Port                        : 1/2,
  Operational state           : Up,

  Protected VLANs             : 10-20, 23, 25, 30-100,600,700,800,
  Un protected VLANs          : 900, 1980, 1987,234,
  Active VLAN                 : 10-20, 23, 25, 30-100,600,700,800,
```

Release History

Release 6.4.4; command was introduced.

Related Commands

dhl num	Configures a session ID for the DHL session.
dhl num linka linkb	Configures a port or a link aggregate as dual homed links (linkA, linkB) of a DHL session.
dhl num vlan-map linkb	Configures a VLAN or a range of VLANs from a common pool to operate on DHL linkB.
show dhl num	Displays information about a specific DHL session.

MIB Objects

```
alaDHLLinksTable
   alaDHLLinksSessionIndex
   alaDHLLinkslinkA
   alaDHLLinkslinkAOperStatus
   alaDHLLinkslinkB
alaDHLVpaTable
   alaDHLVpalink
   alaDHLVpaVlan
   alaDHLVpaVlanType
   alaDHLVpaOperationalLink
alaDHLVlanMapTable
   alaDHLVlanMapSessionIndex
   alaDHLVlanMapVlanStartala
   alaDHLVlanMapVlanEnd
```

show linkagg

Displays information about static and dynamic (LACP) aggregate groups.

show linkagg [*agg_num***] port [***slot***/***port***]**

Syntax Definitions

agg_num	Specifies the aggregate group. Configured through the **static linkagg size** or **lacp linkagg size** command.
slot	The slot number for this aggregate.
port	The port number for this aggregate.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 is displayed only. 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 100
Number  Aggregate  SNMP Id  Size  Min Size Admin State  Oper State Att/Sel Ports
-------+----------+--------+----+------------+------------+----------------
   1     Static    40000001   8    1      ENABLED      UP             2   2
   2     Dynamic   40000002   4   1       ENABLED      DOWN           0   0
   3     Dynamic   40000003   8    1      ENABLED      DOWN           0   2
   4     Dynamic   40000004   8    1      ENABLED      UP             3   3
   5     Static    40000005   2    1       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 4-194) for static aggregate groups and with the **lacp linkagg admin state** command (see page 4-201) for dynamic aggregate groups.
Operational State	The current operational state of the aggregate group, which can be **UP** or **DOWN**.
Sel Ports	The number of ports that could possibly attach to the aggregate group.
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,
  Aggregate minimum size   : 1,
  Number of Selected Ports : 0,
  Number of Reserved Ports : 0,
  Number of Attached Ports : 0,
  Primary Port             : NONE
```

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 4-193).
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 4-194).
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 1
Dynamic Aggregate
  SNMP Id                   : 40000001,
  Aggregate Number          : 1,
  SNMP Descriptor           : Dynamic Aggregate Number 1 ref 40000001 size 2,
  Name                      : AGG 2,
  Admin State               : ENABLED,
  Operational State         : UP,
  Aggregate Size            : 2,
  Aggregate minimum size    : 1,
  Number of Selected Ports  : 1,
  Number of Reserved Ports  : 1,
  Number of Attached Ports  : 8,1
  Primary Port              : NONE
LACP
  MACAddress                : [e8:e7:32:3e:a3:94],
  Actor System Id           : [00:e0:b1:94:d0:38],
  Actor System Priority     : 0,
  Actor Admin Key           : 1,
  Actor Oper Key            : 1,
  Partner System Id         : [e8:e7:32:39:ca:00],
  Partner System Priority   : 0,
  Partner Admin Key         : 0,
  Partner Oper Key          : 1,
  Pre-emption               : DISABLED,
  Pre-empt Value            : 30
  Wait-to-restore timer     : 5
```

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 4-200).
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 4-201).
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.

output definitions (continued)

Number of Attached Ports	The number of ports actually attached to this dynamic aggregate group.
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 4-205).
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 4-204).
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 4-203).
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 4-206).
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 4-208).
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 4-209).
Partner Oper Key	The operational key of the remote system to which the dynamic aggregation group is attached.
Pre-emption	The pre-emption status of the link agg ID.
Pre-empt Value	The value of the pre-emption timer.
Wait-to-restore timer	The value of WTR delay. Configures the wait-to-restore timer value on the dynamic linkagg. It is disabled by default. When enabled, if the port joining the Linkagg is not the first one, the port attach in Linkagg is delayed by WTR Timer by the required minutes. You can modify this parameter with the **lacp linkagg wait-to-restore-timer** command (see page 7-45).

Release History

Release 6.1; command was introduced.
Release 6.4.3: **Pre-emption** and **Pre-empt Value** fields added.
Release 6.4.5; **Wait-to-restore timer** status added in output.

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
- alclnkaggAggPortLacpType
- alclnkaggAggMcLagType
- alclnkaggAggNbrSelectedPorts
- alclnkaggAggNbrAttachedPorts
- alclnkaggPrimaryPortIndex
- alclnkaggAggMACAddress
- alclnkaggAggActorSystemPriority
- alclnkaggAggActorSystemID
- alclnkaggAggPartnerAdminKey
- alclnkaggAggActorAdminKey
- alclnkaggAggActorOperKey
- alclnkaggAggPartnerSystemID
- alclnkaggAggPartnerSystemPriority
- alclnkaggAggPartnerOperKey
- alclnkaggAggPreemptState
- alclnkaggAggPreemptValue

show linkagg port

Displays the aggregate group information about a particular slot and port.

show linkagg [*agg_num***] port [***slot/port***]**

Syntax Definitions

agg_num	Specifies the aggregate group. Configured through the **static linkagg size** or **lacp linkagg size** command
slot	The slot number for this aggregate.
port	The port number for this aggregate.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- If no *slot/port* is specified, the information for all 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.
- If no *agg_num* is specified, the information for all aggregates is displayed.

Examples

```
-> show linkagg port
Slot/Port Aggregate SNMP Id   Status   Agg  Oper Link Prim Standby
---------+---------+-------+----------+----+----+----+----+--------
   1/9    Static      1009  ATTACHED     1  UP   UP   YES   NO
   1/10   Static      1010  ATTACHED     1  UP   UP   NO    YES
   1/11   Static      1011  ATTACHED     2  UP   UP   YES   NO

-> show linkagg 1 port
Slot/Port Aggregate SNMP Id   Status   Agg  Oper Link Prim Standby
---------+---------+-------+----------+----+----+----+----+--------
   1/9    Static      1009  ATTACHED     1  UP   UP   YES   NO
   1/10   Static      1010  ATTACHED     1  UP   UP   NO    YES
```

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**.

output definitions

SNMP Id	The SNMP ID associated with the aggregate group.
Status	The current status of the port (**ATTACHED, CONFIGURED**, **PENDING**, **SELECTED**, or **RESERVED**).
Agg	The number of the aggregate groups associated with this port.
Oper	The current operational state of the port (**UP** or **DOWN**).
Link	The current operational state of the link from this port to its remote partner (**UP** or **DOWN**).
Prim	Whether or not the port is the primary port in the link agg.
Standby	Whether or not the port is a standby port. A standby port is one of two ports that participate in a dynamic dual-home link aggregate. Configured through the **lacp agg standby** command.

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 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 (**ENABLED** or **DISABLED**).
Operational State	The current operational state of the port (**UP** or **DOWN**).
Port State	The current operational state of the port (**CONFIGURED**, **PENDING**, **SELECTED**, or **RESERVED**).
Link State	The current operational state of the link from this port to its remote partner (**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 (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
  Standby State                 : ENABLED
```

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 (**ENABLED** or **DISABLED**).
Operational State	The current operational state of the port (**UP** or **DOWN**).
Port State	The current operational state of the port (**CONFIGURED**, **PENDING**, **SELECTED**, or **AGGREGATED**).
Link State	The current operational state of the link from this port to its remote partner (**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.
Actor System Priority	The actor system priority of this port. Configured through the **lacp agg actor system priority** command.
Actor System Id	The actor system ID (that is, MAC address) of this port. Configured through the **lacp agg actor system id** command.
Actor Admin Key	The actor administrative key value for this port. Configured through the **lacp agg actor admin key** command.

output definitions (continued)

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. Configured through the **lacp agg partner admin system priority** command.
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. Configured through the **lacp agg partner admin system id** command.
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. Configured through the **lacp agg partner admin key** command.
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. Configured through the **lacp agg actor port priority** command.
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. Configured through the **lacp agg partner admin port** command.
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. Configured through the **lacp agg partner admin port priority** command.
Partner Oper Port Priority	The priority value assigned to the this port by the partner.
Actor Admin State	The administrative state of the port. Configured through the **lacp agg actor admin state** command.
Actor Oper State	The current operational state of the port.
Partner Admin State	The administrative state of the partner's port. Configured through the **lacp agg partner admin state** command.

output definitions (continued)

Partner Oper State	The current operational state of the partner's port.
Standby State	The standby state of the port. This value indicates if the port will participate as a standby port in a dynamic dual-home link aggregate. Configured through the **lacp agg standby** command.

Release History

Release 6.1; command was introduced.
Release 6.3.4; *agg_num* parameter added.
Release 6.4.3; **Standby** field added.

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
   alclnkaggAggMcLagType
   alclnkaggAggPortActorPort
   alclnkaggAggPortActorPortPriority
   alclnkaggAggPortPartnerAdminPort
   alclnkaggAggPortPartnerOperPort
   alclnkaggAggPortPartnerAdminPortPriority
   alclnkaggAggPortPartnerOperPortPriority
   alclnkaggAggPortActorAdminState
   alclnkaggAggPortActorOperState
   alclnkaggAggPortPartnerAdminState
   alclnkaggAggPortPartnerOperState
   alclnkaggAggPortStandbyState
```

linkagg range

Modifies the range of standard and MC-LAG link aggregation identifiers.

linkagg range local {*agg_num-agg_num* } **peer** {*agg_num-agg_num*} **multi-chassis** {*agg_num-agg_num*}

Syntax Definitions

agg_num	The first or last identifier in the range.
local	The range of standard local aggregate identifiers.
peer	The range of standard peer aggregate identifiers.
multi-chassis	The range of MC-LAG aggregate identifiers.

Defaults

parameter	default
local	0 - 127 when multi-chassis is disabled and 0 - 31 when multi-chassis is enabled
peer	Not applicable when multi-chassis is disabled and 32 - 63 when multi-chassis is enabled
MC-LAG	Not applicable when multi-chassis is disabled and 65 - 127 when multi-chassis is enabled

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- The local range configured on the local chassis must match the remote range configured on the peer chassis and vice-versa. Otherwise, the multi-chassis feature will not be operational.
- The switch must be rebooted for the ranges to take affect.
- The local range configured on the local chassis must match the remote range configured on the peer chassis and vice-versa. Otherwise, the multi-chassis feature will not be operational.
- None of the ranges can overlap.
- The end of the range must always be greater than the start. In other words, each range must have at least one aggregate number assigned to it.
- The range specified for the MC-LAG aggregates must be the same on both chassis.
- Use this command in conjunction with the MC-LAG feature to change the maximum number of MC-LAG link aggregates that can be configured.
- The maximum number of combined standard and MC-LAG link aggregates is 128.

Examples

```
-> linkagg range local 0-47 peer 48-95 multi-chassis 96-127
-> linkagg range local 48-95 peer 0-47 multi-chassis 96-127
```

Release History

Release 6.4.5; command introduced.

Related Commands

show linkagg range Displays the link aggregate range.

MIB Objects

```
alclnkAggLocalRangeConfiguredMin
alclnkAggLocalRangeConfiguredMax
alclnkAggLocalRangeOperMin
alclnkAggLocalRangeOperMax
alclnkAggPeerRangeConfiguredMin
alclnkAggPeerRangeConfiguredMax
alclnkAggPeerRangeOperMin
alclnkAggPeerRangeOperMax
alclnkAggMcLagRangeConfiguredMin
alclnkAggMcLagRangeConfiguredMax
alclnkAggMcLagRangeOperMin
alclnkAggMcLagRangeOperMax
```

show linkagg range

Displays information about the configured or operational link aggregate range identifiers for standard and MC-LAG link aggregates.

show linkagg range [operation | config]

Syntax Definitions

operation	Indicates the values currently in effect in the system.
config	Indicates the values that takes effect after the next reset.

Defaults

N/A

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **operation** parameter to display only the operational link aggregate identifiers.
- Use the **config** parameter to display only the configured link aggregate identifiers.
- A chassis reboot is required for the configured values to become operational.

Examples

```
> show linkagg range

LAG                   Operational              Configured
                      Min         Max          Min           Max
--------------------+--------+----------+--------------+-------------
Local                   0         47              0         47
Peer                   48         95             48         95
Multi-Chassis          96        127             96        127

-> show linkagg range operation
                      Operational
                      Min       Max
--------------------+--------+---------
Local                   0        47
Peer                   48        95
Multi-Chassis          96       127
```

```
-> show linkagg range config
                       Configured
                       Min       Max
--------------------+--------+--------
Local                    0        47
Peer                    48        95
Multi-Chassis           96       127
```

Release History

Release 6.4.5; command introduced.

Output Definations

Operational	Operational parameters that are currently being used by the system.
Configured	Parameters that are configured and that are implemented after switch reset.
local	0 - 127 when multi-chassis is disabled and 0 - 31 when multi-chassis is enabled.
peer	Not applicable when multi-chassis is disabled and 32 - 63 when multi-chassis is enabled.
MC-LAG	Not applicable when multi-chassis is disabled and 65 - 127 when multi-chassis is enabled.

Related Commands

linkagg range	Configure the ranges for aggregate numbers.

MIB Objects

```
alclnkAggLocalRangeConfiguredMin
alclnkAggLocalRangeConfiguredMax
alclnkAggLocalRangeOperMin
alclnkAggLocalRangeOperMax
alclnkAggPeerRangeConfiguredMin
alclnkAggPeerRangeConfiguredMax
alclnkAggPeerRangeOperMin
alclnkAggPeerRangeOperMax
alclnkAggMcLagRangeConfiguredMin
alclnkAggMcLagRangeConfiguredMax
alclnkAggMcLagRangeOperMin
alclnkAggMcLagRangeOperMax
```

8 Multi-Chassis Commands

Multi-Chassis Virtual-Fabric Aggregation (MC-VFA) enables dual homing of any standard based edge switches to two or more aggregation switches without running the Spanning Tree protocols between the edge and aggregation devices. The feature operates in a mode whereby all ports that are members of the multi-chassis aggregates are actively forwarding traffic. The overall system provides fast fail-over with a bound convergence time for all cases when edge uplinks fail.

MIB information for the Multi-Chassis commands is as follows:

Filename: ALCATEL-IND1-MULTI-CHASSIS-MIB.mib
Module: alcatelIND1MultiChassisMIB

A summary of available commands is listed here:

multi-chassis chassis-id hello-interval
multi-chassis hello-interval
multi-chassis hello-interval
multi-chassis chassis-group
multi-chassis ipc-vlan
multi-chassis loop-detection
multi-chassis loop-detection transmit-interval
multi-chassis vf-link create
multi-chassis vf-link member-ports
multi-chassis vf-link default-vlan
multi-chassis vip-vlan
show multi-chassis status
show multi-chassis loop-detection
show multi-chassis vf-link
show multi-chassis vf-link member-port
show multi-chassis consistency
show multi-chassis consistency linkagg
clear multi-chassis loop-detection

multi-chassis chassis-id hello-interval

Assigns a globally unique chassis identifier to the switch and enables the switch to operate in multi-chassis mode.

multi-chassis chassis-id *chassis_id* **[hello-interval** *interval***]**

no multi-chassis chassis-id *chassis_id* **[hello-interval** *interval***]**

Syntax Definitions

chassis_id	Chassis identifier within the multi-chassis operational range 1 - 2. The chassis identifier must be globally unique within the set of switches configured to provide multi-chassis services.
interval	Time interval, in seconds, in which multi-chassis control hello messages are to be sent to the peer switch.The range is [1 - 10].

Defaults

parameter	default
chassis_id	0 (standalone or no multi-chassis operation allowed)
interval	5 seconds

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- A globally unique chassis identifier within the range [1 - 2] must be assigned through the management interface for the multi-chassis feature to be operational. Use the **no** form of this command to change the chassis ID back to “0” (the default). If the chassis identifier is equal to “0”, then the switch operates in a standalone mode and all multi-chassis related configuration commands are no longer active for the switch.
- Switches having the same chassis identifier are not allowed to operate in a multi-chassis mode. If a duplicate chassis identifier is configured, the multi-chassis functionality will remain in a “down” operational state.
- Configuration to the chassis ID value is effective after the switch reboot.
- The hello protocol parameters must match between peer chassis as well.
- MC-LAG is only supported between two peer switches of the same type and when both switches are running the same version of AOS Release 6. For example, MC-LAG is not supported between an OmniSwitch 9000E and another OmniSwitch version.

Examples

```
-> multi-chassis chassis-id 1
-> no multi-chassis chassis-id 1
-> multi-chassis chassis-id 1 hello-interval 1
```

Release History

Release 6.4.5; command introduced.

Related Commands

show multi-chassis status	Displays the configured and operational parameters related to the multi-chassis feature on the switch.
show multi-chassis consistency	Displays the system level mandatory consistency parameters of both the local and peer switches.

MIB Objects

```
multiChassisConfig
    multiChassisConfigChassisId
    multiChassisConfigHelloInterval
```

multi-chassis hello-interval

Configures the multi-chassis hello-interval parameter on the switch. Hello packets are sent periodically on the virtual fabric link (VFL) interfaces to establish a relationship and bidirectional communication between multi-chassis peer switches. The hello-interval value determines how often these packets are sent.

multi-chassis hello-interval *interval*

Syntax Definitions

interval	Time interval, in seconds, in which multi-chassis control hello messages are to be sent to the peer switch within the range 1 - 10.

Defaults

parameter	default
interval	5 seconds

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- This command is available only on switches that are configured with a valid multi-chassis chassis ID number (1-2).
- The hello-interval is a mandatory consistency parameter between two multi-chassis peer switches. The MC-LAG protocol will not be established between the peer switches if each switch is configured with a different hello-interval value. The hello protocol parameters must match between peer chassis as well. Consistency parameters are parameters that are checked to verify that they meet the rules of the parameter and are termed to be consistent and bring up MC-LAG.
- lf the switches are configured with different hello-interval values, any change to the hello-interval value is effective after the switch reboot.

Examples

```
-> multi-chassis hello-interval 2
```

Release History

Release 6.4.5; command introduced.

Related Commands

multi-chassis chassis-id hello-interval	Assigns a globally unique chassis identifier to the switch and enables or disables the switch to operate in multi-chassis mode.
multi-chassis ipc-vlan	Configures the IPC-VLAN parameter, which is used for multi-chassis control communication, on the local switch.
show multi-chassis status	Displays the configured and operational parameters related to the multi- chassis feature on the switch.
show multi-chassis consistency	Displays the system level mandatory consistency parameters of both the local and peer switches.

MIB Objects

```
multiChassisConfig
   multiChassisConfigHelloInterval
```

multi-chassis chassis-group

Assigns a globally unique chassis group identifier to a multi-chassis peer switch. Each switch in a multi-chassis domain must use the same group ID. The group ID uniquely identifies a pair of switches operating in a multi-chassis mode.

multi-chassis chassis-group *num*

Syntax Definitions

num	Chassis group identifier. The valid range is 0–255.

Defaults

parameter	default
num	0

Platforms Supported

OmniSwitch 9000E

Usage Guidelines:

- The chassis group identifier is a mandatory consistency parameter between two multi-chassis peer switches. The MC-LAG protocol will not be established between the peer switches if each switch is configured with a different chassis-group identifier number.
- This command is only available on switches that are configured with a valid multi-chassis chassis ID.
- Use the **no** form of this command to set the chassis group ID to zero (the default).
- Each multi-chassis domain must use a different group ID number to differentiate the domain within the network environment. This helps to avoid duplicate MAC address scenarios in a network topology that may contain more than one MC-LAG domain (for example, in a back-to-back MC-LAG topology).
- Two chassis that are part of the same multi-chassis pair must have the same chassis group ID, whereas chassis belonging to different pairs must have different chassis group ID.
- There is no automatic detection or correction if two different multi-chassis domains are configured with the same group ID. Ensure each domain within the network uses a group ID number that is only associated with that domain. If the user modifies the chassis group ID at runtime causing an inconsistency, the Multi-Chassis Manager (MCM) protocol goes down after the 30 seconds consistency window. If MCM protocol goes down, the *show multi-chassis status* displays the status as “down” and the chassis behaves like an independent chassis. The applications gets a multi-chassis down event and will not be aware of the other chassis.

Examples

```
-> multi-chassis chassis-group 2
-> no multi-chassis num
```

Release History

Release 6.4.5; command introduced.

Related Commands

multi-chassis chassis-id hello-interval	Assigns a globally unique chassis identifier to the switch and enables or disables the switch to operate in multi-chassis mode.
multi-chassis ipc-vlan	Configures the IPC-VLAN parameter, which is used for multi-chassis control communication, on the local switch.
show multi-chassis status	Displays the configured and operational parameters related to the multi- chassis feature on the switch.
show multi-chassis consistency	Displays the system level mandatory consistency parameters of both the local and peer switches.

MIB Objects

```
multiChassisConfig
   multiChassisConfigChassisGroup
```

multi-chassis ipc-vlan

Configures the multi-chassis control VLAN on the switch. The multi-chassis control VLAN must be configured with the same VLAN ID on all the switches that will operate in multi-chassis mode.

multi-chassis ipc-vlan *vid*

Syntax Definitions

vid	A VLAN ID number. The valid range is 2 - 4094.

Defaults

parameter	default
vid (Multi-chassis control VLAN)	4094

Platforms Supported

OmniSwitch 9000E

Usage Guidelines.

- This command is only supported on switches that are configured with a valid multi-chassis chassis ID number (1 or 2).
- Specify a VLAN ID that does not exist in the switch configuration. This command will automatically create the VLAN as a multi-chassis control VLAN.
- The control VLAN is a mandatory consistency parameter between two multi-chassis peer switches. The MC-LAG protocol will not come up between the peer switches if each switch is configured with a different parameter.
- Any configuration to the VLAN ID value is effective after the switch reboot.
- The VLAN configured as multi-chassis control VLAN is shown as a different VLAN type.
- No front-panel ports (user ports) can be manually configured as members of the multi-chassis control VLAN and that VLAN cannot be disabled.
- Spanning tree configuration commands are not allowed on the multi-chassis control VLAN.
- VLAN 1 is not allowed to be configured as the multi-chassis control VLAN.

Examples

```
-> multi-chassis ipc-vlan 4094
```

Release History

Release 6.4.5; command introduced.

Related Commands

multi-chassis chassis-id hello-interval	Assigns a globally unique chassis identifier to the switch and enables or disables the switch to operate in multi-chassis mode.
multi-chassis hello-interval	Configures the multi-chassis hello-interval parameter on the switch.
show multi-chassis status	Displays the configured and operational parameters related to the |multi- chassis feature on the switch.
show multi-chassis consistency	Displays the system level mandatory consistency parameters of both the local and peer switches.

MIB Objects

```
multiChassisConfig
   multiChassisConfigIpcVlan
```

multi-chassis loop-detection

Configures the multi-chassis loop-detection function on the switch that is used to detect loops and automatically disable offending ports where the loop-detection control packets originated by the local switch are received.

multi-chassis loop-detection {enable|disable}

Syntax Definitions

enable	Enables loop-detection operation.
disable	Disables loop-detection operation.

Defaults

parameter	default
loop-detection	enable

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- This command is only available on switches that are configured with a valid multi-chassis chassis ID number (1 or 2).
- While configuring the multi-chassis feature on an existing network, it is recommended to keep the default settings.
- Loop-detection is enabled by default on switches that operate in multi-chassis mode, that is, whose operational chassis identifier is within the range 1 -2. The feature is disabled by default on switches that operate in standalone mode, that is, whose operational chassis identifier is “0”.
- Disabling loop detection is not recommended when configuring MC-LAG in an existing network.
- Configure the multi-chassis feature parameters on the local chassis for loop-detection.
- Proprietary MAC addresses are used as the source addresses for loop detection control packets. Some of the OmniSwitch platforms are aware of these addresses will not learn them. However, other vendor switches will learn these addresses at the rate of one MAC address per VLAN.

Examples

```
-> multi-chassis loop-detection enable
-> multi-chassis loop-detection disable
```

Release History

Release 6.4.5; command introduced.

Related Commands

show multi-chassis loop-detection	Displays the configured and operational parameters related to the multi- chassis loop-detection feature on the switch.
multi-chassis loop-detection transmit-interval	Displays the loop detection status and parameter values for the switch.
clear multi-chassis loop-detection	Clears the MC-LAG loop detection information maintained by the switch.

MIB Objects

```
multiChassisConfig
   multiChassisConfigLoopDetectionAdminStatus
```

multi-chassis loop-detection transmit-interval

Configures the loop detection transmit-interval parameter. When loop detection is enabled, the switch generates multicast loop detection PDU (LDPDU) on each active VLAN. The loop detection transmit- interval determines how often the LDPDU are sent.

multi-chassis loop-detection transmit-interval *interval*

Syntax Definitions

interval	The interval, in seconds the switch waits between each transmission of loop detection packets. The valid range is 1–10 seconds.

Defaults

parameter	default
interval	1 second

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- This command is available only on switches that are configured with a valid multi-chassis chassis ID number (1 or 2).
- Increasing the transmit interval time as the number of configured VLANs increases is recommended to minimize the amount of bandwidth consumed by loop detection control packets. For example, if thousands of VLANs are configured on a switch, set the transmit interval to a number close to or equal to 10 seconds instead of using the default value, that is, 1 second.

Examples

```
-> multi-chassis loop-detection transmit-interval 2
-> multi-chassis loop-detection transmit-interval 3
```

Release History

Release 6.4.5; command introduced.

Related Commands

show multi-chassis loop-detection	Displays the configured and operational parameters related to the multi- chassis loop-detection feature on the switch.
multi-chassis loop-detection	Configures the multi-chassis loop-detection function on the switch.

MIB Objects

```
multiChassisConfig
   multiChassisLoopDetectionTransmitInterval
```

multi-chassis vf-link create

Configures a VFL between peer switches to enable them to operate in multi-chassis mode. It defines its administrative status.

multi-chassis vf-link create

no multi-chassis vf-link

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- This command is only available on switches that are configured with a valid multi-chassis chassis ID number (1 or 2).
- Use the **no** form of this command to remove the VFL configuration from the switch.
- Although the switch supports runtime configuration of the VFL and its member ports, configuring the VFL at the same time as the chassis ID is configured and before rebooting the switch is recommended.
- The VFL can be brought up when the administravie status of both the link and the multi-chassis feature is enabled.

Examples

```
-> multi-chassis vf-link create
-> no multi-chassis vf-link
```

Release History

Release 6.4.5; command introduced.

Related Commands

multi-chassis vf-link member-ports	Adds a port to the list of member ports of the virtual fabric link.
multi-chassis vf-link default-vlan	Configures the default VLAN on the virtual fabric link.
show multi-chassis vf-link	Displays a summary of the configured and operational parameters related to the virtual fabric link on the switch.
show multi-chassis vf-link member-port	Displays detailed information about the configured and operational parameters related to the virtual fabric link member ports on the switch.

MIB Objects

```
multiChassisLinkTable
   multiChassisLinkIfIndex
   multiChassisLinkOperStatus
   multiChassisLinkActivePortNum
   multiChassisLinkRowStatus
```

multi-chassis vf-link member-ports

Configures member ports for the virtual fabric link (VFL).

multi-chassis vf-link member-ports *slot/port*

no multi-chassis vf-link member-ports *slot/port*

Syntax Definitions

slot/port	Slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).

Defaults

N/A

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- This command is only available on switches that are configured with a valid multi-chassis chassis ID number (1 or 2).
- A maximum of 8 interfaces can be configured as virtual fabric link members.
- Currently, only ports capable of operating at 10 Gbps (XNI-U32 only on OmniSwitch 9000E) and in full duplex mode can support the virtual fabric link operation. Ports on other types of modules are not eligible to become virtual fabric link member ports.
- If an eligible port is operationally down when the port is configured as a member of the VFL, the configuration is accepted. When that port then becomes operational, however, the switch will verify the port is operating at the required speed and duplex mode before accepting the port as a member. If these conditions are not met, the VFL configuration is removed from the port and a syslog message and SNMP trap are generated.
- Although the switch supports runtime configuration of the virtual fabric link and its member ports, it is recommended to configure the virtual fabric link at the same time the chassis identifier is configured and before rebooting the switches in multi-chassis mode.
- The virtual fabric link member ports become operational only when a switch comes up running in the multi-chassis mode. In other words, runtime configuration of a chassis identifier on a switch currently operating in standalone mode does not activate the member ports.
- For resiliency reasons, it is recommended configuring at least four interfaces as virtual fabric link members. An ideal set up would be to have two interfaces configured per network interface card. Within each network interface card, using an interface in the lower port range (that is, ports 1 through 16) and one interface in the upper port range (that is, ports 17 through 32) is recommended.

Examples

```
-> multi-chassis vf-link member-port 3/1
-> no multi-chassis vf-link member-port 3/2
```

Release History

Release 6.4.5; command introduced.

Related Commands

multi-chassis vf-link create	Configures a virtual fabric link between two peer switches to enable them to operate in multi-chassis mode.
multi-chassis vf-link default-vlan	Configures the default VLAN on the virtual fabric link.
show multi-chassis vf-link	Displays a summary of the configured and operational parameters related to the virtual fabric link on the switch.
show multi-chassis vf-link member-port	Displays detailed information about the configured and operational parameters related to the virtual fabric link member ports on the switch.

MIB Objects

```
multiChassisLinkMemberPortTable
   multiChassisLinkMemberPortLinkIfIndex
   multiChassisLinkMemberPortIfindex
   multiChassisLinkMemberPortOperStatus
   multiChassisLinkMemberPortRowStatus
```

multi-chassis vf-link default-vlan

Configures the default VLAN on the virtual fabric link.

multi-chassis vf-link default-vlan *vlan*

no multi-chassis vf-link default-vlan *vlan*

Syntax Definitions

vlan	VLAN to be configured as the default VLAN on the virtual fabric link in the range 1 - 4094.

Defaults

parameter	default
vlan (Virtual fabric-link default-vlan)	1

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- This command is only supported on switches that are configured with a valid multi-chassis chassis ID number (1 or 2).
- Use the no form of this command to remove the default VLAN assignment from the VFL.
- When configuration is not provided, the default or untagged VLAN on the VFL is VLAN 1.
- When no configuration is explicitly provided, the default or untagged VLAN for the virtual fabric link is VLAN 1.
- A VLAN must be created in advance using the **vlan** command to allow the VLAN as the default VLAN on the virtual fabric link.
- Specify a VLAN ID that already exists in the switch configuration.
- If the VLAN currently configured as the default VLAN for the virtual fabric link is removed using VLAN management commands (**no vlan** *vlan_id*), VLAN 1 is automatically reinstated as the default VLAN for the virtual fabric link.

Examples

```
-> multi-chassis vf-link default-vlan 2
-> no multi-chassis vf-link default-vlan
-> no vlan 2
```

Release History

Release 6.4.5; command introduced.

Related Commands

multi-chassis vf-link create	Configures a virtual fabric link between two peer switches to enable them to operate in multi-chassis mode.
show multi-chassis vf-link member-port	Adds a port to the list of member ports of the virtual fabric link.
show multi-chassis vf-link	Displays a summary of the configured and operational parameters related to the virtual fabric link on the switch.
show multi-chassis vf-link member-port	Displays detailed information about the configured and operational parameters related to the virtual fabric link member ports on the switch.

MIB Objects

```
multiChassisLinkTable
   multiChassisLinkfIndex
   multiChassisLinkMemberPortLinkIfIndex,
   multiChassisLinkMemberPortOperDefaultVlan
```

multi-chassis vip-vlan

Configures a virtual IP (VIP) VLAN, which is a special type of VLAN used to provide the underlying LAN infrastructure for the support of basic IP/Layer 3 services on a multi-chassis link aggregation group.

multi-chassis vip-vlan *vid* **[{admin-state {enable|disable}} { name {num}{***"string"* **string} {** *mtu-ip num***}][{ 1x1 | flat }** *stp* **{enable | disable}]**

no multi-chassis vip-vlan *vid*

Syntax Definitions

vid	VLAN to be created as a virtual IP VLAN within the range [1 - 4094].
admin-state	The admin state of the VIP VLAN to enable or disable.
name	Description to the VIP VLAN with number or string.
mtu-ip	Maximum Transmission Unit(MTU) value to the VIP VLAN.
1x1	Specifies that the Spanning Tree status for the VIP- VLAN applies when the switch is running in the 1x1 Spanning Tree mode.
flat	Specifies that the Spanning Tree status for the VIP-VLAN applies when the switch is running in the flat Spanning Tree mode.
enable	Enables Spanning Tree for the specified VIP- VLAN.
disable	Disables Spanning Tree for the specified VIP-VLAN.

Defaults

N/A

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- This command is only supported on switches that are configured with a valid multi-chassis chassis ID number (1 or 2).
- Use the **no** form of this command to remove a VIP VLAN from the switch configuration.
- The virtual IP VLANs are distinguished from the others by a distinct type of VLAN using the VLAN management show commands.
- Specify a VLAN ID that does not exist in the switch configuration. This command will automatically create the VLAN as a VIP VLAN.
- Although VIP VLANs are identified as a special VLAN type for MC-LAG purposes, assigning non-MC-LAG ports to this type of VLAN is supported. In addition, assigning MC-LAG ports to standard VLANs (non-VIP VLANs) is supported.

- The IP interfaces configured on a virtual IP VLAN have limited functionality. Routing protocols and VRRP cannot be configured on such IP interfaces.
- The **no multi-chassis vip-vlan** command is processed directly by the VLAN Manager sub-system.
- The IP interfaces configured on a virtual IP VLAN have limited functionality. Routing protocols and VRRP cannot be configured on such IP interfaces.
- Currently IPv6 interfaces cannot be configured on a virtual IP VLAN.
- There are two IP addresses associated with a VIP VLAN IP interface: a management address and a virtual IP address.

  > The management address is a unique IP address used by each switch within a multi-chassis domain to provide management services. Each peer switch must have a unique management IP address.

  > The virtual IP address is used to route packets that terminate on the multi-chassis peer switches. Unlike the management address, the VIP address must be the same on each peer switch.

Examples

```
-> multi-chassis vip-vlan 3
-> no multi-chassis vip-vlan 3
```

Release History

Release 6.4.5; command introduced.

Related Commands

show vlan	Displays a list of VLANs configured on the switch.
multi-chassis chassis-id hello-interval	Assigns a unique chassis identifier to the switch and enables or disables the switch to operate in multi-chassis mode.
ip interface	Configures an IP interface for a VLAN. Use this command to configure an IPv4 interface for a VIP VLAN.

MIB Objects

```
vlanTable
   vlanEntry
```

show multi-chassis status

Displays the configured and operational parameters related to the multi-chassis feature on the switch.

show multi-chassis status

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

N/A

Examples

```
-> show multi-chassis status
Multi-Chassis Operational Configured
----------------+-----------+---------
Chassis ID 1  2
Chassis Role Primary N/A
Status UP N/A
Chassis-Type     OS9802E       N/A
Hello Interval 5s 5s
IPC VLAN 4904 4094
Chassis-Group     10            10
```

Output fields are defined here:

output definitions

Operational	Operational parameters that are currently being used by the system.
Configured	Parameters that are configured and that are implemented after switch reset.
Chassis ID	Chassis identifier within the multi-chassis operational range [1 - 2]. The chassis identifier must be globally unique within the set of switches configured to operate together providing multi-chassis services.
Chassis Role	The chassis role determines which of the switches operating in multi-chassis mode is the master of the combined system. The role information can be used by various software components as needed.
Status	The current status of the multi-chassis feature, which can be **Down**, **Up**, or **Inconsistent**.
Chassis-Type	The peer switch chassis type.(OS9000E).

output definitions

Hello Interval	Time interval, in seconds, at which multi-chassis control hello messages are to be sent to the peer switch within the range [1 - 10].
IPC VLAN	Multi-chassis control VLAN used for all multi-chassis control communication between the peer switches within the range [2 - 4094].
Chassis-Group	The multi-chassis group ID for the switch. Peer switches must use the same group ID.

Release History

Release 6.4.5; command introduced.

Related Commands

multi-chassis chassis-id hello-interval	Assigns a globally unique chassis identifier to the switch and enables or disables the switch to operate in multi-chassis mode.
multi-chassis hello-interval	Configures the multi-chassis hello-interval parameter on the switch.
multi-chassis ipc-vlan	Configures the IPC-VLAN parameter, which is used for multi-chassis control communication, on the local switch.
show multi-chassis consistency	Displays the system level mandatory consistency parameters of both the local and peer switches.

MIB Objects

```
multiChassisOperation
   multiChassisOperChassisId
   multiChassisOperChassisRole
   multiChassisOperStatus
   multiChassisOperHelloInterval
   multiChassisOperIpcVlan
multiChassisConfig
   multiChassisConfigChassisId
   multiChassisConfigHelloInterval
   multiChassisGroup
   multiChassisType
```

show multi-chassis loop-detection

Displays the configured and operational parameters related to the multi-chasiss loop-detection feature on the switch.

show multi-chassis loop-detection

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

If a loop is detected, disable loop detection and then use **clear multi-chassis loop-detection** command to clear the loop detection information from the ports that were downed. This will ensure that **multi-chassis loop-detection** command displays the most current status for such ports.

Examples

```
-> show multi-chassis loop-detection
Status              : Enabled,
Transmit Interval   : 2s,
Total Transmit Count: 135701,
Total Loop Count    : 11,
Port Down List      : 7/1
```

Output fields are defined here:

output definitions

Status	Administrative status of the loop-detection feature. Can be **Enabled** or **Disabled**
Transmit Interval	Transmit interval, in seconds, which determines the time interval between the transmission of successive loop-detection packets on each VLAN active on the switch within the range [1 - 10].
Total Transmit Count	Total number of control packets transmitted on all VLANs configured on the switch.
Total Loop Count	Total number of control packets that were transmitted and received, that is. looped back to the originator on all VLANs.
Port Down List	List of ports that were brought down because a loop was detected.

Release History

Release 6.4.5; command introduced.

Related Commands

multi-chassis loop-detection	Configures the multi-chassis loop-detection function on the switch.
multi-chassis loop-detection transmit-interval	Configures the loop-detection transmit interval, which determines the time interval between the transmission of successive loop-detection packets on each VLAN active on the switch.
clear multi-chassis loop-detection	Clears the MC-LAG loop detection information maintained by the switch.

MIB Objects

```
multiChassisLoopDetection
   multiChassisLoopDetectionTransmitCount
   multiChassisLoopDetectionCount
   multiChassisLoopDetectionPortDownList
   multiChassisLoopDetectionAdminStatus
   multiChassisLoopDetectionTransmitInterval
```

show multi-chassis vf-link

Displays a summary of the configured and operational parameters related to the virtual fabric link on the switch.

show multi-chassis vf-link

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

N/A

Examples

```
-> show multi-chassis vf-link
VFLink ID   Oper     Primary Port   Config Port   Active Port   Def Vlan
----------+--------+--------------+-------------+-------------+---------
0           Up       1/2            4             4             5
```

Output fields are defined here:

output definitions

VFLink ID	Virtual Fabric Link identifier. Currently a single virtual fabric link with identifier equal to zero is supported.
Oper	The current status of the Virtual Fabric Link, which can be **Disabled**, **Down** or **Up**. The **Disabled** state occurs whenever the multi-chassis feature is disabled because the operational chassis identifier currently effective is the standalone chassis identifier, that is, zero.
Primary Port	Identifies the primary port of the virtual fabric link. This concept is relevant because all the non-unicast traffic, that is, broadcast, multicast and unknown unicast is distributed across ports of the network interface module that hosts the virtual fabric link's primary port.
Config Port	Number of physical ports configured as virtual fabric link member ports in the range [0 - 8].
Active Port	Number of physical ports that are operational or active members of the virtual fabric link in the range [0 - 8].
Def Vlan	Default VLAN on the virtual fabric link within the range [1 - 4094].

Release History

Release 6.4.5; command introduced.

Related Commands

multi-chassis vf-link create	Configures a virtual fabric link between two peer switches to enable them to operate in multi-chassis mode.
multi-chassis vf-link member-ports	Adds a port to the list of member ports of the virtual fabric link.
multi-chassis vf-link default-vlan	Configures the default VLAN on the virtual fabric link.
show multi-chassis vf-link member-port	Displays detailed information about the configured and operational parameters related to the virtual fabric link member ports on the switch.

MIB Objects

```
multiChassisLinkTable
   multiChassisLinkIfIndex
   multiChassisLinkOperStatus
   multiChassisLinkPrimaryPort
   multiChassisLinkConfigPortNum
   multiChassisLinkActivePortNum
vlanTable
   vlanEntry
```

show multi-chassis vf-link member-port

Displays detailed information about the configured and operational parameters related to the virtual fabric link member ports on the switch.

show multi-chassis vf-link member-port [*slot/port***]**

Syntax Definitions

slot/port	Specify the slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).

Defaults

N/A

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

N/A

Examples

```
-> show multi-chassis vf-link member-port
VFLink ID   Slot/Port   Oper      Is Primary
----------+-----------+---------+------------
0           1/1         Up        No
0           1/2         Up        Yes
0           1/17        Up        No
0           1/18        Up        No

-> show multi-chassis vf-link member-port 3/1
VFLink ID   Slot/Port   Oper      Is Primary
----------+-----------+---------+------------
0           1/2         Up        Yes
```

Output fields are defined here:

output definitions

VFLink ID	Virtual Fabric Link identifier. Currently a single virtual fabric link with identifier equal to zero is supported.
Slot/Port	The slot/port that defines each of the physical ports that are members of the virtual fabric link.

output definitions

Oper	The current status of each virtual fabric link member port, which can be **Disabled**, **Down** or **Up**.The **Disabled** state occurs whenever the multi-chassis feature is disabled because the operational chassis identifier currently effective is the standalone chassis identifier, that is, zero.
Is Primary	Specifies whether a physical port is the primary port of the virtual fabric link. It may assume the values **Yes** or **No**.

Release History

Release 6.4.5; command introduced.

Related Commands

multi-chassis vf-link create	Configures a virtual fabric link between two peer switches to enable them to operate in multi-chassis mode.
multi-chassis vf-link member-ports	Adds a port to the list of member ports of the virtual fabric link.
multi-chassis vf-link default-vlan	Configures the default VLAN on the virtual fabric link.
show multi-chassis vf-link	Displays a summary of the configured and operational parameters related to the virtual fabric link on the switch.

MIB Objects

```
multiChassisLinkMemberPortTable
   multiChassisLinkMemberPortLinkIfIndex
   multiChassisLinkMemberPortIfindex
   multiChassisLinkMemberPortOperStatus
   multiChassisLinkMemberPortIsPrimary
```

show multi-chassis consistency

Displays the system level mandatory consistency parameters of both the local and peer switches.

show multi-chassis consistency

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

N/A

Examples

```
-> show multi-chassis consistency
Consistency           Local     Peer      Status
--------------------+---------+---------+---------
Chassis-ID            1         2         OK
Chassis-Type          OS9802E   OS9802E   OK
Hello-Interval        5         5         OK
IPC-VLAN              4094      4094      OK
CHASSIS_GROUP         0         0         OK
STP-Path-Cost-Mode    Auto      Auto      OK
STP-Mode              Per-VLAN  Per-VLAN  OK
```

Output fields are defined here:

output definitions

Consistency	Provides a list of global mandatory consistency parameters for the local and remote switches operating in multi-chassis mode.
Local	Value of a given consistency parameter on the local switch.
Peer	Value of a given consistency parameter on the peer switch.
Status	Specifies the overall status of a consistency parameter within the entire multi-chasiss system comprised by the individual switches. The possible values are **OK**, **NOK**, and **N/A** if there is a mismatch of any of the parameters listed in this command or if the chassis identifier of the two switches is the same, the multi-chassis operational status will not be “Up”. In this case the "Status" column shown in this output indicates which parameter has a problem. The N/A value in the "Peer" column indicates that the information is unavailable from the peer. This will always be the case when the multi-chassis operational status is **Down.**

output definitions

Chassis ID	Globally unique chassis identifier. The valid range for the multi-chassis operational range is [1 - 2], whereas the value for standalone operation is zero.
Chassis-Type	The peer switch chassis type.
Hello Interval	Time interval, in seconds, at which multi-chassis control hello messages are to be sent to the peer switch within the range [1 - 10].
STP-Path-Cost-Mode	Specifies the STP path cost mode whose possible values are Auto and 32Bit.
STP-Mode	Specifies the STP mode whose possible values are **Per-VLAN** and **Flat**

Release History

Release 6.4.5; Command introduced.

spantree mode	Assigns a flat Spanning Tree or per-vlan Spanning Tree operating mode for the switch. These modes are exclusive; however, it is not necessary to reboot the switch when the STP modes are changed.
multi-chassis chassis-id hello-interval	Assigns a globally unique chassis identifier to the switch and enables or disables the switch to operate in multi-chassis mode.
multi-chassis hello-interval	Configures the multi-chassis hello-interval parameter on the switch.
multi-chassis ipc-vlan	Configures the IPC-VLAN parameter, which is used for multi-chassis control communication, on the local switch.
show multi-chassis status	Displays the configured and operational parameters related to the multi- chassis feature on the switch.
show multi-chassis consistency	Displays the system level mandatory consistency parameters of both the local and peer switches.

MIB Objects

```
multiChassisGlobalConsistency
   multiChassisLocalChassisId
   multiChassisPeerlChassisId
   multiChassisIdConsistency
   multiChassisLocalHelloInterval
   multiChassisPeerHelloInterval
   multiChassisHelloIntervalConsistency
   multiChassisLocalStpPathCostMode
   multiChassisPeerStpPathCostMode
   multiChassisStpPathCostModeConsistency
   multiChassisLocalStpMode
   multiChassisPeerStpMode
   multiChassisStpModeConsistency
vlanTable
   vlanEntry
```

show multi-chassis consistency linkagg

Displays the per-multi-chassis aggregate level optional consistency parameters of both the local and peer switches.

show multi-chassis consistency linkagg *agg_num* **[vlan-list]**

Syntax Definitions

agg_num	The number corresponding to the static or dynamic multi-chassis aggregate group within the range [0-127] and subject to the settings specified through the linkagg range command.
vlan-list	Lists the local and peer VLANs associated with the aggregate.

Defaults

N/A

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- This command provides data related to multi-chassis aggregates only. It cannot be used for ordinary aggregates. To determine the type of an aggregate and classify this aggregate as a multi-chassis aggregate, use the **linkagg range** command.
- Use the **linkagg range** command to identify the ranges assigned to aggregate.
- Mismatch of any of the parameters listed in this command represent network mis-configurations and may cause traffic problems. In case of mismatch the "Status" column shown in this output will indicate which parameter has a problem.

Examples

```
-> show multi-chassis consistency linkagg
Local  Peer
Linkagg  Exist  Exist  Status
-------+------+------+-------
98       Yes    No     N/A


-> show multi-chassis consistency linkagg 3
Consistency Local Peer Status
----------------------+--------------------+------------------+---------
Chassis-ID 1  2  OK
Agg-ID 3  3  OK
LAG-Type LACP  SATIC  NOK
LACP-System-ID 00:d0:95:a3:ec:67 00:d0:95:a3:ec:67  OK
LACP-Priority 100 100 OK
Default-Vlan1 1 OK
VLAN-List Configured Configured NOK
```

Output fields are defined here:

output definitions

Consistency	Provides a list of per-multi-chassis aggregate optional consistency parameters for the local and remote switches operating in multi-chassis mode.
Local	Value of a given consistency parameter on the local switch.
Peer	Value of a given consistency parameter on the peer switch.
Status	Specifies the overall status of a consistency parameter within the entire multi-chasiss system comprised by the individual switches. The possible values are **OK**, **NOK**, and **N/A**. or In case of mismatch of any of the parameters listed in this command or if the chassis identifier of the two switches is the same, the multi-chassis operational status will not become Up. In this case the "Status" column shown in this output will indicate which parameter has a problem. The N/A value in the "Peer" column indicates that the information is unavailable from the peer. This will always be the case when the multi-chassis operational status is **Down**.
Chassis-ID	Globally unique chassis identifier. The valid range for the multi-chassis operational range is [1 - 2], whereas the value for standalone operation is zero.
Agg-ID	The number corresponding to the static or dynamic multi-chassis aggregate group within the range [0-127].
LAG-Type	Defines the aggregate type as static or dynamic (that is, LACP)
LACP-System-ID	Specifies the system identifier (MAC address format) used by the LACP protocol.
LACP-Priority	Provides the system priority used by the LACP protocol.
Default-Vlan	Specifies the value of the default VLAN configured on the multi-chassis aggregate within the range [1 - 4094].
VLAN List	Indicates whether other types of VLANs (distinct from the default VLAN) are configured on the multi-chassis aggregate.
Local Count	The number of VLANs on the local chassis.
Peer Count	The number of VLANs on the peer chassis.

Release History

Release 6.4.5; command introduced.

Related Commands

linkagg range	Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

```
multiChassisLinkaggConsistencyTable
   multiChassisLinkaggAggIndex
   multiChassisLinkaggAggIndexConsistency
```

```
multiChassisLinkaggLocalAggType
multiChassisLinkaggPeerAggType
multiChassisLinkaggAggTypeConsistency
multiChassisLinkaggLocalVlanType
multiChassisLinkaggPeerVlanType
multiChassisLinkaggVlanTypeConsistency
multiChassisLinkaggLocalVlanListConfig
multiChassisLinkaggLocalVlanListConfig
multiChassisLinkaggVlanListConfigConsistency
multiChassisLinkaggLocalAggActorSystemID
multiChassisLinkaggPeerAggActorSystemID
multiChassisLinkaggAggActorSystemIDConsistency
multiChassisLinkaggLocalAggActorSystemPriority
multiChassisLinkaggPeerAggActorSystemPriority
multiChassisLinkaggAggActorSystemPriorityConsistency
```

clear multi-chassis loop-detection

Clears the configured and operational parameters related to the multi-chasiss loop-detection feature on the switch.

clear multi-chassis loop-detection

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

If a loop is detected, disable the loop detection and use the **clear multi-chassis loop-detection** command to clear the loop detection information from the ports that were downed. This ensures that **show multi-chassis loop-detection** command displays the recent status for such ports.

Examples

```
-> clear multi-chassis loop-detection
```

Release History

Release 6.4.5; command introduced.

Related Commands

multi-chassis loop-detection	Configures the multi-chassis loop-detection function on the switch.
show multi-chassis loop-detection	Displays the configured and operational parameters related to the multi-chasiss loop-detection feature on the switch.

MIB Objects

```
multiChassisLoopDetection
```

9 Ethernet Ring Protection Commands

Ethernet Ring Protection (ERP) is a protection switching mechanism for Ethernet ring topologies, such as multi-ring and ladder networks. The implementation of ERP on Alcatel-Lucent OmniSwitch is based on ERP Version 2 (ITU-T G.8032/Y.1344 to 2010) using the Ring Automatic Protection Switching (R-APS) protocol to coordinate and prevent network loops within a bridged Ethernet ring.

ERP v2 supports multi rings and ladder to ladder networks. ERPv2 functionalities allow configuration of Sub-Rings within a Master Ethernet Ring, interconnected nodes and shared links between the rings.

MIB information for Ethernet Ring Protection commands is as follows:

Filename: AlcatelIND1Erp.mib
Module: ALCATEL-IND1-ERP-MIB

A summary of available commands is listed here:

erp-ring
erp-ring reset-version-fallback
erp-ring rpl-node
erp-ring wait-to-restore
erp-ring enable
erp-ring guard-timer
erp-ring sub-ring
erp-ring virtual-channel
erp-ring revertive
erp-ring clear
erp-ring ethoam-event
clear erp statistics
show erp
show erp statistics

erp-ring

Creates an Ethernet Ring Protection (ERP) using the specified ports and service VLAN ID. The service VLAN transmits ERP control traffic, such as Ring Automatic Protection Switching (R-APS) messages, through the ring. The specified level number identifies an APS Management Entity Group (MEG) to which the service VLAN belongs.

erp-ring *ring_id* **port1 {***slot/port* **| linkagg** *agg_num***} port2 {***slot/port* | **linkagg** *agg_num***} service-vlan** *vlan_id* **level** *level_num* **[guard-timer** *guard_timer***] [enable | disable]**

no erp-ring *ring_id*

Syntax Definitions

ring_id	The ERP ring ID number. The valid range is 1 to 2147483647.
slot/port	The slot number for the module and the physical port number on that module.
agg_num	The link aggregate ID number.
vlan_id	The service VLAN ID number.The valid range is 1 to 4094.
level_num	The MEG level number for the service VLAN. The valid range is 0 to 7.
guard-timer	The guard timer value, in centi seconds, for the ring node.
enable	Administratively enables the ERP ring**.**
disable	Administratively disables the ERP ring.

Defaults

parameter	default
guard_timer	50
**enable	disable**	disable

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a ring from the switch configuration. Administratively disable the ring ports before deleting the ring to avoid creating any network loops. Once the ring is deleted, ensure that the same ports are administratively enabled under Spanning Tree control.
- The specified ring identification number must be unique within a switch.
- ERP is not supported on mobile ports, mirroring ports, link aggregate member ports, high availability ports, Multicast VLAN receiver ports (ERP is supported on Multicast VLAN sender ports only), VLAN Stacking user network interface (UNI) ports, or RRSTP ring ports.

- If a port is tagged with the service VLAN ID or the service VLAN is the default VLAN for the port, then the port is not eligible to become an ERP ring port.
- Specify an existing VLAN ID for the service VLAN ID. Use the same VLAN ID and level number for the service VLAN on each switch that participates in the ERP ring.
- If the ERP switch participates in an Ethernet OAM Maintenance Domain (MD), configure the ERP service VLAN to use the same level number that is used for the Ethernet OAM MD.
- Specify a static VLAN ID for the ERP service VLAN; dynamic VLANs are not configurable as service VLANs.
- The service VLAN can belong to only one ERP ring at a time. A maximum of 8 rings are allowed per switch.
- The specified service VLAN ID must not participate in a Spanning Tree instance that is associated with non-ERP VLANs. Ideally, change the Spanning Tree configuration for the VLAN ID prior to using this command.
- An ERP ring port can belong to only one ERP ring at a time.
- Create an NNI-SVLAN binding before establishing an ERPv2 ring on that SVLAN-NNI binding.The SVLAN-NNI binding can be created with the **ethernet service svlan nni** command.
- ERP is not supported over MC-LAG if the slot/port is an MC-LAG port.
- ERP is not supported if the slot/port is an MC-LAG member port, and an error message is displayed that it is an MC-LAG aggregable port.
- ERP is also not supported if the slot/port is a VFL member port and an error message is displayed specifing that it is an VFL aggregable port.

Examples

```
-> erp-ring 1 port1 1/1 port2 2/4 service-vlan 10 level 2 enable
-> erp-ring 2 port1 linkagg 1 port2 2/10 service-vlan 20 level 2
-> erp-ring 3 port1 linkagg 2 port2 linkagg 4 service-vlan 30 level 7
-> no erp-ring 2
```

Release History

Release 6.3.4; command introduced.

Related Commands

show erp	Displays the ERP ring configuration for the switch.
show erp statistics	Displays ERP ring statistics.
ethernet-service svlan nni	Creates an NNI-SVLAN binding.

MIB Objects

```
alaErpRingTable
   alaErpRingServiceVid
   alaErpRingMEGLevel
   alaErpRingStatus
   alaErpRingPort1
   alaErpRingPort2
   alaErpRingGuardTimer
   alaErpRingRowStatus
```

erp-ring reset-version-fallback

Reverts the ERP ring to ERPv2 mode after upgradation and is issued on all the devices of the ring, starting from the RPL owner.

erp-ring *ring_id* **reset-version-fallback**

Syntax Definitions

ring_id	The ERP ring ID number. The valid range is 1 to 2147483647.

Defaults

NA

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines:

- This command must be issued after the ERP devices are upgraded from AOS 6.4.4 to AOS 6.4.5 as part of the ERPv2 upgradation process. To configure ERPv2 ring this command must be issued on all the nodes starting from the RPL node.
- Use the **show erp ring** command to verify the ERP version running on the switch.
- If this command is issued when the switch is already running ERPv2, then the following error message is displayed. **"ERROR: Ring** *ring_id* **is running as ERP protocol V2"**

Examples

```
-> erp-ring 1 reset-version-fallback
```

Release History

Release 6.4.5; command introduced.

Related Commands

show erp	Displays the ERP ring configuration for the switch.

MIB Objects

```
alaErpRingTable
   alaErpRingActiveVersion
   alaErpRingResetVersionFallback
```

erp-ring rpl-node

Configures a switch as a RPL node. This command also identifies the ERP port as an RPL connection port. The RPL remains blocked to prevent loops within the ERP ring.

erp-ring *ring_id* **rpl-node {port** *slot/port* **| linkagg** *agg_num***}**

no erp-ring *ring_id* **rpl-node**

Syntax Definitions

ring_id	An existing ERP ring ID number. The range is 1 to 2147483647.
slot	The slot number for the module.
port	The physical port number on the module.
agg_num	The link aggregate ID number.

Defaults

NA

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove the RPL designation for the specified ring.
- The RPL node can be configured only when the ring is disabled. RPL configurations applied to the Ethernet ring while it is enabled, is rejected.
- The specified ERP ring ID must exist in the switch configuration.
- This command applies only to ERP ring ports; ports not configured as ERP ring ports are not eligible to become RPL ports.
- Only one of the two ring ports configured for the switch can be designated as an RPL node port.
- For RPL configuration on member ports of VFL, if the slot/port is a VFL or MC-LAG member port an error message is displayed.

Examples

```
-> erp-ring 1 rpl-node port 2/1
-> erp-ring 2 rpl-node linkagg 2
-> no erp-ring 2 rpl-node
```

Release History

Release 6.3.4; command introduced.

Related Commands

erp-ring	Configures an ERP ring.
erp-ring wait-to-restore	Configures the wait-to-restore timer value for the Ring Protection Link (RPL) node.
show erp	Displays the ERP ring configuration for the switch.

MIB Objects

```
alaErpRingPortEntry
   alaErpRingPortIfIndex
   alaErpRingPortType
```

erp-ring wait-to-restore

Configures the wait-to-restore timer value for the RPL switch. This timer determines the interval in minutes the RPL switch waits before returning the RPL ports to a blocked state after the ERP ring has recovered from a link failure.

erp-ring *ring_id* **wait-to-restore** *wtr_timer*

no erp-ring *ring_id* **wait-to-restore**

Syntax Definitions

ring_id	An existing ERP ring ID number. The valid range is 1 to 2147483647.
wtr_timer	The number of minutes to wait before restoring the RPL to a blocked state. The valid range is 1 to 12 minutes.

Defaults

By default, the wait-to-restore timer value is set to 5 minutes.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to set the timer back to the default setting of 5 minutes.
- The specified ERP ring ID must exist in the switch configuration.
- This command applies only on a switch that serves as the RPL node for the ERP ring.

Examples

```
-> erp-ring 1 wait-to-restore 6
-> no erp-ring 1 wait-to-restore
```

Release History

Release 6.3.4 ; command introduced.

Related Commands

erp-ring	Configures an ERP ring.
erp-ring rpl-node	Configures a Ring Protection Link (RPL) port connection.
show erp	Displays the ERP ring configuration for the switch.

MIB Objects

```
alaErpRingId
   alaErpRingWaitToRestoreTimer
```

erp-ring enable

Enables or disables an ERP ring identified by the specified ring ID. This command applies to enabling or disabling existing ERP rings.

erp-ring *ring_id* **{enable** | **disable}**

Syntax Definitions

ring_id	An existing ERP ring ID number. The valid range is 1to2147483647.

Defaults

By default, ERP rings are disabled when they are created.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The specified ring ID must exist in the switch configuration.
- Enabling a ring is also allowed at the time the ring is created.

Examples

```
-> erp-ring 1 enable
-> erp-ring 1 disable
```

Release History

Release 6.3.4 ; command introduced.

Related Commands

erp-ring	Configures an ERP ring.
show erp	Displays the ERP ring configuration for the switch.

MIB Objects

```
alaErpRingId
   alaErpRingStatus
```

erp-ring guard-timer

Configures the guard timer value for the specified ERP ring node. The guard timer is used to prevent ring nodes from receiving outdated Ring Automatic Protection Switching (R-APS) messages. During the amount of time determined by this timer, all received R-APS messages are ignored by the ring protection control process.

erp-ring *ring_id* **guard-timer** *guard_timer*

no erp-ring *ring_id* **guard-timer**

Syntax Definitions

ring_id	An existing ERP ring ID number. The valid range is 1–2147483647.
guard_timer	The guard timer value. The valid range is 1–200 centi-secs.

Defaults

parameter	default
guard_timer	50

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to set the timer back to the default value of 50 centi-secs.
- The specified ring ID must exist in the switch configuration.

Examples

```
-> erp-ring 1 guard-timer 10
-> no erp-ring 1 guard-timer
```

Release History

Release 6.3.4 ; command introduced.

Related Commands

erp-ring	Configures an ERP ring.
show erp	Displays the ERP ring configuration for the switch.

MIB Objects

```
alaErpRingId
   alaErpRingGuardTimer
```

erp-ring sub-ring

Creates an Ethernet Ring Protection (ERP) sub-ring.

erp-ring *ring_id* **sub-ring-port {***slot/port* **| linkagg** *agg_num***} service-vlan** *vlan_id* **level** *level_num* **[guard-timer** *guard_timer***] [enable | disable]**

no erp-ring *ring_id* **{***slot/port* **| linkagg** *agg_num***}**

Syntax Definitions

ring_id	The ERP ring ID number. The valid range is 1 to 2147483647.
slot/port	The slot number for the module and the physical port number on that module.
agg_num	The link aggregate ID number.
vlan_id	The service VLAN ID number.The valid range is 1 to 4094.
level_num	The MEG level number for the service VLAN. The valid range is 0 to 7.
guard-timer	The guard timer value, in centi-secs, for the ring node.
enable	Administratively enables the ERP sub-ring**.**
disable	Administratively disables the ERP sub-ring.

Defaults

parameter	default
guard_timer	50
**enable	disable**	disable

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a sub-ring from the switch configuration. Adminstratively disable ring ports before deleting the ring to avoid creating any network loops. Once the ring is deleted, ensure that the same ports are administratively enabled under Spanning Tree control.
- The specified ring identification number must be unique within a switch.
- ERP is not supported on mobile ports, mirroring ports, link aggregate member ports, high availability ports, Multicast VLAN receiver ports (ERP is supported on Multicast VLAN sender ports only), VLAN Stacking user network interface (UNI) ports, or RRSTP ring ports.
- VLAN tagging must be enabled before the ERPv2 ring is enabled.
- Specify an existing VLAN ID for the service VLAN ID. Use the same VLAN ID and level number for the service VLAN on each switch that participates in the ERP ring.

- If the ERP switch participates in an Ethernet OAM Maintenance Domain (MD), configure the ERP service VLAN to use the same level number that is used for the Ethernet OAM MD.
- Specify a static VLAN ID for the ERP service VLAN; dynamic VLANs are not configurable as service VLANs.
- The service VLAN can belong to only one ERP ring at a time. A maximum of four rings are allowed per switch.
- An ERP ring port can belong to only one ERP ring at a time.
- An ERP type NNI-SVLAN binding must exist before establishing an ERP ring.

Examples

```
-> erp-ring 1 sub-ring-port 1/1 service-vlan 10 level 2 enable
-> erp-ring 2 sub-ring-port linkagg 1 port2 2/10 service-vlan 20 level 2
-> no erp-ring 2
```

Release History

Release 6.4.5; command introduced.

Related Commands

erp-ring	Creates an Ethernet Ring Protection (ERP) ring.
show erp	Displays the ERP ring configuration for the switch.
show erp statistics	Displays ERP ring statistics.
ethernet-service svlan nni	Creates a NNI-SVLAN binding.

MIB Objects

```
alaErpRingTable
   alaErpRingId
   alaErpRingServiceVid
   alaErpRingMEGLevel
   alaErpRingStatus
   alaErpRingPort1
   alaErpRingPort2
   alaErpRingGuardTimer
   alaErpRingRowStatus
```

erp-ring virtual-channel

Enables or disables an Ethernet Ring Protection (ERP) Ring Virtual Channel.

erp-ring *ring_id* **virtual-channel [enable | disable]**

Syntax Definitions

ring_id	The ERP ring ID number. The valid range is 1 to 2147483647.
enable	Administratively enables the ERP virtual channel**.** If enabled, Ring Automatic Protection Switching (R-APS) protocol messages are encapsulated and transmitted over a virtual channel configured on the major ring.
disable	Administratively disables the ERP virtual channel. If disabled, R-APS messages are terminated at the interconnection nodes between the rings but not blocked at the Ring Protection Link (RPL) of the sub-ring.

Defaults

parameter	default
enable | disable	enable

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The specified ring identification number must be unique within a switch.
- The ring identified by Ring ID must be created before configuring the virtual channel state for ring node.

Examples

```
-> erp-ring 2 virtual-channel disable
-> erp-ring 1 virtual-channel enable
```

Release History

Release 6.4.5; command introduced.

Related Commands

erp-ring	Creates an Ethernet Ring Protection (ERP) ring.
erp-ring sub-ring	Creates an Ethernet Ring Protection (ERP) ring sub ring.
show erp	Displays the ERP ring configuration for the switch.
show erp statistics	Displays ERP ring statistics.

MIB Objects

```
alaErpRingTable
   alaErpRingId
   alaErpRingVirtualChannel
```

erp-ring revertive

This command is only applicable for the RPL-owner switch. Enables or disables revertive mode on the specified node.

erp-ring *ring_id* **revertive [enable | disable]**

Syntax Definitions

ring_id	The ERP ring ID number. The valid range is 1 to 2147483647.
enable	Administratively enables Revertive Mode**.** Now, if the RPL is unblocked due to a failure within the ring, the RPL automatically reverts to the "Blocked" state when the failed link recovers.
disable	Administratively disables Revertive Mode. Now, if the RPL is unblocked due to a failure within the ring, the RPL does not automatically revert to "Blocked" state when the failed link recovers.

Defaults

parameter	default
enable | disable	enable

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The specified ring identification number must be unique within a switch.
- The ring identified by the Ring ID must be created using the **erp-ring** command, before configuring the revertive mode for ring node.

Examples

```
-> erp-ring 1 revertive enable
-> erp-ring 2 revertive disable
```

Release History

Release 6.4.5; command introduced.

Related Commands

erp-ring	Creates an Ethernet Ring Protection (ERP) ring.
erp-ring sub-ring	Creates an Ethernet Ring Protection (ERP) ring sub ring.
erp-ring clear	Clears any pending state (for example, non-revertive restoring).
show erp	Displays the ERP ring configuration for the switch.
show erp statistics	Displays ERP ring statistics.

MIB Objects

```
alaErpRingTable
   alaErpRingId
   alaErpRingRevertive
```

erp-ring clear

This command is only applicable for the RPL-owner switch. Clears any pending state (for example, non-revertive restoring).

erp-ring *ring_id* **clear**

Syntax Definitions

ring_id	The ERP ring ID number. The valid range is 1 to 2147483647.
clear	Clears any pending state on the ring.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The specified ring identification number must be unique within a switch.

Examples

```
-> erp-ring 1 clear
```

Release History

Release 6.4.5; command introduced.

Related Commands

erp-ring	Creates an Ethernet Ring Protection (ERP) ring.
erp-ring sub-ring	Creates an Ethernet Ring Protection (ERP) ring sub ring.
show erp	Displays the ERP ring configuration for the switch.
show erp statistics	Displays ERP ring statistics.

MIB Objects

```
alaErpRingTable
   alaErpRingId
   alaErpRingClearAction
```

erp-ring ethoam-event

Configures a ring port to accept a “loss of connectivity” event from Ethernet OAM for a remote endpoint.

erp-ring *ring_id* **ethoam-event {***slot/port* **| linkagg** *agg_num***} remote-endpoint** *mep_id*

no erp-ring *ring_id* **ethoam-event {***slot/port* **| linkagg** *agg_num***}**

Syntax Definitions

ring_id	The ERP ring ID number. The valid range is 1 to 2147483647.
slot/port	The slot number for the module and the physical port number on that module.
agg_num	The link aggregate ID number.
mep_id	The remote endpoint ID.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The specified ring identification number must be unique within a switch.

Examples

```
-> erp-ring 1 ethoam-event 1/1 remote-endpoint 10
-> erp-ring 1 ethoam-event linkagg 1 remote-endpoint 10
```

Release History

Release 6.4.5; command introduced.

Related Commands

erp-ring	Creates an Ethernet Ring Protection (ERP) ring.
erp-ring sub-ring	Creates an Ethernet Ring Protection (ERP) ring sub ring.
show erp	Displays the ERP ring configuration for the switch.
show erp statistics	Displays ERP ring statistics.

MIB Objects

```
alaErpRingTable
   alaErpRingId
   alaErpRingPortIfIndex
   alaErpRingPortEthOAMEvent
   alaErpRingPortRmepId
```

clear erp statistics

Clears ERP statistics for all rings, a specific ring, or a specific ring port.

clear erp statistics [ring *ring_id* **[port** *slot/port* **| linkagg** *agg_num***]]**

Syntax Definitions

ring_id	An existing ERP ring ID number. The valid range is 1 to 2147483647.
slot/port	The slot number for the module and the physical port number on that module.
agg_num	The link aggregate ID number.

Defaults

By default, statistics are cleared for all ERP rings in the switch configuration.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Enter a ring ID to clear the statistics for a specific ring.
- Enter a ring ID and a ring port number or link aggregate ID to clear the statistics for a specific port or link aggregate.
- The specified ring ID must exist in the switch configuration.
- The specified port must belong to the ring identified by the ring ID.

Examples

```
-> clear erp statistics
-> clear erp statistics ring 5
-> clear erp statistics ring 5 port 1/2
-> clear erp statistics ring 5 linkagg 10
```

Release History

Release 6.3.4 ; command introduced.

Related Commands

erp-ring	Configures an ERP ring.
show erp	Displays the ERP ring configuration for the switch.
show erp statistics	Displays ERP ring statistics.

MIB Objects

```
alaErpClearStats
alaErpRingTable
   alaErpRingId
   alaErpRingClearStats
alaErpRingPortTable
   alaErpRingPortIfIndex
   alaErpRingPortClearStats
```

show erp

Displays the ERP configuration information for all rings, a specific ring, or for a specific ring port.

show erp [ring *ring_id* **| [port** *slot/port* **| linkagg** *agg_num***]]**

Syntax Definitions

ring_id	An existing ERP ring ID number. The valid range is 1 to 2147483647.
slot/port	The slot number for the module and the physical port number on that module.
agg_num	The link aggregate ID number.

Defaults

By default, configuration information is displayed for all ERP rings in the switch configuration.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Enter a ring ID to display the configuration for a specific ring.
- Enter a ring port number or a link aggregate ID to display the configuration for a specific port or link aggregate.
- The specified ring ID must exist in the switch configuration.

Examples

Output for Normal Ring :

```
-> show erp ring 1
Ring Id                 : 1,
Ring Type               : Normal Ring,
Ring Port1              : 1/1,
Ring Port2              : 1/2,
Ring Status             : enabled,
Service VLAN            : 500,
Revertive Mode          : enabled,
WTR Timer (min)         : 5,
Guard Timer (centi-sec) : 50,
Virtual Channel         : enabled,
MEG Level               : 1,
Ring State              : idle,
Active ERP version      : Ver 2,
Ring Node Type          : non-rpl,
Last State Change       : FRI AUG 31 07:33:26 2012  (sysUpTime 00h:29m:29s)
```

Output for Sub Ring :

```
-> show erp ring 2
Ring Id                 : 2,
Ring Type               : Sub-ring,
Sub-ring Port           : 1/4,
Ring Status             : enabled,
Service VLAN            : 700,
Revertive Mode          : enabled,
WTR Timer (min)         : 5,
Guard Timer (centi-sec) : 50,
Virtual Channel         : enabled,
MEG Level               : 1,
Ring State              : protection,
Active ERP version      : Ver 2,
Ring Node Type          : non-rpl,
Last State Change       : MON SEP 03 02:54:15 2012  (sysUpTime 01h:31m:44s)
```

Command output when ERP version 1 is active:

```
-> show erp ring 1
Ring Id                 : 1,
Ring Type               : Normal Ring,
Ring Port1              : 1/5,
Ring Port2              : 1/6,
Ring Status             : disabled,
Service VLAN            : 190,
Revertive Mode          : enabled,
WTR Timer (min)         : 5,
Guard Timer (centi-sec) : 50,
Virtual Channel         : enabled,
MEG Level               : 1,
Ring State              : init,
Active ERP version      : Ver 1,
Ring Node Type          : non-rpl,
Last State Change       : TUE NOV 27 21:27:44 2012  (sysUpTime 00h:00m:00s)
```

```
-> show erp

         WTR  to Wait To Restore
         MEG  to Maintenance Entity Group

  Ring      Ring  Ring    Ring     Serv  WTR  Guard  MEG        Ring      Ring
   ID       Port1 Port2   Status   VLAN Timer Timer Level       State     Node
                                       (min) (csec)
----------+------+------+---------+----+-----+-----+-----+-----------+--------
         1   1/15    1/1   enabled 4094    3    50     2         idle      rpl
         2    6/7    4/1   enabled 4093    1    50     1         idle      rpl
         3    4/7    6/1   enabled 4092    1    50     3         idle      rpl
         4    4/8   6/23   enabled 4091    5    50     4         idle  non-rpl

Total number of rings configured = 4
```

output definitions

Ring ID	The ERP ring ID number.
Ring Ports	The slot and port number of the ring ports.
Ring Status	The ring status **(enabled** or **disabled)**.
Service VLAN	The Service VLAN ID.
WTR Timer	The wait-to-restore timer value in minutes for RPL node.
Guard Timer	The guard timer value in centi-secs for the ring node.
MEG Level	The Service VLAN Management Entity Group (MEG) level.
Ring State	Indicates the state of the ring.
Active ERP Version	Specifies the active ERP version on the Switch - **ERP Version 1** or **ERP Version 2.**
Ring Node Type	Indicates the type of the ring node.
Last State Change	Indicates the time when the last state change occurred.

```
-> show erp port 1/1

Ring-Id : 1

Ring Port Status     : forwarding,
Ring Port Type       : non-rpl,
Ethoam Event         : disabled,
Remote-endpoint Id   : none
```

output definitions

Ring ID	The ERP ring ID number.
Ring Port Status	The status of the ring port (**blocking** or **forwarding**).
Ring Port Type	The type of ring port (**RPL** or **non-RPL**).
Ethoam Event	Indicates whether or not the ring port will accept Ethernet OAM loss of connectivity events (**enabled** or **disabled)**.
Remote-endpoint ID	The remote Ethernet OAM MEP ID number from which this port accepts loss of connectivity events. This field displays only when the ring port is configured to receive such events.

Release History

Release 6.3.4 ; command introduced.
Release 6.4.5; **Active ERP version** field added

Related Commands

show erp statistics	Displays ERP ring statistics.

MIB Objects

```
alaErpRingId
   alaErpRingStatus
   alaErpRingServiceVid
   alaErpRingMEGLevel
   alaErpRingPort1
   alaErpRingPort2
   alaErpRingPortIfIndex
   alaErpRingState
   alaErpRingPortStatus
   alaErpRingPortType
   alaErpRingPortEthOAMEvent
   alaErpRingPortRmepId
   alaErpRingGuardTimer
   alaErpRingLastStateChange
   alaErpRingTimeToRevert
```

show erp statistics

Displays the ERP statistics for all rings, a specific ring, or a specific ring port.

show erp statistics [ring *ring_id* **[port** *slot/port* **| linkagg** *agg_num***]]**

Syntax Definitions

ring_id	An existing ERP ring ID number. The valid range is 1 to 2147483647.
slot/port	The slot number for the module and the physical port number on that module.
agg_num	The link aggregate ID number.

Defaults

By default, statistics are displayed for all ERP rings in the switch configuration.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Enter a ring ID to display the statistics for a specific ring.
- Enter a ring ID and a ring port number or link aggregate ID to display the statistics for a specific port or link aggregate.
- The specified ring ID must exist in the switch configuration.
- The specified port must belong to the ring identified by the ring ID.

Examples

```
-> show erp statistics

Signal_Fail_PDUs No_Request_PDUs No_Req_Block_PDUs     Invalid_PDUs

Ring  Port Sent  Recv Drop Sent  Recv    Drop   Sent     Recv     Drop   Receive
-----+----+----+----+----+------+------+-------+------+---------+-------+--------
  1   1/1   0    0     0    0    0      0       0      2066       0       0

  1   1/2    0   0     0     0   0     0        0      2066       0       0

  2   1/4    0  2024   0    0     6      0       0      49       0       0
```

output definitions

Ring ID	The ERP ring ID number.
Ring Port	The slot and port number of the ring port.

output definitions (continued)

R-APS	The type of Ring Automatic Switching Protocol (R-APS) event message (**NR** = no request, **RB** = RPL is blocked, **SF** = signal failure). APS is the protocol ERP uses to monitor and control ring links.
Send	Total number of R-APS messages sent.
Recv	Total number of R-APS messages received.
Drop	Total number of R-APS messages dropped.

Release History

Release 6.3.4 ; command introduced.

Related Commands

show erp	Displays the ERP ring configuration for the switch.
clear erp statistics	Clears ERP ring statistics.

MIB Objects

```
alaERPClearStats
alaERPRingClearStats
alaErpRingPortClearStats
alaErpRingId
   alaErpRingPortIfIndex
   alaErpStatsSignalFailPduTx
   alaErpStatsSignalFailPduRx
   alaErpStatsSignalFailPduDrop
   alaErpStatsNoRequestPduTx
   alaErpStatsNoRequestPduRx
   alaErpStatsNoRequestPduDrop
   alaErpStatsRPLBlockPDUTx
   alaErpStatsRPLBlockPDURx
   alaErpStatsRPLBlockPDUDrop
   alaErpStatsPDUErr
```

10 Loopback Detection Commands

Loopback Detection (LBD) automatically detects and prevents forwarding loops on ports that have forwarded network traffic which has looped back to the originating switch. LBD detects and prevents Layer 2 forwarding loops on a port either in the absence of other loop detection mechanisms such as STP/ RSTP/MSTP, or when these mechanisms cannot detect it (e.g., a client's equipment may drop BPDUs, or the STP protocol may be restricted to the network edge). On a linkagg port, if one port of linkagg is getting shutdown due to LBD then all the ports of linkagg will go to shutdown state.

Loopback Detection is enabled system wide and on a per-port basis.Once a loop is discovered, the port from which the loop originated is placed into an “Inactive” state and when the two ports of a switch is connected to each other via a hub, either the ports will be shutdown or it will be in normal state.

When loopback occurs, a trap is sent and the event is logged. The port can manually be enabled again when the problem is resolved.

MIB information for the Loopback Detection commands is as follows:

Filename: alcatelIND1LBD.mib
Module: ALCATEL-IND1-LBD-MIB

A summary of available commands is listed here:

loopback-detection
loopback-detection port
loopback-detection transmission-timer
show loopback-detection
show loopback-detection port
show loopback-detection statistics port

loopback-detection

Enables or disables Loopback Detection (LBD) globally on the switch.

loopback-detection {enable | disable}

Syntax Definitions

enable	Enables LBD on the switch.
disable	Disables LBD on the switch.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- LBD can be enabled globally and per port without any dependency but loopback-detection will be operational only if LBD is enabled globally and also on the specific port.
- LBD can be configured for a port and the configuration can be applied and retained, whether or not LBD is enabled globally. However, LBD functionality on a port is available only when LBD is enabled globally on the switch.

Examples

```
-> loopback-detection enable
```

Release History

Release 6.4.5; command was introduced.

Related Commands

loopback-detection port	Enables or disables LBD on a specific port.
show loopback-detection	Displays LBD configuration information.

MIB Objects

```
alaLdbConfigTable
   alaLdbGLobalConfigStatus
```

loopback-detection port

Enables or disables LBD on a specific port.

loopback-detection port *slot/port* [*-port2*] **{enable | disable}**

Syntax Definitions

slot/port	The slot number and the physical port number of the module that is being configured for LBD.
-port2	Specifies the last port in the range of ports.
enable	Enables LBD on the specified port.
disable	Disables LBD on the specified port.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Loopback Detection must be enabled globally to enable LBD functionality on a specific port.
- LBD can be configured for a port and the configuration can be applied and retained, whether or not LBD is enabled globally. However, LBD functionality on a port is available only when LBD is enabled globally on the switch.

Examples

```
-> loopback-detection port 1/1 enable
-> loopback-detection port 1/1-8 enable
```

Release History

Release 6.4.5; command was introduced.

Related Commands

loopback-detection	Enables or disables LBD globally on the switch.
show loopback-detection	Displays LBD configuration information.

MIB Objects

```
alaLdbPortConfigTable
   alaLdbPortConfigEntry
   alaLdbPortConfigIndex
   alaLdbPortConfigLdbAdminStatus
   alaLdbPortConfigLdbOperStatus
```

loopback-detection transmission-timer

Configures the LBD transmission timer on the switch.The transmission time is the time period between the consecutive LBD packet transmissions.

loopback-detection transmission-timer *seconds*

Syntax Definitions

seconds	The time period in seconds between LBD packet transmissions. The valid range is from 5 to 600 seconds.

Defaults

parameter	default
seconds	30

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- If the timer value is not configured, the default value of 30 seconds is assigned to the transmission period.
- The timer can be modified at any time. However, the new timer value will come into effect only after the timer is restarted.

Examples

```
-> loopback-detection transmission-timer 200
```

Release History

Release 6.4.5; command was introduced.

Related Commands

loopback-detection	Enables or disables LBD globally on the switch.
show loopback-detection	Displays LBD configuration information.

MIB Objects

```
alaLdbConfigTable
   alaLdbGLobalConfigTransmissionTimer
```

show loopback-detection

Displays the global LBD configuration information for the switch.

show loopback-detection

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use this command to display the global configuration of LDB.
- To view information for a specific port, use the **show loopback-detection port** command.

Examples

```
-> show loopback-detection

Global LBD Status                          : Enabled
Global LBD Transmission Timer              : 200 sec

-> show loopback-detection port 1/1

Global LBD Status                          : Enabled
Global LBD Transmission Timer              : 200 sec
Port LBD Status                            : Enabled
Port LBD State                             : Normal
```

output definitions

Global LBD Status	The current status of LBD of the switch (**Enabled** or **Disabled**).
Globas LBD Transmission Timer	Displays the time interval in seconds between LBD packet transmissions.

Release History

Release 6.4.5; command was introduced.

Related Commands

loopback-detection	Enables or disables LBD globally on the switch.
show loopback-detection port	Displays LBD configuration information for all ports on the switch.

MIB Objects

```
alaLdbConfigTable
   alaLdbGLobalConfigStatus
```

show loopback-detection port

Displays global LBD configuration information on the switch. When slot and port number is mentioned, the LBD configuration information of the specific port is displayed.

show loopback-detection port [*slot/port*]

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use this command to view LBD information of a specific port on a switch.

Examples

```
-> show loopback-detection port
Slot/Port     Admin State       OperState
------------+---------------+-----------------

1/2           enabled         Normal

-> show loopback-detection port 1/1
Global LBD Status                          : Enabled
Global LBD Transmission Timer              : 200 sec
Port LBD Status                            : Enabled
Port LBD State                             : Normal
```

output definitions

Global LBD Status	The current status of LBD of the switch (**Enabled** or **Disabled**).
Globas LBD Transmission Timer	Displays the time interval in seconds between LBD packet transmissions.
Slot/Port	The slot/port number LBD port.
Admin State	The administrative state of the port (**Enabled** or **Disabled**).
Oper State	The operational state of the port (**Normal** or **Inactive**).

Release History

Release 6.4.5; command was introduced.

Related Commands

loopback-detection	Enables or disables LBD globally on the switch.
show loopback-detection	Displays LBD configuration information for the switch or for a specific port.

MIB Objects

```
alaLdbConfigTable
   alaLdbGLobalConfigStatus
```

show loopback-detection statistics port

Displays LBD statistics information for a specific port on the switch.

show loopback-detection statistics port [*slot/port*]

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use this command to view LDB statistics of a specific port on a switch.

Examples

```
-> show loopback-detection statistics port 1/1

LBD Port Statistics
LBD Packet Send               : 1
Invalid LBD Packet Received   : 0
```

output definitions

Slot/Port	The slot/port number LBD port.
LBD Packet Send	The number of LBD packet sent from the port.
Invalid LBD Packet Received	The number of invalid LBD packets received on the port.

Release History

Release 6.4.5; command was introduced.

Related Commands

loopback-detection	Enables or disables LBD globally on the switch.
show loopback-detection	Displays LBD configuration information for the switch or for a specific port.

MIB Objects

```
alaLdbConfigTable
   alaLdbGLobalConfigStatus
```

11 CPE Test Head Commands

The Customer Provider Edge (CPE) Test Head traffic generator and analyzer is a Test-OAM (Operation, Administration, and Maintenance) tool used in the Metro Ethernet Network to validate the customer Service Level Agreements (SLA). This functionality allows the operator to validate the Metro Ethernet Network between customer end points, which is critical when provisioning or troubleshooting network services.

The implementation of CPE Test Head supports unidirectional, ingress tests. Traffic is generated at the UNI port as if the traffic was generated from a test head connected to the UNI port. This validates the actual customer SLA by subjecting the test traffic to the ingress QoS defined at the UNI port (Ethernet SAP profile or QoS policy rules for priority and bandwidth control) and the egress QoS defined at the egress NNI port and carrier network.

The CPE test is non-disruptive to traffic running on other UNI ports that are associated with the same SAP profile as the test UNI port. All UNI ports, including CPE test ports, are subject to any SAP profile or QoS configuration associated with the port. This is important to consider when analyzing test results.

The feature provides a multi-stream test capability. The feature supports a stack containing up to eight switches.

Multi-stream test requires an extra port which is known as the feeder port. The feeder port can be any port with any configuration. When a multi-stream test starts, the port is made out of service. The port is made operational again and the configuration is retained when the test is stopped.

MIB information for the CPE Test Head commands are:

Filename: alcatelIND1testoam.mib
Module: ALCATEL-IND1-TEST-OAM-MIB

A summary of available commands is listed here:

Single-test	**test-oam** **test-oam direction** **test-oam src-endpoint dst-endpoint** **test-oam port** **test-oam vlan test-frame** **test-oam role** **test-oam duration rate packet-size** **test-oam frame** **test-oam start stop** **show test-oam** **show test-oam statistics** **clear test-oam statistics**
Multi-test	**test-oam group** **test-oam group tests** **test-oam feeder-port** **test-oam group src-endpoint dst-endpoint** **test-oam group role** **test-oam group port** **test-oam group direction** **test-oam group duration rate** **test-oam group start** **test-oam group stop** **clear test-oam group statistics** **show test-oam group** **show test-oam group statistics**

test-oam

Configures the CPE test name and an optional description. The test name is used to identify and configure a CPE test profile.

test-oam *string* **[descr** *description***]**

no test-oam *string*

Syntax Definitions

string	The name of the CPE test, an alphanumeric string between 1 and 32 characters. This name is used to identify a specific CPE test and is also referred to as the test ID.
description	The description to assign to the test name, an alphanumeric string between 1 and 32 characters.

Defaults

parameter	default
description	DEFAULT

Platforms Supported

OmniSwitch 6400, 6850E, 6855-U24X, 9000E

Usage Guidelines

- Use the **no** form of this command to remove the specified CPE test configuration.
- This command creates a CPE test profile that is identified by the test name. Make sure the name specified does not exist in the switch configuration.
- A maximum of 32 tests can be configured.
- Only one test can be active on the switch at any given time.

Examples

```
-> test-oam Test1
-> test-oam Test2 descr second-test
-> no test-oam Test2
```

Release History

Release 6.4.5; command was introduced.

Related Commands

show test-oam	Displays the CPE test configuration and status.
show test-oam statistics	Displays CPE test statistics.

MIB Objects

```
alaTestOamConfigTable
   alaTestOamConfigTestName
   alaTestOamConfigTestDescription
   alaTestOamConfigRowStatus
```

test-oam direction

Configures the CPE test direction.

test-oam *string* **[direction {unidirectional | bidirectional}]**

Syntax Definitions

string	The name of the CPE test, an alphanumeric string between 1 and 32 characters. This name is used to identify a specific CPE test and is also referred to as the test ID.
direction	The direction of the cpe test.

Defaults

parameter	default
unidirectional | bidirectional	unidirectional

Platforms Supported

OmniSwitch 6400, 6850E, 6855-U24X, 9000E

Usage Guidelines

This command assignes the direction to the cpe test.

Examples

```
-> test-oam Test1 direction unidirectional
```

Release History

Release 6.4.5; command was introduced.

Related Commands

show test-oam	Displays the CPE test configuration and status.
show test-oam statistics	Displays CPE test statistics.

MIB Objects

```
alaTestOamConfigTable
   alaTestOamConfigTestName
   alaTestOamConfigDirection
```

test-oam src-endpoint dst-endpoint

Configures the source and destination endpoints for the specified test.

test-oam *string* **[src-endpoint** *src-string***] [dst-endpoint** *dst-string***]**

Syntax Definitions

string	The name of an existing CPE test.
src-string	The management IP address or DNS host name of the switch that transmits test traffic.
dst-string	The management IP address or DNS host name of the switch that receives test traffic. This is the switch on which traffic analysis is done.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855-U24X, 9000E

Usage Guidelines

- Using the DNS host name of the switch is highly recommended, as this name is unique and is mapped to an IP address configured for the switch.
- This command automatically overwrites the source and destination endpoint values previously configured for the specified CPE test.

Examples

```
-> test-oam Test1 src-endpoint SW1 dst-endpoint SW2
-> test-oam Test1 src-endpoint SW1
-> test-oam Test1 dst-endpoint SW2
```

Release History

Release 6.4.5; command was introduced.

Related Commands

test-oam port	Configures the port on which the CPE test will run.
show test-oam	Displays the CPE test configuration and status.

MIB Objects

```
alaTestOamConfigTable
   alaTestOamConfigTestName
   alaTestOamConfigSourceEndpoint
   alaTestOamConfigDestinationEndpoint
```

test-oam port

Configures the port on which the CPE test will run. Use this command on the switch that will generate the test traffic. If the switch is going to receive test traffic, configuring a test port is not necessary.

test-oam *string* **port** *slot/port*

Syntax Definitions

string	The name of an existing CPE test.
slot/port	The port on which the CPE test will generate traffic.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855-U24X, 9000E

Usage Guidelines

- In an Ethernet Service environment, the UNI port is designated as the test port on the generator switch to simulate traffic coming in on the port as if it was sent from a test head device. This will subject the test traffic to the SAP profile.
- Note that the customer traffic is disrupted on ports configured as CPE test ports. Configuring a port that is not in use is recommended. In addition, if the test port is a UNI port associated with an SAP profile, only that UNI port is used for the test. Traffic on other UNI ports associated with the same profile is *not* disrupted by the CPE test.
- All UNI ports, including CPE test ports, are subject to any SAP profile or QoS configuration associated with the port. This should be considered when test results are analyzed.
- This command automatically overwrites the port value previously configured for the specified CPE test.
- If VFL or MCLAG is already configured on DUT, then an error message is displayed that the Test-oam configuration is not allowed on DUT's having MCLAG and VFL configuration.
- It is recommended to configure the ports of the same speed for the feeder and generator.

Examples

```
-> test-oam Test1 port 1/2
```

Release History

Release 6.4.5; command was introduced.

Related Commands

test-oam vlan test-frame	Configures the source mac-address, destination mac-address, and the SVLAN for the test-frame used in the test.
show test-oam	Displays the CPE test configuration and status.

MIB Objects

```
alaTestOamConfigTable
   alaTestOamConfigTestName
   alaTestOamConfigPort
```

test-oam vlan test-frame

Configures the SVLAN and the source and destination MAC addresses for the test frame. Use this command to configure these test parameters on both the generator (local) switch and the analyzer (remote) switch for the specified CPE test.

test-oam *string* **[vlan** *svlan***] [[test-frame [src-mac** *src-address***] [dst-mac** *dst-address***]]**

Syntax Definitions

string	The name of an existing CPE test.
svlan	The service VLAN ID. This is used for traffic analysis and test-frame accounting.
src-address	Source mac-address of the test-frame.
dst-address	Destination mac-address of the test-frame.

Defaults

parameter	default
src-address	00:00:00:00:00:00
dst-address	00:00:00:00:00:00

Platforms Supported

OmniSwitch 6400, 6850E, 6855-U24X, 9000E

Usage Guidelines

- Although the source and destination MAC addresses are optional parameters with this command, the test will not run if these addresses are set to all zeros (the default).
- Make sure that routing is disabled on the specified SVLAN.
- Avoid configuring any IEEE reserved MAC addresses as the destination MAC address for the test.
- This command automatically overwrites the SVLAN, source MAC, or destination MAC values previously configured for the specified CPE test.

Examples

```
-> test-oam Test1 vlan 100 test-frame src-mac 00:01:02:00:00:02 dst-mac
00:00:01:00:00:90
-> test-oam Test1 vlan 100
-> test-oam Test1 test-frame src-mac 00:01:02:00:00:02 dst-mac 00:00:01:00:00:90
-> test-oam Test1 test-frame src-mac 00:01:02:00:00:02
-> test-oam Test test-frame dst-mac 00:00:01:00:00:90
```

Release History

Release 6.4.5; command was introduced.

Related Commands

test-oam role	Configures the switch as a generator or analyzer for the test.
show test-oam	Displays the CPE test configuration and status.

MIB Objects

```
alaTestOamConfigTable
   alaTestOamConfigTestName
   alaTestOamConfigVlan
   alaTestOamConfigFrameSrcMacAddress
   alaTestOamConfigFrameDstMacAddress
```

test-oam role

Configures the role the switch will perform for the specified CPE test. The type of role assigned determines whether the switch transmits (generator) or receives (analyzer) test frames.

test-oam *string* **role {generator | analyzer}**

Syntax Definitions

string	The name of an existing CPE test.
generator	Configures the switch as the test generator.
analyzer	Configures the switch as the test analyzer.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855-U24X, 9000E

Usage Guidelines

- Use this command on the switch that will perform the specified role.
- Configuring a generator and an analyzer switch for each test is required.
- It is recommended to configure the ports of the same speed for the feeder and generator.
- Only one role can be assigned to the switch for a particular test.
- This command automatically overwrites the previously configured switch role for the specified CPE test.

Examples

```
-> test-oam Test1 role generator
-> test-oam Test2 role analyzer
```

Release History

Release 6.4.5; command was introduced.

Related Commands

test-oam duration rate packet-size	Configures the test frame duration, rate, and packet-size for the test.
show test-oam	Displays the CPE test configuration and status.

MIB Objects

```
alaTestOamConfigTable
   alaTestOamConfigTestName
   alaTestOamConfigRole
```

test-oam duration rate packet-size

Configures the duration, rate, and packet-size for the specified test. Use this command to configure these test parameters on the generator switch.

test-oam *string* **[duration** *secs***] [rate** *rate***] [packet-size** *bytes***]**

Syntax Definitions

string	The name of an existing CPE test.
secs	The duration of the test, in seconds. This is the amount of time the generator will actively transmit test packets to the remote (analyzer) switch. The valid time range is 5–3600 seconds
rate	The rate, in kbps or mbps, at which test traffic is generated. The minimum value allowed is 64 kbps to line rate. The granularity of the transmit rate is 64 Kbps for 100 Mbps port and 2 Mbps for 1Gig ports.
bytes	The packet size, in bytes. The valid range is 64–9212 bytes.

Defaults

Parameter	Default
secs	5 secs
rate	64 kbps
bytes	64 byte

Platforms Supported

OmniSwitch 6400, 6850E, 6855-U24X, 9000E

Usage Guidelines

- This command automatically overwrites any duration, rate, and packet size parameter values previously configured for the specified CPE test.
- The status of the CPE test will change to “ended” when the test duration time expires.
- This command automatically overwrites the duration, rate, or packet size values previously configured for the specified CPE test.
- For ipv6 test frames the minimum packet size should be 74 for UDP and 86 for TCP.

Examples

```
-> test-oam Test1 duration 10 rate 64k packet-size 64
-> test-oam Test1 rate 64k
-> test-oam Test1 duration 10
-> test-oam Test1 packet-size 64
```

Release History

Release 6.4.5; command was introduced.

Related Commands

test-oam frame	Configures the test frame parameter values for the CPE test.
show test-oam	Displays the CPE test configuration and status.

MIB Objects

```
alaTestOamConfigTable
   alaTestOamConfigTestName
   alaTestOamConfigDuration
   alaTestOamConfigGeneratorBandwidth
   alaTestOamConfigGeneratorPacketSize
```

test-oam frame

Configures the test frame parameter values for the specified CPE test. Use this command on the switch that will generate the test frame traffic.

test-oam *string* **frame**
[vlan-tag *vlan-id* **[drop-eligible {true|false}] [priority** *num***] |**
[ether-type {
[ipv4 {src-ip *src-ipv4* **dst-ip** *dest-ipv4***} [data-pattern** *pattern***] [protocol {udp | tcp {src-port** *port* **dst-port** *port***}}] [ttl** *ttl***] [tos** *tos***]]|**
[ipv6 {src-ip *src-ipv6* **dst-ip** *dest-ipv6***} [data-pattern** *pattern***] [hop-limit** *hop-limit***] [flow-label** *flow-label***] [next-header {udp|tcp {src-port** *port* **dst-port** *port***}}] [traffic-class** *traffic-class***]]**
]}

Syntax Definitions

string	The name of an existing CPE test.
vlan-id	The VLAN ID of the frame.
drop-eligible	The drop-eligible value, either true or false.
priority	The priority value. The valid range is 0–7.
ether-type	The ether-type is configured for L2 packet. The ether-type can be ipv4 or ipv6.
ipv4	Use ipv4 to configure the frame type as ipv4. The related ipv4 parameters must be configured.
src-ipv4	The source IP address for an IPv4 test frame.
dest-ipv4	The destination IP address for an IPv4 test frame.
pattern	The data pattern present in the generated test frame. The valid range is 0x0000–0xffff.
protocol	configure protocol type, either udp or tcp.
udp	Specifies the UDP protocol.
tcp	Specifies the TCP protocol.
src-port	The source port of the generated test frame.
dst-port	The destination port of the generated test frame.
ttl	The time-to-live value. The valid range is 0–255.
tos	The type-of-service value for QoS features. The valid range is 0x0–0xff.
ipv6	Use ipv6 to configure the frame type as ipv6. The related ipv6 parameters must be configured.
src-ipv6	The source IP address for an IPv6 test frame.
dest-ipv6	The destination IP address for an IPv6 test frame.

hop-limit	Configure the maximum hop-limit.
flow-label	Configure the flow-level for the flow-specific treatment.
next-header	Configure the next transport layer protocol (udp/tcp).
traffic-class	Configure the Differentiated Services Code Point (DSCP) value for traffic management.

Defaults

Parameter	Default
priority	7
drop-eligible	false
ttl	64
tos	0x0
pattern	0x0000

Platforms Supported

OmniSwitch 6400, 6850E, 6855-U24X, 9000E

Usage Guidelines

- Specify the Ether type in hexadecimal format to configure a Layer 2 test frame.
- Specify **ipv4** or **ipv6** as the Ether type to configure a Layer 3 test frame. When this option is selected, entering a source and destination IP address is required.
- For **ipv6** as ether type, the minimum packet size must be 74 for UDP and 86 for TCP.
- Do not specify reserved Ether type values.
- This command automatically overwrites the test packet parameter values previously configured for the specified CPE test.

Examples

If the ether-type is a hexadecimal number (Layer 2 test frame):

```
-> test-oam Test1 frame vlan-tag 1 priority 2 drop-eligible 0 ether-type 0x0100
data-pattern 0x0010
```

If the ether-type is IPV4 (Layer 3 test frame):

```
-> test-oam Test1 frame vlan-tag 1 priority 2 drop-eligible 0 ether-type ipv4 src-
ip 1.1.1.1 dst-ip 2.2.2.2 ttl 4 tos 0x01 protocol udp src-port 2000 dst-port 3000
data-pattern 0x0010
```

If the ether-type is IPV6:

```
-> test-oam  Test1 frame vlan-tag 10 priority 5 ipv6 src-ip 10::1 dst-ip 20::1 tcp
src-port 2000 dst-port 3000
```

Release History

Release 6.4.5; command was introduced.

Related Commands

test-oam start stop	Start or stop the CPE test.
show test-oam	Displays the CPE test configuration and status.

MIB Objects

```
alaTestOamConfigTable
   alaTestOamConfigTestName
alaTestOamEtherConfigTable
alaTestOamIpv4ConfigTable
```

test-oam start stop

Starts or stops the CPE test operation.

test-oam *string* **{[vlan** *vlan-id***] [port** *slot/port***] [packet-size** *bytes***] start | stop}**

Syntax Definitions

string	The name of an existing CPE test.
vlan-id	The service VLAN ID. This value is required only for traffic analysis and test frame accounting and is not related to the VLAN tag specified for the actual test frame.
slot/port	The switch port on which the test is run.
bytes	The size of the test packet, in bytes. The valid packet size range is 64–9212 bytes.
start	Starts the CPE test operation.
stop	Stops the CPE test operation.

Defaults

Parameter	Default
bytes	64

Platforms Supported

OmniSwitch 6400, 6850E, 6855-U24X, 9000E

Usage Guidelines

- Ensure that routing is disabled on the specified service VLAN.
- The optional **vlan**, **port,** and **packet-size** parameters specify “active” parameter values that are applied when the specified CPE test is started. If these same parameters are defined within a CPE test profile, they are considered “configured” parameter values. Active parameter values override configured parameter values when the test is started.
- If no active parameter values are specified with this command, the test is started using the configured values defined in the CPE test profile. However, if active parameter values are not specified and the CPE test does not contain any configured values for these parameters, the test will not run.
- Specifying any of the optional parameter values does not change the configured values associated with the CPE test.
- If the specified port resides on a switch that will transmit test traffic, the port will generate the test frames. However, if the switch is an analyzer switch, specifying a port is not required.
- Start the specified test on the analyzer switch first and then on the generator switch.

- The test will stop when the test duration time expires or when the test is manually stopped using the **test-oam stop** command.
- Manually restart the test if the test is interrupted by a takeover, restart, or hot swap.
- The previous statistics related to the test will be cleared automatically once the test is started.

Examples

```
-> test-oam Test1 start
-> test-oam Test1 vlan 100 start
-> test-oam Test1 port 1/1 start
-> test-oam Test1 packet-size 100 start
-> test-oam Test1 vlan 100 port 1/1 packet-size 100 start
-> test-oam Test1 stop
```

Release History

Release 6.4.5; command was introduced.

Related Commands

show test-oam statistics	Displays CPE test statistics.
show test-oam	Displays the CPE test configuration and status.

MIB Objects

```
alaTestOamConfigTable
   alaTestOamConfigTestName
   alaTestOamConfigVlan
   alaTestOamConfigPort
   alaTestOamConfigGeneratorPacketSize
   alaTestOamConfigTestIdState
```

show test-oam

Displays the CPE test configuration and status.

show test-oam [tests | *string***]**

Syntax Definitions

tests	Displays information for all the CPE tests**.**
string	The name of an existing CPE test.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855-U24X, 9000E

Usage Guidelines

- Use the **tests** parameter to display information for all CPE tests configured on the switch.
- Use the *string* parameter to display detailed information for a specific CPE test.

Examples

```
-> show test-oam tests
Total Test-Ids: 4
Test-Id  Port  Src-Mac           Dst-Mac            Vlan  Direction     Status
---------+-----+-----------------+------------------+-----+-------------+-----------
Test1    1/1  00:11:22:33:44:55 00:22:33:44:55:66  100   unidirectional ended
Test2    1/2  00:44:22:33:44:55 00:66:33:44:55:66  200   unidirectional stopped
Test3    2/3  00:00:00:00:00:03 00:00:00:00:00:04  200   unidirectional not-started
Test4    1/1  00:00:00:00:00:07 00:00:00:00:00:08  100   unidirectional running
```

output definitions

Test-Id	The CPE test name (ID). Configured through the **test-oam** command.
Port	The port on which the test is run. Configured through the **test-oam port** command.
Src-Mac	The source MAC address of the test frame. Configured through the **test-oam vlan test-frame** command.
Dst-Mac	The destination MAC address of the test frame. Configured through the **test-oam vlan test-frame** command.
Vlan	The service VLAN (SVLAN) associated with the test. Configured through the **test-oam vlan test-frame** command.
Direction	The direction of the test traffic. Note that only unidirectional traffic tests are supported.
Status	The operational status of the test

```
-> show test-oam Test1
Legend: dei-drop eligible indicator
TEST Parameters for Test1:
  Source Endpoint      : SW1,
  Destination Endpoint : SW2,
  Test Description     : Ether Test,
  Direction            : unidirectional,
  Source MAC           : 00:11:22:33:44:55,
  Destination MAC      : 00:22:33:44:55:66,
  Duration             : 10(secs),
  Vlan                 : 100,
  Role                 : generator,
  Port                 : 1/1,
  Tx Rate              : 80m,
  Frame Size           : 100,
  State                : start,
  Status               : running

Frame Configuration:
  Frame Type : ether,
  Vlan       : 200,
  Priority   : 7,
  Pattern    : 0x0001,
  Ether Type : 0x8000,
  Dei        : none,
```

Example for ether-type as ipv6:

```
-> show test-oam Test2
TEST Parameters for Test2:
  Source Endpoint      : SW1,
  Destination Endpoint : SW2,
  Test Description     : IPV6 Test,
  Direction            : unidirectional,
  Source MAC           : 00:11:22:33:44:55,
  Destination MAC      : 00:22:33:44:55:66,
  Duration             : 10(secs),
  Vlan                 : 100,
  Role                 : generator,
  Port                 : 1/1,
  Tx Rate              : 8k,
  Frame Size           : 100,
  State                : start,
  Status               : running

    Frame Configuration :
      Frame Type       : ipv6,
      Vlan             : 200,
      Priority         : 7,
      Pattern          : 0x0001,
      Dei              : true,
      Source Ip        : 2001:db8:0:0:0:ff00:42:8329,
      Destination Ip   : 1080:0:0:0:8:800:200C:4171,
      Source Port      : 10,
      Destination Port : 20,
      Next Header      : tcp,
      Hop-Count        : 50,
      Traffic-Class    : 0xff
```

```
Flow-Label       : 0x0
```

output definitions

Source Endpoint	The host name for the source (generator) switch. Configured through the **test-oam src-endpoint dst-endpoint** command.
Destination Endpoint	The host name for the destination (analyzer) switch. Configured through the **test-oam src-endpoint dst-endpoint** command.
Test Description	Description for the test name. Configured through the **test-oam** command.
Direction	The direction of the test traffic. Note that only unidirectional traffic tests are supported.
Source MAC	The source MAC address for the test frame. Configured through the **test-oam vlan test-frame** command.
Destination MAC	The destination MAC address for the test frame. Configured through the **test-oam vlan test-frame** command.
Duration	The amount of time the test will run. Configured through the **test-oam duration rate packet-size** command.
Vlan	The service VLAN (SVLAN) associated with the test. Configured through the **test-oam vlan test-frame** command.
Role	The role of the switch for this test (**generator** or **analyzer**). Configured through the **test-oam role** command
Port	The port on which the test is run. Configured through the **test-oam port** command.
Tx Rate	The rate at which packets are transmitted on the test port. Configured through the **test-oam duration rate packet-size** command.
Frame Size	The size of the test frame. Configured through the **test-oam duration rate packet-size** command.
State	The administrative state of the test (**stop** or **start**). Configured through the **test-oam start stop** command.
Status	The operational status of the test (**running**, **ended**, **stopped**, or **not started**).
Frame Configuration	The test frame type (**ether**, **ipv4, or ipv6**) and associated parameter values. Configured through the **test-oam frame** command.

Release History

Release 6.4.5; command was introduced.

Related Commands

show test-oam statistics	Displays CPE test statistics.

MIB Objects

```
alaTestOamConfigTable
alaTestOamEtherConfigTable
alaTestOamIpv4ConfigTable
```

show test-oam statistics

Displays the statistics for all CPE tests or for a specific test name. Use this command on both the generator and analyzer switch to determine test results.

show test-oam [*string***] statistics**

Syntax Definitions

string	The name of an existing CPE test.

Defaults

By default, statistics are displayed for all CPE tests.

Platforms Supported

OmniSwitch 6400, 6850E, 6855-U24X, 9000E

Usage Guidelines

- Use the *string* parameter with this command to display statistics for a specific CPE test.
- The statistics displayed depend on the role the switch is performing for the test (generator or analyzer). For example, the analyzer switch may not show any packet count in the **TX** fields because it is the receiving switch.

Examples

```
-> show test-oam Test1 statistics
Test-Id            TX-Ingress   TX-Egress    RX-Ingress
-----------------+------------+------------+-----------
Test1              1200366      1200366           0

-> show test-oam statistics
Test-Id            TX-Ingress   TX-Egress    RX-Ingress
-----------------+------------+------------+--------------
Test1              1200366      1200366          0
Test2                0            0          1200366
```

output definitions

Test-Id	The CPE test name (ID).
TX-Ingress	The number of ingress test packets generated on the ingress UNI.
TX-Egress	The number of egress test packets transmitted on the egress NNI.
RX-Ingress	The number of test packets received on the ingress NNI. This value is relevant on the receiving (analyzer) switch for the specific test.

Release History

Release 6.4.5; command was introduced.

Related Commands

show test-oam	Displays the CPE test configuration and status.
clear test-oam statistics	Clears CPE test statistics.

MIB Objects

```
alaTestOamConfigTable
   alaTestOamConfigTestName
   alaTestOamTxIngressCounter
   alaTestOamTxEgressCounter
   alaTestOamRxIngressCounter
```

clear test-oam statistics

Clears the statistics for all CPE tests or for a specific test name.

clear test-oam [*string***] statistics**

Syntax Definitions

string	The name of an existing CPE test.

Defaults

By default, statistics are cleared for all CPE tests.

Platforms Supported

OmniSwitch 6400, 6850E, 6855-U24X, 9000E

Usage Guidelines

Use the *string* parameter with this command to clear the statistics for a specific CPE test.

Examples

```
-> clear test-oam Test1 statistics
-> clear test-oam statistics
```

Release History

Release 6.4.5; command was introduced.

Related Commands

show test-oam statistics	Displays CPE test statistics.
show test-oam	Displays the CPE test configuration and status.

MIB Objects

```
alaTestOamConfigTable
   alaTestOamConfigTestName
   alaTestOamStatsClearStats
```

test-oam group

Configures the CPE test group name and an optional description. The group name is used to identify and configure a CPE test group.

test-oam group *string* **[descr** *description***]**

no test-oam group *string*

Syntax Definitions

string	The name of the CPE test group, an alphanumeric string between 1 and 32 characters. This name is used to identify a specific CPE test-oam group.
description	The description to assign to the CPE test group, an alphanumeric string between 1 and 32 characters.

Defaults

parameter	default
description	DEFAULT

Platforms Supported

OmniSwitch 6400, 6850E, 6855-U24X, 9000E

Usage Guidelines

- Use the **no** form of this command to remove the specified CPE test group.
- This command creates a CPE test group that is identified by the test-oam name. Make sure the name specified does not exist in the switch configuration.
- To configure a CPE test group, the individual test must be configured.
- A maximum of eight tests can be configured to run concurrently.
- Only one CPE test group can be active on the switch at any given time.

Examples

```
-> test-oam group Testgroup1
-> test-oam group Testgroup2 descr second-testgroup
-> no test-oam group Testgroup1
```

Release History

Release 6.4.5; command was introduced.

Related Commands

show test-oam group	Displays the configuration and status of the CPE test groups.
show test-oam group statistics	Displays the statistics for all CPE test groups or for a specific CPE test group.

MIB Objects

```
alaTestOamGroupConfigTable
   alaTestOamConfigGroupId
   alaTestOamConfigGroupDescription
   alaTestOamGroupConfigRowStatus
```

test-oam group tests

This defines the list of CPE test group tests that need to be added in the test-oam group.

test-oam group *string* **[tests** *string1.....string8***]**

test-oam group *string* **[no tests** *string1.....string8***]**

Syntax Definitions

string	The name of the CPE test group, an alphanumeric string between 1 and 32 characters. This name is used to identify a specific CPE test group.
string1.....string8	The name of the configured test-oam tests.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855-U24X, 9000E

Usage Guidelines

- This command defines the list of test-oam tests that need to run concurrently.
- The test must exist, while configuring the test-oam list.
- A maximum of eight tests can be configured to run concurrently.
- When a CPE test group is running, the modification of a test which is part of the group shall not be allowed.
- When a CPE test group is running, the modification of test-oam group parameters shall not be allowed.
- When a CPE test group is running, the modification of a feeder port shall not be allowed.
- use the **no** form of the command to remove the test-oam tests from the CPE test group.

Examples

```
-> test-oam test1
-> test-oam test2
-> test-oam test3
-> test-oam test4
-> test-oam test5
-> test-oam test6
-> test-oam test7
-> test-oam test8
-> test-oam group Testgroup1 descr first-testgroup
-> test-oam group Testgroup1 tests test1 test2 test3 test4 test5 test6 test7 test8
-> test-oam group Testgroup1 no tests test1 test2 test3
```

Release History

Release 6.4.5; command was introduced.

Related Commands

show test-oam group	Displays the configuration and status of the CPE test groups.
show test-oam group statistics	Displays the statistics for all CPE test groups or for a specific CPE test group.

MIB Objects

```
alaTestOamGroupFlowConfigTable
   alaTestOamConfigGroupId
   alaTestOamConfigTestId
   alaTestOamGroupFlowConfigRowStatus
```

test-oam feeder-port

This configures the feeder port globally in the system for CPE test group to feed the test traffic to generator port.

test-oam feeder-port *slot/port*

no test-oam feeder-port

Syntax Definitions

slot/port	The port to be used to feed the test traffic only to generator port.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855-U24X, 9000E

Usage Guidelines

- This command configures the feeder port globally in the system.
- The feeder port cannot be the generator port and the generator port cannot be the feeder port.
- It is recommended to configure the ports of the same speed for the feeder and generator.
- When a CPE test group is running, the modification to the feeder port shall not be allowed.
- use the **no** form of the command to remove the feeder port from the system for CPE test group.

Examples

```
-> test-oam feeder-port 1/4
-> no test-oam feeder-port
```

Release History

Release 6.4.5; command was introduced.

Related Commands

test-oam group port	Configures the port on which the CPE test group will run.
show test-oam group	Displays the configuration and status of the CPE test groups.

MIB Objects

```
alaTestOamGloabalFeederPort
```

test-oam group src-endpoint dst-endpoint

Configures the source and destination endpoints for the CPE test group.

test-oam group *string* **[src-endpoint** *src-string* **dst-endpoint** *dst-string***] [src-endpoint** *src-string***] [dst-endpoint** *dst-string***]**

Syntax Definitions

string	The name of an existing CPE test group.
src-string	The management IP address or DNS host name of the switch that will transmit test traffic.
dst-string	The management IP address or DNS host name of the switch that will receive test traffic. This is the switch on which traffic analysis is done.

Defaults

parameter	default
src-endpoint	DEFAULT
dst-endpoint	DEFAULT

Platforms Supported

OmniSwitch 6400, 6850E, 6855-U24X, 9000E

Usage Guidelines

- Using the DNS host name of the switch is highly recommended, as this name is unique and is mapped to an IP address configured for the switch.
- When a CPE test group is running, the modification of a test which is part of the group shall not be allowed.
- When a CPE test group is running, the modification of test-oam group parameters shall not be allowed.
- When a CPE test group is running, the modification of a feeder port shall not be allowed.

Examples

```
-> test-oam group Testgroup1 src-endpoint SW1 dst-endpoint SW2
-> test-oam group Testgroup1 src-endpoint SW1
-> test-oam group Testgroup1 dst-endpoint SW2
```

Release History

Release 6.4.5; command was introduced.

Related Commands

test-oam group duration rate	Configures the duration and rate for the specified CPE test group.
show test-oam group	Displays the configuration and status of the CPE test groups.

MIB Objects

```
alaTestOamGroupConfigTable
   alaTestOamConfigGroupId
   alaTestOamGroupConfigSourceEndpoint
   alaTestOamGroupConfigDestinationEndpoint
```

test-oam group role

Configures the role the switch will perform for the specified CPE test group. The type of role assigned determines whether the switch transmits (generator) or receives (analyzer) test frames.

test-oam group *name* **role {generator | analyzer}**

Syntax Definitions

name	The name of an existing CPE test group.
generator	Configures the switch as the test generator.
analyzer	Configures the switch as the test analyzer.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855-U24X, 9000E

Usage Guidelines

- When a CPE test group is running, the modification of a test which is part of the group shall not be allowed.
- When a CPE test group is running, the modification of CPE test group parameters shall not be allowed.
- When a CPE test group is running, the modification of a feeder port shall not be allowed.

Examples

```
-> test-oam group Testgroup1 role generator
-> test-oam group Testgroup2 role analyzer
```

Release History

Release 6.4.5; command was introduced.

Related Commands

test-oam group duration rate	Configures the duration and rate for the specified CPE test group.
show test-oam group	Displays the configuration and status of the CPE test groups.

MIB Objects

```
alaTestOamGroupConfigTable
   alaTestOamConfigGroupId
   alaTestOamGroupConfigRole
```

test-oam group port

Configures the port on which the CPE test group will run. Use this command on the switch that will generate the test traffic.

test-oam group *string* **port** *slot/port*

Syntax Definitions

string	The name of an existing CPE test group.
slot/port	The port on which the CPE test will generate traffic.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855-U24X, 9000E

Usage Guidelines

- Configuring a port that is not in use is recommended. In addition, if the test port is a UNI port associated with an SAP profile, only that UNI port is used for the test. Traffic on other UNI ports associated with the same profile is *not* disrupted by the CPE test.
- This command automatically overwrites the port value previously configured for the specified CPE test group.
- The feeder port cannot be the generator port and the generator port cannot be the feeder port.
- When a CPE test group is running, the modification of a test which is part of the group shall not be allowed.
- When a CPE test group is running, the modification of CPE test group parameters shall not be allowed.
- When a CPE test group is running, the modification of a feeder port shall not be allowed.

Examples

```
-> test-oam group Testgroup1 port 1/2
```

Release History

Release 6.4.5; command was introduced.

Related Commands

test-oam group start	Starts the traffic test for the CPE test group on the configured port or the given port.
test-oam group stop	Stops the traffic test for the CPE test group on the configured port or the given port.
show test-oam group	Displays the configuration and status of the CPE test groups.

MIB Objects

```
alaTestOamGroupConfigTable
   alaTestOamConfigGroupId
   alaTestOamGroupConfigPort
```

test-oam group direction

Configures the test direction of the test-oam group.

test-oam group *string* **[direction unidirectional]**

Syntax Definitions

string	The name of an existing CPE test group.
direction	The direction of the CPE test group.

Defaults

parameter	default
direction	unidirectional

Platforms Supported

OmniSwitch 6400, 6850E, 6855-U24X, 9000E

Usage Guidelines

- When a CPE test group is running, the modification of a test which is part of the group shall not be allowed.
- When a CPE test group is running, the modification of CPE test group parameters shall not be allowed.
- When a CPE test group is running, the modification of a feeder port shall not be allowed.

Examples

```
-> test-oam group Testgroup1 direction unidirectional
```

Release History

Release 6.4.5; command was introduced.

Related Commands

test-oam group duration rate	Configures the duration and rate for the specified CPE test group.
show test-oam group	Displays the configuration and status of the CPE test groups.

MIB Objects

```
alaTestOamGroupConfigTable
   alaTestOamConfigGroupId
   alaTestOamGroupConfigDirection
```

test-oam group duration rate

Configures the duration and rate for the specified test-oam group. Use this command to configure these test parameters on the generator switch.

test-oam group *string* **[duration** *secs***] [rate** *rate***]**

Syntax Definitions

string	The name of an existing CPE test group.
secs	The duration of the test, in seconds. This is the amount of time the generator will actively transmit test packets to the remote (analyzer) switch. The valid time range is 5–3600 seconds.
rate	The rate, in kbps or mbps, at which test traffic is generated. The minimum value allowed is 64 kbps to line rate. The granularity of the transmit rate is 64 Kbps for 100 Mbps port and 2 Mbps for 1Gig ports.

Defaults

Parameter	Default
secs	5 secs
rate	64 kbps

Platforms Supported

OmniSwitch 6400, 6850E, 6855-U24X, 9000E

Usage Guidelines

- This command automatically overwrites any duration and rate parameter values previously configured for the specified CPE test group.
- The status of the CPE test group will change to “ended” when the test duration time expires.
- When a CPE test group is running, the modification of a test which is part of the group shall not be allowed.
- When a CPE test group is running, the modification of CPE test group parameters shall not be allowed.
- When a CPE test group is running, the modification of a feeder port shall not be allowed.

Examples

```
-> test-oam group Testgroup1 duration 10
-> test-oam group Testgroup1 rate 64k
-> test-oam group Testgroup1 duration 10 rate 64k
```

Release History

Release 6.4.5; command was introduced.

Related Commands

show test-oam group	Displays the configuration and status of the CPE test groups.

MIB Objects

```
alaTestOamGroupConfigTable
   alaTestOamConfigGroupId
   alaTestOamGroupConfigDuration
   alaTestOamGroupConfigGeneratorBandwidth
```

test-oam group start

Starts the traffic test for the test-oam group on the configured port or the given port.

test-oam group *string* **[port** *slot/port***] start**

Syntax Definitions

string	The name of an existing CPE test group.
slot/port	The port on which the CPE test group will generate traffic.
start	Enables the test.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855-U24X, 9000E

Usage Guidelines

- When a CPE test group is running, the modification of a test which is part of the group shall not be allowed.
- When a CPE test group is running, the modification of CPE test group parameters shall not be allowed.
- When a CPE test group is running, the modification of a feeder port shall not be allowed.

Examples

```
-> test-oam group Testgroup1 port 1/2 start
-> test-oam group Testgroup2 start
```

Release History

Release 6.4.5; command was introduced.

Related Commands

test-oam group stop	Stops the traffic test for the CPE test group on the configured port or the given port.
show test-oam group	Displays the configuration and status of the CPE test groups.

MIB Objects

```
alaTestOamGroupConfigTable
   alaTestOamConfigGroupId
   alaTestOamGroupConfigPort
   alaTestOamGroupConfigState
```

test-oam group stop

Stops the traffic test for the CPE test group on the configured port or the given port.

test-oam group *string* **stop**

Syntax Definitions

string	The name of an existing CPE test group.
stop	Disables the test.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855-U24X, 9000E

Usage Guidelines

- When a CPE test group is running, the modification of a test which is part of the group shall not be allowed.
- When a CPE test group is running, the modification of CPE test group parameters shall not be allowed.
- When a CPE test group is running, the modification of a feeder port shall not be allowed.

Examples

```
-> test-oam group Testgroup1 stop
-> test-oam group Testgroup2 stop
```

Release History

Release 6.4.5; command was introduced.

Related Commands

test-oam group start	Starts the traffic test for the CPE test group on the configured port or the given port.
show test-oam group	Displays the configuration and status of the CPE test groups.

MIB Objects

```
alaTestOamGroupConfigTable
   alaTestOamConfigGroupId
   alaTestOamGroupConfigPort
   alaTestOamGroupConfigState
```

clear test-oam group statistics

This clears the statistics of the CPE test group.

clear test-oam group *string* **statistics**

Syntax Definitions

string	The name of an existing CPE test group.
statistics	Clears the statistics for the give CPE test group.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855-U24X, 9000E

Usage Guidelines

- When a CPE test group is running, the modification of a test which is part of the group shall not be allowed.
- When a CPE test group is running, the modification of CPE test group parameters shall not be allowed.
- When a CPE test group is running, the modification of a feeder port shall not be allowed.

Examples

```
-> clear test-oam group Testgroup1 statistics (Clears the statistics for the
specified test-oam group)
-> clear test-oam group statistics (Clears the statistics for all the test-oam
groups)
```

Release History

Release 6.4.5; command was introduced.

Related Commands

show test-oam group statistics	Displays the statistics for all test-oam groups or for a specific CPE test group.
show test-oam group	Displays the configuration and status of the CPE test groups.

MIB Objects

```
alaTestOamGroupConfigTable
   alaTestOamConfigGroupId
   alaTestOamGroupConfigStatsClear
```

```
alaTestOamGlobalGroupClearStats
```

show test-oam group

Displays the configuration and status of the CPE test groups.

show test-oam group [tests | *string***]**

Syntax Definitions

tests	Displays information for all the CPE test groups**.**
string	The name of an existing CPE test group.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855-U24X, 9000E

Usage Guidelines

- Use the **tests** parameter to display information for all CPE test groups configured on the switch.
- Use the *string* parameter to display detailed information for a specific CPE test group.

Examples

```
-> show test-oam group tests
Total Test-Groups: 4
Feeder Port      : 1/2
Test-Group      Port  Duration     Rate    Nb of      Direction       Status
                      (secs)             Flows
-------------+-------+---------+---------+-------+---------------+-------------
TestGroup1      1/1     10        100M       8     unidirectional    not-started
TestGroup2      1/3     30         -         3     unidirectional          ended
TestGroup3      2/4     40         -         2     unidirectional        running
```

output definitions

Test-Groups	The CPE test group. Configured through the **test-oam group** command.
Port	The port on which the test is run.
Duration	The amount of time the test will run.
Rate	The rate at which packets are transmitted on the test port. Configured through the **test-oam group duration rate** command.
Nb of Flows	Number of test flows configured for the respective CPE test group.
Direction	The direction of the test traffic. Note that only unidirectional traffic tests are supported.
Status	The operational status of the test

```
-> show test-oam group TestGroup2

TEST Parameters for TestGroup2:
  Source Endpoint         : SW1,
  Destination Endpoint    : SW2,
  Test Group Description  : DEFAULT,
  Direction               : unidirectional,
  Role                    : generator,
  Tx Rate                 : -,
  Duration                : 20 (secs),
  Port                    : 1/2,
  State                   : stop,
  Status                  : stopped

Flow1:
      Test Name       : test_1,
      Vlan            : 1001
      Tx Rate         : 1M,
      Source MAC      : 00:00:00:00:01:01,
      Destination MAC : 00:00:00:00:01:02,
      Frame size      : 64,

Flow2:
      Test Name       : test_2,
      Vlan            : 1002
      Tx Rate         : 10M,
      Source MAC      : 00:00:00:00:02:01,
      Destination MAC : 00:00:00:00:02:02,
      Frame size      : 1518,

Flow3:
      Test Name       : test_3,
      Vlan            : 1003
      Tx Rate         : 15M,
      Source MAC      : 00:00:00:00:03:01,
      Destination MAC : 00:00:00:00:03:02,
      Frame size      : 1518,

Flow4:
      Test Name       : test_4,
      Vlan            : 1004
      Tx Rate         : 5M,
      Source MAC      : 00:00:00:00:04:01,
      Destination MAC : 00:00:00:00:04:02,
      Frame size      : 1518,
```

output definitions

Test-Groups	The CPE test group. Configured through the **test-oam group** command.
Port	The port on which the test is run.
Source Endpoint	The host name for the source (generator) switch. Configured through the **test-oam group src-endpoint dst-endpoint** command.
Destination Endpoint	The host name for the destination (analyzer) switch. Configured through the **test-oam group src-endpoint dst-endpoint** command.

output definitions

Source Mac	The source MAC address of the test frame. Configured through the **test-oam vlan test-frame** command.
Destination Mac	The destination MAC address of the test frame. Configured through the **test-oam vlan test-frame** command.
Duration	The amount of time the test will run.
Role	The role of the switch for this test (**generator** or **analyzer**). Configured through the **test-oam role** command
Rate	The rate at which packets are transmitted on the test port. Configured through the **test-oam group duration rate** command.
Frame Size	The size of the test frame. Configured through the **test-oam group duration rate** command.
Direction	The direction of the test traffic. Note that only unidirectional traffic tests are supported.
Status	The operational status of the test

Release History

Release 6.4.5; command was introduced.

Related Commands

show test-oam group statistics	Displays the statistics for all CPE test groups or for a specific CPE test group.

MIB Objects

```
alaTestOamGloabalFeederPort
alaTestOamGroupConfigTable
   alaTestOamConfigGroupId
   alaTestOamGroupConfigPort
   alaTestOamGroupConfigDuration
   alaTestOamGroupConfigGeneratorBandwidth
   alaTestOamGroupConfigFlowCount
   alaTestOamGroupConfigDirection
   alaTestOamGroupConfigStatus
alaTestOamGroupConfigTable
     alaTestOamConfigGroupId
     alaTestOamGroupConfigSourceEndpoint
     alaTestOamGroupConfigDestinationEndpoint
     alaTestOamConfigGroupDescription
     alaTestOamGroupConfigDirection
     alaTestOamGroupConfigRole
     alaTestOamGroupConfigGeneratorBandwidth
     alaTestOamGroupConfigDuration
     alaTestOamGroupConfigPort
     alaTestOamGroupConfigState
     alaTestOamGroupConfigStatus

   alaTestOamGroupFlowConfigTable
     alaTestOamConfigTestId
```

```
alaTestOamGroupFlowVlan
 alaTestOamGroupFlowGeneratorBandwidth
 alaTestOamGroupFlowFrameSrcMacAddress
 alaTestOamGroupFlowFrameDstMacAddress
 alaTestOamGroupFlowGeneratorPacketSize
```

show test-oam group statistics

Displays the statistics for all CPE test groups or for a specific CPE test group. Use this command on both the generator and analyzer switch to determine test results.

show test-oam group [*string***] statistics**

Syntax Definitions

string	The name of an existing CPE test group.

Defaults

By default, statistics are displayed for all CPE test groups.

Platforms Supported

OmniSwitch 6400, 6850E, 6855-U24X, 9000E

Usage Guidelines

- Use the *string* parameter with this command to display statistics for a specific CPE test group.
- The statistics displayed depend on the role the switch is performing for the test (generator or analyzer). For example, the analyzer switch may not show any packet count in the **TX** fields because it is the receiving switch.

Examples

```
-> show test-oam group TestGroup4 statistics
Test-Group         Flow          TX-Ingress        TX-Egress    RX-Ingress
-------------+--------------+------------------+---------------+------------
TestGroup4        flow1              19017            19017     0
TestGroup4        flow2              19017            19017     0

-> show test-oam group statistics
Test-Group        Flow           TX-Ingress       TX-Egress    RX-Ingress
-------------+-------------+------------------+---------------+-----------
TestGroup1        flow1              19017           19017      0
TestGroup1        flow2              19017           19017      0
TestGroup1        flow3              19017           19017      0
TestGroup1        flow4              19017           19017      0
TestGroup1        flow5              19017           19017      0
TestGroup1        flow6              19017           19017      0
TestGroup1        flow7              19017           19017      0
TestGroup1        flow8              19017           19017      0
TestGroup2        flow1              19017           19017      0
TestGroup2        flow2              19017           19017      0
TestGroup2        flow3              19017           19017      0
TestGroup2        flow4              19017           19017      0
TestGroup3        flow1              19017           19017      0
TestGroup4        flow8              19017           19017      0
```

output definitions

Test-Group	The CPE test group.
TX-Ingress	The number of ingress test packets generated on the ingress UNI.
TX-Egress	The number of egress test packets transmitted on the egress NNI.
RX-Ingress	The number of test packets received on the ingress NNI. This value is relevant on the receiving (analyzer) switch for the specific test.

Release History

Release 6.4.5; command was introduced.

Related Commands

show test-oam group	Displays the configuration and status of the CPE test groups.
clear test-oam group statistics	Clears the statistics of the CPE test group.

MIB Objects

```
alaTestOamGroupConfigTable
   alaTestOamConfigGroupId
   alaTestOamConfigTestId
   alaTestOamGroupFlowTxIngressCounter
   alaTestOamGroupFlowTxEgressCounter
   alaTestOamGroupFlowRxIngressCounter
```

12 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 vpls permanent sap
mac-address-table vpls permanent mesh-sdp
mac-address-table static-multicast
mac-address-table aging-time
source-learning chassis-distributed
source-learning
show mac-address-table
show mac-address-table all
show mac-address-table vpls
show mac-address-table vpls sap
show mac-address-table vpls mesh-sdp
show mac-address-table static-multicast
show mac-address-table count
show mac-address-table vpls count
show mac-address-table all count
show mac-address-table aging-time
show source-learning
show source-learning chassis-distributed

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] *mac_address* **{***slot/port* | **linkagg** *link_agg***}** *vid* **[bridging | filtering]**

no mac-address-table [permanent | 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.
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 7, "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	permanent
bridging | **filtering**	bridging

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a MAC address from the Source Learning MAC Address Table.
- 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.
- 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 12-10) 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
-> no mac-address-table
-> no mac-address-table 5/1 755
-> no mac-address-table permanent
```

Release History

Release 6.1; 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 vpls permanent sap

Configures a static MAC address and associates that address with the specified Service Access Point (SAP) ID for the specified Virtual Private LAN Service (VPLS).

mac-address-table vpls *service-id* **permanent** *mac-address* **sap {***sap-id* **| linkagg** *sap-id***}**

no mac-address-table vpls *service-id* **permanent** *mac-address*

no mac-address-table vpls *service-id* **learned [sap** *sap-id* **| linkagg** *sap-id***]** *mac-address*

Syntax Definitions

service-id	An existing VPLS ID number.
mac-address	A 48-bit MAC address (*aa:bb:cc:dd:ee:ff*). Valid addresses are any non-broadcast, non-multicast MAC, and non-IEEE reserved addresses.
sap-id	The access slot and port number or link aggregate ID (0–31) and encapsulation value for an existing SAP (e.g., 1/10:0, 1/12:all, 20:150, 10:all).
learned	Specifies that the MAC address is a dynamically learned address. This option is only available with the **no** form of this command.

Defaults

N/A

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to remove the configured static MAC from the source learning FDB.
- The specified VPLS ID and SAP ID must already exist in the VPLS configuration for the switch. See the “VPLS Commands” chapter in this guide for information about how to configure a VPLS and SAP.
- A SAP ID is comprised of an access (customer-facing) port or link aggregate and an encapsulation value that is used to identify the type of customer traffic to map to the associated service.
- Static MACs associated with a SAP are classified as local MACs. A local MAC is used by the associated VPLS so that MAC addresses are not learned on the edge device.
- A MAC address can participate in only one static MAC address entry (local or remote) for a specific VPLS.
- Static MAC addresses configured on one edge device are not propagated to other edge devices associated with the same VPLS instance. Each edge device has an independent forwarding database for the associated VPLS.

Examples

```
-> mac-address-table vpls 10 permanent 00:00:da:3e:44:01 sap 1/2:100
-> mac-address-table vpls 10 permanent 00:00:da:3e:44:01 sap linkagg 10:100
```

```
-> no mac-address-table vpls 10 00:00:da:3e:44:01
-> no mac-address-table vpls 10 permanent 00:00:da:3e:44:01
-> no mac-address-table vpls 20 learned 00:2a:3e:11:22:10
-> no mac-address-table vpls 30 learned 1/10:all 00:2a:3e:11:22:09
-> no mac-address-table vpls 40 learned linkagg 10:all 00:2a:3e:11:22:08
```

Release History

Release 6.4.2; command was introduced.

Related Commands

show mac-address-table all	Displays Source Learning MAC Address Table contents for the VLAN and VPLS domain.
show mac-address-table vpls sap	Displays the Source Learning MAC Address Table contents for the specified VPLS Service Access Point binding.

MIB Objects

```
slMacAddressGlobalTable
   slMacDomain
   slLocalType
   slOriginId
   slServiceId
   slMacAddressGbl
```

mac-address-table vpls permanent mesh-sdp

Configures a static MAC address and associates that address with the specified Service Distribution Point (SDP) ID binding with the specified Virtual Private LAN Service (VPLS).

mac-address-table vpls *service-id* **permanent** *mac-address* **mesh-sdp** *sdp-id***[***:vc-id***]**

no mac-address-table vpls *service-id* **permanent** *mac-address*

no mac-address-table vpls *service-id* **learned [mesh-sdp** *sdp-id***[***:vc-id***]]** *mac-address*

Syntax Definitions

service-id	An existing VPLS ID number.
mac-address	A 48-bit MAC address (*aa:bb:cc:dd:ee:ff*). Valid addresses are any non-broadcast, non-multicast MAC, and non-IEEE reserved addresses.
sdp-id	An existing SDP ID number that is bound to the specified service ID number.
vc-id	*Optional*. The VC ID number appended to the specified SDP ID number.
learned	Specifies that the MAC address is a dynamically learned address. This option is only available with the **no** form of this command.

Defaults

parameter	default
vc-id	*service-id* value

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to remove the configured static MAC from the source learning FDB.
- The specified VPLS ID and SDP ID must already exist in the VPLS configuration for the switch. See the “VPLS Commands” chapter in this guide for information about how to configure a VPLS and SDP.
- Static MACs associated with SDPs are classified as remote MACs. A remote MAC is used by the associated VPLS so that MAC addresses are not learned on the edge device.
- A MAC address can participate in only one static MAC address entry (local or remote) for a specific VPLS.
- Static MAC addresses configured on one edge device are not propagated to other edge devices associated with the same VPLS instance. Each edge device has an independent forwarding database for the associated VPLS.

Examples

```
-> mac-address-table vpls 10 permanent 00:00:da:3e:44:01 mesh-sdp 10
-> no mac-address-table vpls 10 learned 00:00:da:3e:44:01
-> no mac-address-table vpls 20 learned mesh-sdp 20 00:2a:d5:11:2a:31
```

Release History

Release 6.4.2; command was introduced.

Related Commands

show mac-address-table	Displays Source Learning MAC Address Table information.
show mac-address-table vpls mesh-sdp	Displays Source Learning MAC Address Table information for the specified VPLS mesh-SDP binding.

MIB Objects

```
slMacAddressGlobalTable
   slMacDomain
   slLocalType
   slOriginId
   slServiceId
   slMacAddressGbl
```

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 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 7, "Link Aggregation Commands."
vid	VLAN ID number (1–4094).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this 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 a MAC address is considered a multicast MAC address if the least significant bit of the most significant octet of the address is enabled. For example, MAC addresses with a prefix of 01, 03, 05, 13, etc., are multicast MAC addresses.
- If a multicast prefix value 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. Also note that multicast addresses within the following ranges are not supported:

  01:00:5E:00:00:00 to 01:00:5E:7F:FF:FF
  01:80:C2:XX.XX.XX
  33:33:XX:XX:XX:XX

- 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.
- In addition to configuring the same static multicast address for multiple ports within a given VLAN, it is also possible to use the same multicast address across multiple VLANs.
- 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 the **configuration snapshot** or **write memory** command is entered after a static multicast MAC address is configured, the resulting ASCII file or **boot.cfg** file will include the following additional syntax for the **mac-address-table static-multicast** command:

  group *num*

  This syntax indicates the number of the multicast group that the switch has assigned to the multicast MAC address for the given VLAN association. Each multicast address – VLAN association is treated as a unique instance and assigned a group number specific to that instance. Up to 1022 such instances are supported per switch.
- Note that if the port assigned to a multicast MAC address is down or administratively disabled when the **configuration snapshot** or **write memory** command is used, the multicast MAC address is not saved to the resulting ASCII file or **boot.cfg** file.

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 6.1.2; 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*

no mac-address-table aging-time

Syntax Definitions

seconds	Aging time value (in seconds). Do not use commas in value. The range is 60—1000000.

Defaults

By default, the aging time is set to 300 seconds.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to set the aging-time back to the default value of 300 seconds.
- The aging time value is a global value that applies to all VLANs. Configuring this value on a per VLAN basis is not supported on this platform.
- Note that an inactive MAC address may take up to twice as long as the aging time value specified to age out of the MAC address table. For example, if an aging time of 60 seconds is specified, the MAC will age out any time between 60 and 120 seconds of inactivity.
- If the **timeout** parameter is not specified when using the **mac-address-table** command (see page 12-2) to configure a static MAC address, then the aging time value is not applied to the static MAC address.

Examples

```
-> mac-address-table aging-time 1200
-> no mac-address-table aging-time
```

Release History

Release 6.1; command was introduced.
Release 6.1.1; **vlan** parameter not supported.

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
```

source-learning

Configures the status of source MAC address learning on a single port, a range of ports, or on a link aggregate of ports.

source-learning {port *slot/port1***[-***port2***] | linkagg** *linkagg_num***} {enable | disable}**

Syntax Definitions

slot/port1	The slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
-port2	The last port number in a range of ports that you want to configure on the same slot (e.g, 3/1-4 specifies ports 1, 2, 3, and 4 on slot 3).
linkagg_num	Specifies the link aggregate port ID.
enable	Enables source learning.
disable	Disables source learning.

Defaults

By default, source learning is enabled on all ports.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Configuring source learning is not supported on mobile ports, Learned Port Security ports, individual ports which are members of a link aggregate, or Access Guardian (802.1x) ports.
- When port-based source learning is configured for a link aggregate ID, it affects all the ports that are members of the link aggregate.
- When source-learning is disabled on a port or link aggregate, all dynamically learned MAC addresses are removed from the MAC address table.
- Static MAC addresses associated with a port or link aggregate are *not* cleared when source learning is disabled. Also, new static MAC address configurations are allowed on ports or link aggregates even when source learning is disabled on them.
- Disabling source learning on a port or link aggregate is useful on a ring configuration where switch A does not have to learn MAC addresses from switch B or for a Transparent LAN Service, where service provider does not require the MAC addresses of the Customer network.

Examples

```
-> source-learning port 1/2 disable
-> source-learning port 1/3-9 disable
-> source-learning linkagg 10 disable
```

Release History

Release 6.4.2; command added.

Related Commands

show source-learning	Displays Source Learning status of each port or linkagg ports on a switch.

Related MIB Objects

```
slMacAddressTable
slMacLearningControlTable
  slMacLearningControlEntry
  slMacLearningControlStatus
```

source-learning chassis-distributed

Enables or disables the distributed MAC source learning mode for the chassis. Enabling this mode increases the number of learned MAC addresses supported to 16K per module and up to 64K per chassis.

source-learning chassis-distributed {enable | disable}

Syntax Definitions

enable	Enables distributed MAC source learning mode.
disable	Disables distributed MAC source learning mode.

Defaults

By default distributed MAC source learning mode is disabled for the chassis.

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

- After the distributed MAC mode is either enabled or disabled using this command, immediately save the switch configuration using the **write memory** command and then reboot the switch.
- Distributed MAC source learning is not supported on an OmniSwitch stackable switches.
- When the distributed MAC source learning mode is disabled (the default), the maximum number of learned MAC addresses allowed per OmniSwitch chassis-based switch is 16K.

Examples

```
-> source-learning chassis-distributed enable
-> source-learning chassis-distributed disable
```

Release History

Release 6.1.3; command was introduced.

Related Commands

show source-learning chassis-distributed	Displays the current status of the distributed MAC source learning mode.

MIB Objects

```
slMacAddressTable
   slDistributedMacMode
```

show mac-address-table

Displays Source Learning MAC Address Table information.

show mac-address-table [permanent | learned | quarantined] [*mac_address***] [slot** *slot* | *slot/port***] [link-agg** *link_agg***] [***vid* | *vid1-vid2***]**

Syntax Definitions

permanent	Display static MAC addresses with a permanent status.
learned	Display dynamically learned MAC addresses.
quarantined	Display MAC addresses quarantined by the Quarantine Manager and Remediation (QMR) application.
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 7, "Link Aggregation Commands."
vid	A single VLAN ID number (1–4094).
vid1-vid2	A range of VLAN IDs that you want to configure (e.g. 10-12 specifies VLANs 10, 11, and 12).

Defaults

By default, information is displayed for all MAC addresses contained in the table.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Note that only one VLAN entry—a single VLAN ID or a range of VLAN IDs— is allowed with this command. Multiple entries are not accepted.
- If a static MAC address is configured on a port link that is down or disabled, an asterisk appears to the right 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

 Domain  Vlan/SrvcId   Mac Address       Type      Protocol  Operation  Interface
--------+-----------+------------------+----------+---------+----------+-----------
   VLAN   1          00:00:00:00:00:01   learned    0800      bridging     8/1
   VLAN   1          00:d0:95:6a:73:9a   learned    aaaa0003  bridging   10/23

Total number of Valid MAC addresses above = 2


-> show mac-address-table 10-15
Legend: Mac Address: * = address not valid

 Domain  Vlan/SrvcId   Mac Address       Type       Protocol  Operation  Interface
--------+-----------+------------------+-----------+---------+----------+----------
   VLAN   10         00:00:00:00:00:01  learned     0800       bridging    1/2
   VLAN   10         00:d0:95:6a:73:9a  learned     aaaa0003   bridging    1/2
   VLAN   11         00:d0:95:a3:e0:0d  learned       ---      bridging    1/3
   VLAN   11         00:d0:95:a3:e5:09  learned       ---      bridging    1/3
   VLAN   11         00:d0:95:a3:e7:75  learned       ---      bridging    1/4
   VLAN   12         00:d0:95:a3:ed:f7  learned       ---      bridging    2/1
   VLAN   12         00:d0:95:a8:2a:b6  learned       ---      bridging    2/1
   VLAN   12         00:d0:95:ad:e3:cc  learned       ---      bridging    2/1
   VLAN   13         00:d0:95:ae:3b:f6  learned       ---      bridging    2/8
   VLAN   13         00:d0:95:b2:3d:fa  learned       ---      bridging    2/8
   VLAN   14         00:00:0a:00:00:00  quarantined   ---      filtered    5/1
   VLAN   14         00:00:0a:00:00:01  quarantined   ---      filtered    5/1
   VLAN   14         00:00:0a:00:00:02  quarantined   ---      filtered    5/1
   VLAN   14         00:00:0a:00:00:03  quarantined   ---      filtered    5/1

Total number of Valid MAC addresses above = 14

-> show mac-address-table quarantined
Legend: Mac Address: * = address not valid

 Domain  Vlan/SrvcId   Mac Address       Type       Protocol  Operation  Interface
--------+-----------+------------------+-----------+---------+----------+----------
   VLAN   14         00:00:0a:00:00:00  quarantined    ---      filtered     5/1
   VLAN   14         00:00:0a:00:00:01  quarantined    ---      filtered     5/1
   VLAN   14         00:00:0a:00:00:02  quarantined    ---      filtered     5/1
   VLAN   14         00:00:0a:00:00:03  quarantined    ---      filtered     5/1

Total number of Valid MAC addresses above = 14
```

output definitions

Domain	The domain to which the MAC address belongs (**VLAN** or **VPLS**).
VLAN/SrvcId	Vlan ID number or VPLS ID number associated with the MAC address.
Mac Address	MAC address that is currently learned or statically assigned.
Type	MAC address management status: **learned, permanent, or quarantined**. Configured through the **mac-address-table** command.
Protocol	Protocol type for the MAC address entry. Note that if the hardware source learning mode is active for the port, this field is blank.

output definitions

Operation	The disposition of the MAC address: **bridging** (default) or **filtering**. Configured through the **mac-address-table** command.
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 6.1; command was introduced.
Release 6.1.3; *vid* parameter modified to support a range of VLAN IDs.
Release 6.3.1; **quarantined** type added.
Release 6.4.2; **Domain** field added and **SrvcId** added to **Vlan** field.

Related Commands

show mac-address-table all	Displays MAC addresses associated with both VLANs and Virtual Private LAN Service (VPLS) services.
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 all

Displays MAC addresses associated with both VLANs and Virtual Private LAN Service (VPLS) services.

show mac-address-table all [permanent | learned]

Syntax Definitions

permanent	Displays static MAC addresses with a permanent status.
learned	Displays dynamically learned MAC addresses.

Defaults

By default, information is displayed for all MAC addresses contained in the table.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

If a static MAC address is configured on a port link that is down or disabled, an asterisk appears to the right 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

```
SW-D-> show mac-address-table all

Legend: Mac Address: * = address not valid

 Domain  Vlan/SrvcId   Mac Address       Type     Protocol  Operation  Interface
--------+-----------+-----------------+----------+--------+----------+-------------
   VLAN    13        00:d0:95:e9:cf:86  learned     ---     bridging    16/1
   VLAN    13        00:e0:b1:9c:8a:3c  learned     ---     bridging    16/1
   VLAN    15        00:e0:b1:87:8d:68  learned     ---     bridging    16/12
   VLAN    15        00:e0:b1:9c:87:2f  learned     ---     bridging    16/12
   VPLS    1000      00:01:bd:01:01:01  learned     ---    servicing   sdp:222:1000
   VPLS    1000      00:01:bd:01:01:02  learned     ---    servicing   sdp:222:1000
   VPLS    1000      00:01:bd:01:01:03  learned     ---    servicing   sdp:222:1000
   VPLS    1000      00:01:bd:01:01:04  learned     ---    servicing   sdp:222:1000
   VPLS    1000      00:01:bd:01:01:05  learned     ---    servicing   sdp:222:1000

Total number of Valid MAC addresses above = 14
```

output definitions

Domain	The domain to which the MAC address belongs (**VLAN** or **VPLS**).
VLAN/SrvcId	Vlan ID number or VPLS ID number associated with the MAC address.
Mac Address	MAC address that is currently learned or statically assigned.

Type	MAC address management status: **learned, permanent, or quarantined**.
Protocol	Protocol type for the MAC address entry. Note that if the hardware source learning mode is active for the port, this field is blank.
Operation	The disposition of the MAC address: **bridging** (default), **filtering**, or **servicing**.
Interface	The slot/port number that is associated with the MAC address. If the interface is a link aggregate ID, zero is displayed as the slot number (e.g., 0/29). If the MAC is associated with a VPLS service, this field contains the mesh-SDP or SAP binding information.

Release History

Release 6.4.2; command was introduced.

Related Commands

mac-address-table	Configures a static destination Unicast MAC address for a VLAN bridge.
mac-address-table vpls permanent sap	Configures a static MAC address for a VPLS SAP.
mac-address-table vpls permanent mesh-sdp	Configures a static MAC address for a VPLS mesh-SDP binding.

MIB Objects

```
slMacAddressGlobalTable
   slMacAddressGbl
   slMacAddressGblmanagement
   slMacAddressGblDisposition
```

show mac-address-table vpls

Displays Source Learning MAC Address Table contents for VPLS services.

show mac-address-table vpls [*service-id***] [permanent | learned] [***mac-address***]**

Syntax Definitions

service-id	An existing VPLS ID number.
permanent	Display static MAC addresses.
learned	Display dynamically learned MAC addresses.
mac-address	A 48-bit MAC address (*aa:bb:cc:dd:ee:ff*). Valid addresses are any non-broadcast, non-multicast MAC, and non-IEEE reserved addresses.

Defaults

By default, all MAC addresses for all services are displayed.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

Use the optional parameters with this command to display information for specific services and MAC address types.

Example

```
-> show mac-address-table vpls 1002 00:01:db:07:03:02
Legend: Mac Address: * = address not valid

Domain Vlan/SrvcId   Mac Address      Type    Protocol   Operation  Interface
------+------------+-----------------+--------+--------+----------+--------------
VPLS   1002         00:01:db:07:03:02 learned   ---      servicing  sap:0/16:1006


-> show mac-address-table vpls 1002 permanent
Legend: Mac Address: * = address not valid

Domain  Vlan/SrvcId   Mac Address      Type    Protocol Operation   Interface
-------+-----------+-----------------+---------+------+----------+--------------
VPLS    1002        00:00:00:00:00:05 permanent  ---    servicing  sap:0/16:1005

Total number of Valid MAC addresses above = 1

-> show mac-address-table vpls 1002 learned
Legend: Mac Address: * = address not valid

Domain  Vlan/SrvcId   Mac Address      Type    Protocol Operation   Interface
-------+-----------+-----------------+---------+------+----------+--------------
VPLS    1002        00:01:bd:01:02:01 learned    ---    servicing  sdp:222:1002
```

```
VPLS   1002       00:01:bd:01:02:02   learned   ---    servicing  sdp:222:1002
VPLS   1002       00:01:bd:01:02:03   learned   ---    servicing  sdp:222:1002
VPLS   1002       00:01:bd:01:02:04   learned   ---    servicing  sdp:222:1002
VPLS   1002       00:01:bd:01:02:05   learned   ---    servicing  sdp:222:1002
VPLS   1002       00:01:bd:01:02:06   learned   ---    servicing  sdp:222:1002
VPLS   1002       00:01:db:07:03:01   learned   ---    servicing  sap:0/16:1005
VPLS   1002       00:01:db:07:03:02   learned   ---    servicing  sap:0/16:1006
VPLS   1002       00:01:db:07:03:03   learned   ---    servicing  sap:0/16:1007
VPLS   1002       00:01:db:07:03:04   learned   ---    servicing  sap:0/16:1008
VPLS   1002       00:01:db:07:03:05   learned   ---    servicing  sap:0/16:1009
VPLS   1002       00:01:db:07:03:06   learned   ---    servicing  sap:0/16:1010
VPLS   1002        00:d0:95:e5:30:f2  learned    ---    servicing  sap:0/16:1005

Total number of Valid MAC addresses above = 13
```

output definitions

Domain	The domain to which the MAC address belongs: **VLAN** or **VPLS**.
VLAN/SrvcId	VLAN ID number or VPLS ID number associated with the MAC address.
Mac Address	MAC address that is currently learned or statically assigned.
Type	MAC address management status: **learned** or **permanent**.
Protocol	Protocol type for the MAC address entry. Note that if the hardware source learning mode is active for the port, this field is blank.
Operation	The disposition of the MAC address: **bridging** (default), **filtering**, or **servicing**.
Interface	The VPLS mesh-SDP or SAP binding information.

Release History

Release 6.4.2; command introduced

Related Commands

mac-address-table vpls permanent sap	Configures a static MAC address for a VPLS Service Access Point binding.
mac-address-table vpls permanent mesh-sdp	Configures a static MAC address for a VPLS mesh-Service Distribution Point binding.

Related MIB Objects

```
slMacAddressGlobalTable
     slServiceId
     slMacAddressGbl
   slMacAddressGblmanagement
```

show mac-address-table vpls sap

Displays Source Learning MAC Address Table information for the specified VPLS Service Access Point (SAP) binding.

show mac-address-table vpls *service-id* **sap {***sap-id* **| linkagg** *sap-id***}** *mac-address*

Syntax Definitions

service-id	An existing VPLS ID number.
sap-id	The access slot and port number or link aggregate ID (0–31) and encapsulation value for an existing SAP (e.g., 1/10:0, 1/12:all, 20:150, 10:all).
mac-address	A 48-bit MAC address (*aa:bb:cc:dd:ee:ff*). Valid addresses are any non-broadcast, non-multicast MAC, and non-IEEE reserved addresses.

Defaults

N/A

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- The specified VPLS ID and SAP ID must already exist in the VPLS configuration for the switch. See the “VPLS Commands” chapter in this guide for information about how to configure a VPLS and SAP.
- A SAP ID is comprised of an access (customer-facing) port or link aggregate and an encapsulation value that is used to identify the type of customer traffic to map to the associated service.

Example

```
-> show mac-address-table vpls 1002 sap linkagg 16:1006
Legend: Mac Address: * = address not valid

Domain Vlan/SrvcId    Mac Address      Type  Protocol Operation Interface
-----+-----------+-----------------+--------+-------+---------+------------
VPLS   1002      00:01:db:07:03:02  learned  ---    servicing  sap:0/16:1006

Total number of Valid MAC addresses above = 1
```

output definitions

Domain	The domain to which the MAC address belongs: **VLAN** or **VPLS**.
VLAN/SrvcId	The VPLS ID number associated with the MAC address.
Mac Address	MAC address that is currently learned or statically assigned.
Type	MAC address management status: **learned** or **permanent**.
Protocol	Protocol type for the MAC address entry. Note that if the hardware source learning mode is active for the port, this field is blank.

output definitions

Operation	The disposition of the MAC address: **bridging** (default), **filtering**, or **servicing**.
Interface	The VPLS SAP binding to which the MAC address is associated.

Release History

Release 6.4.2; command introduced

Related Commands

mac-address-table vpls permanent sap	Configures a static MAC address for a VPLS SAP binding.
show source-learning chassis-distributed	Displays the Source Learning MAC Address Table contents for VPLS service MAC addresses.

Related MIB Objects

```
slMacAddressGlobalTable
   slServiceId
   slServiceId
   slMacAddressGbl
   slMacAddressGblmanagement
   slOriginId
   slSubId
```

show mac-address-table vpls mesh-sdp

Displays Source Learning MAC Address Table information for the specified VPLS mesh-SDP binding.

show mac-address-table vpls *service-id* **mesh-sdp** *sdp-id***[***:vc-id***]** *mac-address*

Syntax Definitions

service-id	An existing VPLS ID number.
sdp-id	An existing SDP ID number that is bound to the specified service ID number.
vc-id	*Optional*. The VC ID number appended to the specified SDP ID number.
mac-address	A 48-bit MAC address (*aa:bb:cc:dd:ee:ff*). Valid addresses are any non-broadcast, non-multicast MAC, and non-IEEE reserved addresses.

Defaults

parameter	default
vc-id	*service-id* value

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

The specified VPLS ID and SDP ID must already exist in the VPLS configuration for the switch. See the "VPLS Commands" chapter in this guide for information about how to configure a VPLS and SAP.

Example

```
SW-D-> show mac-address-table vpls 1002 mesh-sdp 222
Legend: Mac Address: * = address not valid

Domain Vlan/SrvcId  Mac Address       Type    Protocol  Operation  Interface
------+-----------+-----------------+--------+---------+----------+-------------
VPLS    1002       00:01:bd:01:02:01 learned   ---      servicing  sdp:222:1002
VPLS    1002       00:01:bd:01:02:02 learned   ---      servicing  sdp:222:1002
VPLS    1002       00:01:bd:01:02:03 learned   ---      servicing  sdp:222:1002
VPLS    1002       00:01:bd:01:02:04 learned   ---      servicing  sdp:222:1002
VPLS    1002       00:01:bd:01:02:05 learned   ---      servicing  sdp:222:1002
VPLS    1002       00:01:bd:01:02:06 learned   ---      servicing  sdp:222:1002

Total number of Valid MAC addresses above = 6
```

output definitions

Domain	The domain to which the MAC address belongs: **VLAN** or **VPLS**.
VLAN/SrvcId	The VPLS ID number associated with the MAC address.

output definitions (continued)

Mac Address	MAC address that is currently learned or statically assigned.
Type	MAC address management status: **learned** or **permanent**.
Protocol	Protocol type for the MAC address entry. Note that if the hardware source learning mode is active for the port, this field is blank.
Operation	The disposition of the MAC address: **bridging** (default), **filtering**, or **servicing**.
Interface	The VPLS mesh-SDP binding to which the MAC address is associated.

Release History

Release 6.4.2; command introduced

Related Commands

mac-address-table vpls permanent mesh-sdp	Configures a static MAC for a VPLS mesh-SDP binding.
show source-learning chassis-distributed	Displays Source Learning MAC Address Table information for VPLS service MAC addresses.

Related 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* | *vid1-vid2***]**

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 12, "Link Aggregation Commands."
vid	VLAN ID number (1–4094).
vid1-vid2	The last VLAN ID number in a range of VLANs that you want to configure (e.g. 10-12 specifies VLANs 10, 11, and 12).

Defaults

By default, information is displayed for all static multicast MAC addresses contained in the MAC address table.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Note that only one VLAN entry—a single VLAN ID or a range of VLAN IDs— is allowed with this command. Multiple entries are not accepted.
- 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 MAC address is invalid. 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

In the example below, the static multicast address 01:00:00:00:00:01 is associated with port 1/1, which is down. As a result, this address does not appear in the **show mac-address-table static-multicast** display but is included in the **show mac-address-table** display with an asterisk.

```
-> show mac-address-table static-multicast
Legend: Mac Address: * = address not valid

Domain  Vlan/SrvcId   Mac Address      Type        Protocol   Operation  Interface
-------+-----------+-----------------+-----------+----------+----------+----------
  VLAN   1          01:00:00:00:00:02 static-mcast  ---       bridging      2/6

Total number of Valid MAC addresses above = 1

-> show mac-address-table
Legend: Mac Address: * = address not valid

Domain  Vlan/SrvcId   Mac Address      Type        Protocol   Operation  Interface
-------+-----------+-----------------+-----------+----------+----------+----------
* VLAN   1          01:00:00:00:00:01 static-mcast  0         bridging      1/1
  VLAN   24         00:d0:95:e4:cf:5a learned       ---       bridging      1/2
  VLAN   24         00:d0:95:e5:af:52 learned       ---       bridging      1/2
  VLAN   24         00:e0:4c:bc:ce:a1 learned       ---       bridging      1/2
  VLAN   1          01:00:00:00:00:02 static-mcast  ---       bridging      2/6
  VLAN   1          00:d0:95:e2:77:38 learned       ---       bridging      3/19

Total number of Valid MAC addresses above = 5
```

output definitions

Domain	The domain to which the MAC address belongs: **VLAN** or **VPLS**.
VLAN/SrvcId	The VPLS ID number associated with the MAC 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 (**static-mcast**) address. 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 6.1.2; command was introduced.
Release 6.1.3; *vid* parameter modified to support a range of VLAN IDs.

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

```
slMacAddressTable
   slMacAddress
   slMacAddressManagement
   slMacAddressDisposition
   slMacAddressProtocol
```

show mac-address-table count

Displays Source Learning MAC Address Table statistics for VLAN MAC addresses.

show mac-address-table count [*mac_address***] [slot** *slot* | *slot/port***] [linkagg** *link_agg***] [***vid* | *vid1-vid2***]**

Syntax Definitions

mac_address	A 48-bit MAC address (*aa:bb:cc:dd:ee:ff*). Valid addresses are any non-broadcast, non-multicast MAC, and non-IEEE reserved addresses.
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 7, "Link Aggregation Commands."
vid	VLAN ID number (1–4094).

Defaults

By default, the count statistics are displayed for all MAC addresses contained in the MAC address table.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- To display statistics for all ports on one slot, specify only the slot number for the **slot** parameter value.
- Note that only one VLAN entry—a single VLAN ID or a range of VLAN IDs— is allowed with this command. Multiple entries are not accepted.

Examples

```
-> show mac-address-table count
Mac Address Table count:
  Permanent Address Count             = 1
  DeleteOnReset Address Count         = 0
  DeleteOnTimeout Address Count       = 0
  Dynamic Learned Address Count       = 6
  Static Multicast Address Count      = 0,
  Total MAC Address In Use            = 7

-> show mac-address-table count 10-20
Mac Address Table count:
  Permanent Address Count             = 0
  DeleteOnReset Address Count         = 0
  DeleteOnTimeout Address Count       = 0
  Dynamic Learned Address Count       = 28
  Static Multicast Address Count      = 0,
  Total MAC Address In Use            = 28
```

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).
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).
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 6.1; command was introduced.
Release 6.1.3; *vid* parameter modified to support a range of VLAN IDs.

Related Commands

show mac-address-table	Displays Source Learning MAC Address Table information.
show mac-address-table aging-time	Displays the current aging time value for the Source Learning MAC Address Table.
show mac-address-table all count	Displays the Source Learning MAC Address Table statistics for both VLAN and VPLS MAC addresses.
show mac-address-table vpls count	Displays the Source Learning MAC Address Table statistics for VPLS service MAC addresses.

show mac-address-table vpls count

Displays Source Learning MAC address table statistics for VPLS service MAC addresses.

show mac-address-table vpls *service-id* **count] [***mac-address***]**

Syntax Definitions

service-id	An existing VPLS ID number.
mac-address	A 48-bit MAC address (*aa:bb:cc:dd:ee:ff*). Valid addresses are any non-broadcast, non-multicast MAC, and non-IEEE reserved addresses.

Defaults

By default, all VPLS addresses are counted.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

Enter a MAC address to display statistics for a specific VPLS service MAC address.

Example

```
SW-D-> show mac-address-table vpls 1002 count
Mac Address Table Count:
  Permanent VPLS Address Count       = 1,
  Dynamic Learned VPLS Address Count = 13,
  Total MAC Address In Use           = 14
```

output definitions

Permanent VPLS Address Count	The number of static VPLS MAC addresses configured on the switch with a **permanent** management status (MAC address is never aged out).
Dynamic Learned VPLS Address Count	The number of VPLS MAC Addresses learned by the switch. These addresses are not user-configured permanent addresses.
Total MAC Address In Use	The total number of MAC addresses (learned and static) that are known to the switch.

Release History

Release 6.4.2; command introduced

Related Commands

show mac-address-table all count	Displays Source Learning MAC Address Table statistics for both VLAN and VPLS service MAC addresses.
show mac-address-table count	Displays Source Learning MAC Address Table statistics for VLAN MAC addresses.

Related MIB Objects

```
slMacAddressGlobalTable
     slServiceId
     slMacAddressGbl
   slMacAddressGblmanagement
```

show mac-address-table all count

Displays Source Learning MAC Address Table statistics for both VLAN and VPLS MAC addresses.

show mac-address-table all count

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- This command displays dynamically learned and permanent MAC address for both VLANs and VPLS services. For more information on VPLS, see the “VPLS Commands“ chapter in this guide.
- Use the **show mac-address-table count** command to display statistics for VLAN MAC addresses only.

Examples

```
-> show mac-address-table all count
Mac Address Table Count:
  Permanent Address Count            = 0,
  DeleteOnReset Address Count        = 0,
  DeleteOnTimeout Address Count      = 0,
  Dynamic Learned Address Count      = 5,
  Static Multicast Address Count     = 0,
  Permanent VPLS Address Count       = 1,
  Dynamic Learned VPLS Address Count = 21038,
  Total MAC Address In Use           = 21044
```

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).
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).
Dynamic Learned Address Count	The number of MAC addresses learned by the switch. These are MAC addresses that are not statically configured addresses.

output definitions (continued)

Static Multicast Address Count	The number of static multicast addresses configured on the switch.
Permanent VPLS Address Count	The number of static VPLS MAC addresses configured on the switch with a **permanent** management status (MAC address is never aged out).
Dynamic Learned VPLS Address Count	The number of VPLS MAC Addresses learned by the switch. These addresses are not user-configured permanent addresses.
Total MAC Address In Use	The total number of MAC addresses (learned and static) that are known to the switch.

Release History

Release 6.4.2; command was introduced.

Related Commands

show mac-address-table count	Displays Source Learning MAC Address Table statistics for VLAN MAC addresses.
show mac-address-table vpls count	Displays Source Learning MAC Address Table statistics for VPLS service MAC addresses.

show mac-address-table aging-time

Displays the current aging time value.

show mac-address-table aging-time

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- The MAC Address Table aging time applies to static MAC addresses that were defined using the **time-out** parameter (see page 12-2) and to dynamically learned MAC addresses.
- Note that the aging time is the same for all VLANs and Virtual Private LAN Service (VPLS) services because it is not configurable on a per-VLAN or per-service basis. The aging time value on this platform is a global parameter that applies to all VLANs and VPLS services.

Examples

```
-> show mac-address-table aging-time
Mac Address Aging Time (seconds) = 300
```

Release History

Release 6.1; command was introduced.
Release 6.1.1; **vlan** parameter not supported.
Release 6.4.2; aging time value applied to VPLS services.

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
```

show source-learning

Displays the source learning status of a port or link aggregate of ports.

show source-learning [port *slot/port***[**-*port2***] | linkagg** *linkagg_num***]**

Syntax Definitions

slot/port1	The slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
-port2	The last port number in a range of ports that you want to configure on the same slot (e.g, 3/1-4 specifies ports 1, 2, 3, and 4 on slot 3).
linkagg_num	Specifies the link aggregate identifier.

Defaults

By default, the source learning status for all switch ports and link aggregates is displayed.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **port** *slot/port* or **linkagg** *linkagg_num* parameters to display the source learning status for a specific port or link aggregate ID.
- When the source learning status is configured for a link aggregate ID, it affects all the ports that are members of the link aggregate. However, source learning status cannot be configured on individual ports which are members of the link aggregate.

Example

```
-> show source-learning
port  source-learning
-----+-------------
1/1    disabled
1/2    enabled
1/3    disabled

-> show source-learning port 1/2
port   source-learning
-----+-------------
1/2    disabled

-> show source-learning linkagg 10
port   source-learning
-----+-------------
0/10     disabled
```

output definitions

port	The slot/port number for a switch port or a link aggregate ID number. If the interface is a link aggregate ID, zero is displayed as the slot number (e.g., 0/29).
source-learning	The source learning status of the port or link aggregate (**enabled** or **disabled**). Configured through the **source-learning** command.

Release History

Release 6.4.2; command introduced

Related Commands

source-learning	Configures the status of source MAC address learning on a single port, a range of ports or on a link aggregate of ports.

Related MIB Objects

```
slMacAddressTable
slMacLearningControlTable
  slMacLearningControlEntry
  slMacLearningControlStatus
```

show source-learning chassis-distributed

Displays the current status (enabled or disabled) of the distributed MAC source learning mode.

show source-learning chassis-distributed

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- This command is not supported on OmniSwitch stackable switches.
- When the distributed MAC mode is enabled, the MAC address table size is increased to allow more learned MAC addresses (16K per module; up to 64K per chassis).
- When the distributed MAC mode is disabled (the default), the maximum number of learned MAC addresses defaults to 16K for all OmniSwitch chassis-based switches.

Examples

```
-> show source-learning chassis-distributed
Distributed MAC Mode Configuration = disabled

-> show source-learning chassis-distributed
Distributed MAC Mode Configuration = enabled
```

Release History

Release 6.1.3; command was introduced.

Related Commands

source-learning chassis-distributed	Enables or disables the distributed MAC source learning mode.

MIB Objects

```
slMacAddressTable
   slDistributedMacMode
```

13 PPPoE Intermediate Agent Commands

Point-to-Point Protocol over Ethernet (PPPoE) provides the ability to connect a network of hosts to a Remote Access Concentrator. For example, Broadband Network Gateway over a simple bridging access device. In PPPoE model, each host utilizes its own Point-to-Point Protocol (PPP) stack and the user is presented with a familiar user interface. By using PPPoE, Access control, billing, and type of service can be configured on a per-user, rather than a per-site, basis.

PPPoE Intermediate Agent (PPPoE-IA) solution is designed for the PPPoE access method and is based on the Access Node implementing a PPPoE-IA function to insert access loop identification in PPPoE discovery packets (PADI/PADR/PADT) received from the user side.

MIB information for the PPPoE-IA commands is as follows:

Filename: alcatel-ind1-pppoe-ia-mib.mib
Module: ALCATEL-IND1-PPPOEIA-MIB

A summary of the available commands is listed here.

pppoe-ia
pppoe-ia trust
pppoe-ia client
pppoe-ia access-node-id
pppoe-ia circuit-id
pppoe-ia remote-id
clear pppoe-ia statistics
show pppoe-ia configuration
show pppoe-ia
show pppoe-ia statistics

Configuration procedures for PPPoE-IA are explained in the “Configuring PPPoE Intermediate Agent” chapter of the *OmniSwitch AOS Release 6 Network Configuration Guide*.

pppoe-ia

Configures the global PPPoE-IA status for the switch and the individual PPPoE-IA status for a port or link aggregate. The link aggregate can be either static or dynamic.

pppoe-ia [port *slot*/*port*[-*port2*] **| linkagg** *agg_id***] {enable | disable}**

Syntax Definitions

slot/port**[**-*port2***]**	The slot and port number (3/1) of the interface to configure. Use a hyphen to specify a range of ports (3/1-8).
agg_id	The link aggregate identification number.
enable	Enables PPPoE-IA for the switch or on a port.
disable	Disables PPPoE-IA for the switch or on a port.

Defaults

By default, PPPoE-IA is disabled for the switch and on all ports.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- All PPPoE-IA parameters are configurable irrespective of the per-port PPPoE-IA status (enabled or disabled).
- PPPoE-IA must be enabled globally as well as on a port.
- PPPoE-IA is not supported on port mirroring destination ports. However, the configurations are accepted.
- PPPoE-IA is not supported on aggregable ports.

Examples

```
-> pppoe-ia enable
-> pppoe-ia disable
-> pppoe-ia port 1/1 enable
-> pppoe-ia port 2/4-10 disable
-> pppoe-ia linkagg 1 enable
```

Release History

Release 6.4.5; command introduced.

Related Commands

show pppoe-ia configuration	Displays the global configuration for PPPoE-IA.
show pppoe-ia	Displays the PPPoE-IA configuration for a physical port, physical port range, link aggregate port, or all the physical or link-aggregate ports.
show pppoe-ia statistics	Displays the PPPoE-IA statistics for a physical port, link aggregate port, physical port range, or all the physical or link-aggregate ports.

MIB Objects

```
alaPPPoEIAPortConfigTable
   alaPPPoEIAPortConfigStatus
   alaPPPoEIAGlobalStatus
```

pppoe-ia trust

Configures a port or a link aggregate port as a trusted port for PPPoE-IA. A trusted port is a port that is connected to the Broadband Network Gateway whereas a client port is connected to the host.

pppoe-ia {port *slot*/*port*[-*port2*] **| linkagg** *agg_id***} trust**

Syntax Definitions

slot/port**[-***port2***]**	The slot and port number (3/1) of the interface to configure. Use a hyphen to specify a range of ports (3/1-8).
agg_id	The link aggregate identification number.

Defaults

By default, all ports are client ports.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- All PPPoE-IA parameters are configurable irrespective of per-port PPPoE-IA status (enabled or disabled).
- PPPoE-IA must be enabled globally as well as on a port.
- For PPPoE-IA to work, it must be enabled on a client port as well as a trusted port.
- PPPoE-IA is not supported on aggregable ports.
- PPPoE-IA is not supported on port mirroring destination ports; however, the configurations are accepted.

Examples

```
-> pppoe-ia port 1/1 trust
-> pppoe-ia linkagg 7 trust
```

Release History

Release 6.4.5; command introduced.

Related Commands

pppoe-ia	Enable or disable PPPoE-IA globally on the switch or on a port or link aggregate.
pppoe-ia client	Configures a port or a link aggregate port as a client port for PPPoE-IA.
show pppoe-ia configuration	Displays the global configuration for PPPoE-IA.
show pppoe-ia	Displays the PPPoE-IA configuration for a physical port, physical port range, link aggregate port, or all the physical or link-aggregate ports.
show pppoe-ia statistics	Displays the PPPoE-IA statistics for a physical port, link aggregate port, physical port range, or all the physical or link-aggregate ports.

MIB Objects

```
alaPPPoEIAPortConfigTable
   alaPPPoEIAPortConfigTrustMode
```

pppoe-ia client

Configures a port or a link aggregate port as a client port for PPPoE-IA. A client port is a port that is connected to the host whereas a trusted port is connected to the Broadband Network Gateway.

pppoe-ia {port *slot*/*port*[-*port2*] **| linkagg** *agg_id***} client**

Syntax Definitions

slot/port**[-***port2***]**	The slot and port number (3/1) of the interface to configure. Use a hyphen to specify a range of ports (3/1-8).
agg_id	The link aggregate identification number.

Defaults

By default, all ports are client ports.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- All PPPoE-IA parameters are configurable irrespective of per-port PPPoE-IA status (enabled or disabled).
- PPPoE-IA must be enabled globally as well as on a port.
- For PPPoE-IA to work, it must be enabled on a client port as well as a trusted port.
- PPPoE-IA is not supported on aggregable ports.
- PPPoE-IA is not supported on port mirroring destination ports; however, the configurations are accepted.

Examples

```
-> pppoe-ia port 1/2-6 client
-> pppoe-ia linkagg 2 client
```

Release History

Release 6.4.5; command introduced.

Related Commands

pppoe-ia	Enable or disable PPPoE-IA globally on the switch or on a port or link aggregate.
pppoe-ia trust	Configures a port or a link aggregate port as a trusted port for PPPoE-IA.
show pppoe-ia configuration	Displays the global configuration for PPPoE-IA.
show pppoe-ia	Displays the PPPoE-IA configuration for a physical port, physical port range, link aggregate port, or all the physical or link-aggregate ports.
show pppoe-ia statistics	Displays the PPPoE-IA statistics for a physical port, link aggregate port, physical port range, or all the physical or link-aggregate ports.

MIB Objects

```
alaPPPoEIAPortConfigTable
   alaPPPoEIAPortConfigTrustMode
```

pppoe-ia access-node-id

Globally configures a format to form an identifier that uniquely identifies an access node.

pppoe-ia access-node-id {base-mac | system-name | mgnt-address | user-string *string***}**

Syntax Definitions

base-mac	The base MAC address of the switch.
system-name	The configured name of the switch.
mgnt-address	The IP address of the management interface of the switch.
string	The value of user configured string.

Defaults

By default, PPPoE-IA uses the base MAC address of the switch as the Access-Node-Identifier.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The access-node-identifier can have a maximum of 32 characters. The access-node-identifier longer than 32 characters is truncated to 32 characters.
- The access-node-identifier when configured as user-string must not contain spaces.
- The value of user string must not be NULL.
- In case of management address format, IP address of the Loopback0 interface (if configured and active) or the first active IP interface address is used as the management address. If none of them are available, IP address ‘0.0.0.0’ is used as management address.
- If the access-node-identifier is configured as any other format other than user-string format, then the string value configuration is not allowed through SNMP or Web View application.
- It is mandatory to provide the string value through SNMP using Multi-varbind for the user-string format.

Examples

```
-> pppoe-ia access-node-id base-mac
-> pppoe-ia access-node-id user-string accessnode1
```

Release History

Release 6.4.5; command introduced.

Related Commands

pppoe-ia	Enable or disable PPPoE-IA globally on the switch or on a port or link aggregate.
show pppoe-ia configuration	Displays the global configuration for PPPoE-IA.

MIB Objects

```
alaPPPoEIAGlobalAccessNodeIDFormatType
alaPPPoEIAGlobalAccessNodeIDStringValue
```

pppoe-ia circuit-id

Globally configures a Circuit-ID format that forms an identifier that uniquely identifies an access node and an access loop that receives the PPPoE Active Discovery Initiation (PADI) or PPPoE Active Discovery Request (PADR) or PPPoE Active Discovery Terminate (PADT) from the user end.

pppoe-ia circuit-id {default | ascii [base-mac | system-name | interface | vlan | cvlan | interface-alias | user-string *string* **| delimiter** *char***]}**

Syntax Definitions

default	The default value of the Circuit-ID. Default format of Circuit-ID is "access-node-id eth slot/port:[vlan]"
ascii	Circuit-ID format used to configure Circuit-ID string using the five parameters and delimiter. Maximum five parameters can be selected from the given seven options: base-mac, system-name, interface, vlan, cvlan, interface-alias, and user-string.
base-mac	The base MAC address of the switch.
system-name	Name configured for the switch.
interface	The interface on which the PPPoE message is received.
vlan	VLAN interface on which the PPPoE message is received.
cvlan	Inner-VLAN or customer VLAN of the PPPoE message.
interface-alias	Configured alias of the interface on which the PPPoE message is received.
string	The value of user configured string.
delimiter	A user configurable delimiter used to separate the fields of an ASCII string forming the Circuit-ID.
char	The value (a character) of the user configurable delimiter. The available delimiters are: “:” (colon), “|” (pipe), “/” (forward slash), “\” (backward slash), “-” (hyphen), “'_” (underscore), “ ” (space), “#” (hash), “.” (full stop), “,” (comma), “;” (semicolon).

Defaults

- By default, the value of the Circuit-ID is "access-node-id eth slot/port[:vlan-id]". For example, if the value of access-node-id is "vxTarget", the default value of Circuit-ID is "vxTarget eth 1/1:10", if the packet is received on the interface 1/1 in vlan 10.
- By default, the delimiter used is “:”.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Circuit-ID identification is configurable only globally and cannot be configured on a per-port or per-VLAN basis.
- The Circuit-ID can have a maximum of 63 characters. The Circuit-ID longer than 63 characters is truncated to 63 characters.
- At most, five fields out of the available seven are encoded for the Circuit-ID in the order specified by the user.
- If the access-node-identifier is configured as any other format other than user-string format, then the string value configuration is not allowed through SNMP or Web View application.
- It is mandatory to provide the string value through SNMP using Multi-varbind for the user-string format.
- The value of user string must not be NULL.
- You can configure the same Circuit-ID format multiple times (for example, base MAC address of the switch can be configured multiple times in ASCII format of Circuit-ID).
- If the Circuit-ID format is default, irrespective of the ASCII fields (if configured), the Circuit-ID configuration is not visible in **show pppoe-ia configuration** output.

Examples

```
-> pppoe-ia circuit-id ascii base-mac vlan
-> pppoe-ia circuit-id ascii system-name interface user-string cid1
-> pppoe-ia circuit-id ascii system-name delimiter #
```

Release History

Release 6.4.5; command introduced.

Related Commands

pppoe-ia access-node-id	Configures the access node ID for the switch.
pppoe-ia	Enable or disable PPPoE-IA globally on the switch or on a port or link aggregate.
show pppoe-ia configuration	Displays the global configuration for PPPoE-IA.

MIB Objects

```
alaPPPoEIAGlobalCircuitIDFormatType
alaPPPoEIAGlobalCircuitIDField1
alaPPPoEIAGlobalCircuitIDField1StrVal
alaPPPoEIAGlobalCircuitIDField2
alaPPPoEIAGlobalCircuitIDField2StrVal
alaPPPoEIAGlobalCircuitIDField3
alaPPPoEIAGlobalCircuitIDField3StrVal
alaPPPoEIAGlobalCircuitIDField4
alaPPPoEIAGlobalCircuitIDField4StrVal
alaPPPoEIAGlobalCircuitIDField5
alaPPPoEIAGlobalCircuitIDField5StrVal
alaPPPoEIAGlobalCircuitIDDelimiter
```

pppoe-ia remote-id

Globally configures a format to form an identifier that uniquely identifies the user attached to the access loop.

pppoe-ia remote-id {base-mac | system-name | mgnt-address | user-string *string***}**

Syntax Definitions

base-mac	The base MAC address of the switch.
system-name	The name configured for the switch.
mgnt-address	The management IP address of the switch.
string	The value configured for user string.

Defaults

By default, the base MAC address of the switch is used as the format for Remote-ID.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Remote-ID is configurable only globally and cannot be configured on a per-port or per-VLAN basis.
- Remote-ID can have a maximum of 63 characters. The Remote-ID longer than 63 characters is truncated to 63 characters.
- In case of management address format, IP address of the Loopback0 interface (if configured and active) or the first active IP interface address is used as the management address. If none of them are available, IP address ‘0.0.0.0’ is used as management address.
- If the Remote-ID is configured as any other format other than user-string format, then the string value configuration is not allowed through SNMP or Web View application.
- It is mandatory to provide the string value through SNMP using Multi-varbind for the user-string format.
- The value of user string must not be NULL.

Examples

```
-> pppoe-ia remote-id base-mac
-> pppoe-ia remote-id user-string remoteuser1
```

Release History

Release 6.4.5; command introduced.

Related Commands

pppoe-ia	Enable or disable PPPoE-IA globally on the switch.
show pppoe-ia configuration	Displays the global configuration for PPPoE-IA.

MIB Objects

```
alaPPPoEIAGlobalRemoteIDFormatType
alaPPPoEIAGlobalRemoteIDStringValue
```

clear pppoe-ia statistics

Clears the statistics for all the physical or link-aggregate ports, a single port or a link aggregate port, or a range of physical ports for PPPoE-IA.

clear pppoe-ia statistics [port {*slot/port*[*-port2*] | **linkagg** *agg_id***]**

Syntax Definitions

slot/port**[-***port2***]**	The slot and port number (3/1) of the interface to configure. Use a hyphen to specify a range of ports (3/1-8).
agg_id	The link aggregate identification number.

Defaults

By default, clears the statistics for all ports and link aggregates.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the **port** or **linkagg** parameters to clear statistics for a specific port number or link aggregate ID.

Examples

```
-> clear pppoe-ia statistics
-> clear pppoe-ia statistics port 1/10
-> clear pppoe-ia statistics port 2/1-5
-> clear pppoe-ia statistics linkagg 13
```

Release History

Release 6.4.5; command introduced.

Related Commands

show pppoe-ia statistics	Displays the PPPoE-IA statistics for a physical port, link aggregate port, physical port range, or all the physical or link-aggregate ports.
show pppoe-ia	Displays the PPPoE-IA port or link aggregate configuration for the switch.

MIB Objects

```
alaPPPoEIAGlobalClearStats
alaPPPoEIAStatsTable
   alaPPPoEIAStatsClearStats
```

show pppoe-ia configuration

Displays the global configuration for PPPoE-IA.

show pppoe-ia configuration

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
Default Configuration
-> show pppoe-ia configuration
Status                     : disabled,
Access Node Identifier
  Access-node-id Format    : base-mac,
  Access-node-id String    : 00:d0:95:ee:fb:02,
Circuit Identifier
  Circuit-Id Format        : default,
  Circuit-id Field1        : none,
  Circuit-id Field1 String : ,
  Circuit-id Field2        : none,
  Circuit-id Field2 String : ,
  Circuit-id Field3        : none,
  Circuit-id Field3 String : ,
  Circuit-id Field4        : none,
  Circuit-id Field4 String : ,
  Circuit-id Field5        : none,
  Circuit-id Field5 String : ,
  Circuit-id Delimiter     : ":",
Remote Identifier
  Remote-id Format         : base-mac,
  Remote-id String         : 00:d0:95:ee:fb:02
```

```
-> show pppoe-ia configuration
Status                     : enabled,
Access Node Identifier
  Access-node-id Format    : system-name,
  Access-node-id String    : vxTarget,
Circuit Identifier
  Circuit-Id Format        : ascii,
  Circuit-id Field1        : system-name,
  Circuit-id Field1 String : vxTarget,
  Circuit-id Field2        : base-mac,
  Circuit-id Field2 String : 00:d0:95:ee:fb:02,
  Circuit-id Field3        : interface,
  Circuit-id Field3 String : ,
  Circuit-id Field4        : none,
  Circuit-id Field4 String : ,
  Circuit-id Field5        : none,
  Circuit-id Field5 String : ,
  Circuit-id Delimiter     : "|",
Remote Identifier
  Remote-id Format         : mgnt-address,
  Remote-id String         : 172.21.161.106
```

output definitions

Status	Displays the global PPPoE-IA status: Enabled or Disabled.
Access-node-id Format	The format used to form an identifier that uniquely identifies an access node.
Access-node-id String	The value of user configured string for the access node.
Circuit-Id Format	The format used to form an identifier that uniquely identifies an access node and an access loop.
Circuit-id Field1	The Circuit-ID format.
Circuit-id Field1 String	The value of Circuit-ID depending on the format configured for the Circuit-ID.
Circuit-id Delimiter	A user configurable delimiter (a character) used to separate the fields of an ASCII string forming the Circuit-ID.
Remote-id Format	The format used to form an identifier that uniquely identifies the user attached to the access loop.
Remote-id String	The value of user configured string for the Remote-ID.

Release History

Release 6.4.5; command introduced.

Related Commands

pppoe-ia	Enable or disable PPPoE-IA globally on the switch or for a port or link aggregate.
pppoe-ia access-node-id	Globally configures a format to form an identifier that uniquely identifies an access node.
pppoe-ia circuit-id	Globally configures a Circuit-ID format that forms an identifier that uniquely identifies an access node and an access loop on which the PADI/PADR/PADT is received from the user side.
pppoe-ia remote-id	Globally configures a format to form an identifier that uniquely identifies the user attached to the access loop.

MIB Objects

```
alaPPPoEIAGlobalStatus
alaPPPoEIAGlobalAccessNodeIDFormatType
alaPPPoEIAGlobalAccessNodeIDStringValue
alaPPPoEIAGlobalCircuitIDFormatType
alaPPPoEIAGlobalCircuitIDField1
alaPPPoEIAGlobalCircuitIDField1StrVal
alaPPPoEIAGlobalCircuitIDField2
alaPPPoEIAGlobalCircuitIDField2StrVal
alaPPPoEIAGlobalCircuitIDField3
alaPPPoEIAGlobalCircuitIDField3StrVal
alaPPPoEIAGlobalCircuitIDField4
alaPPPoEIAGlobalCircuitIDField4StrVal
alaPPPoEIAGlobalCircuitIDField5
alaPPPoEIAGlobalCircuitIDField5StrVal
alaPPPoEIAGlobalCircuitIDDelimiter
alaPPPoEIAGlobalRemoteIDFormatType
alaPPPoEIAGlobalRemoteIDStringValue
```

show pppoe-ia

Displays the following:

- PPPoE-IA configuration for a physical or link-aggregate port, physical port range, or all the physical or link-aggregate ports.
- Port or port range configuration for ports with PPPoE-IA enabled or disabled
- Ports that are configured as trust or client port for PPPoE-IA.

show pppoe-ia [port {*slot*/*port*[*-port2*] **| linkagg** *agg_id***] [enabled | disabled | trusted | client]**

Syntax Definitions

slot/port**[-***port2***]**	The slot and port number (3/1) of the interface to configure. Use a hyphen to specify a range of ports (3/1-8).
agg_id	The link aggregate identification number.
enabled	PPPoE-IA enabled port.
disabled	PPPoE-IA disabled port.
trusted	Port configured as trust.
client	Port configured as client.

Defaults

By default, displays information for all PPPoE-IA ports and link aggregates.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the optional command parameters to display information for a specific port or link aggregate.

Examples

```
Default Configuration
-> show pppoe-ia port
Slot/Port    Status      Mode
----------+----------+------------
1/1        enabled     client
1/2        disabled    trusted
1/3        disabled    client
1/4        enabled     trusted
.
.
.
1/24        enabled     client
0/0         enabled     client
0/1         disabled    trusted
```

```
-> show pppoe-ia linkagg 1 enabled
ERROR: PPPoE-IA is disabled on linkagg 1

-> show pppoe-ia port 1/1 trusted
Slot/Port   Status
----------+----------
1/3        enabled

-> show pppoe-ia port 1/1-5 client
Slot/Port   Status
----------+----------
1/1        enabled
1/2        disabled
1/5        disabled
```

output definitions

Slot/Port	Interface slot and port number.
Status	PPPoE-IA enabled or disabled port.
Mode	Port configured as trusted or client port for PPPoE-IA.

Release History

Release 6.4.5; command introduced.

Related Commands

pppoe-ia	Enable or disable PPPoE-IA globally on the switch or on a port or link aggregate.
pppoe-ia trust	Configures a port or a link aggregate port as a trusted port for PPPoE-IA.
pppoe-ia client	Configures a port or a link aggregate port as a client port for PPPoE-IA.

MIB Objects

N/A

show pppoe-ia statistics

Displays the PPPoE-IA statistics for a physical port, link aggregate port, physical port range, or all the physical or link-aggregate ports.

show pppoe-ia statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
Default Configuration
-> show pppoe-ia statistics
Slot/  PADI   PADR   PADT    PADI     PADR    PADT    PADO    PADS
Port    Rx     Rx     Rx    Discard  Discard Discard Discard Discard
------+------+------+------+--------+-------+-------+-------+--------
1/1     2      2      0      1        0       0       2       3
1/2     2      1      0      1        0       0       2       0
1/3     3      2      2      2        1       2       2       3
.
.
1/24    2      2      0      1        0       0       2       3
0/0     2      2      0      1        0       0       2       3
0/1     2      2      0      1        0       0       2       3

-> show pppoe-ia linkagg 1 statistics
Slot/  PADI   PADR   PADT    PADI     PADR    PADT    PADO    PADS
Port    Rx     Rx     Rx    Discard  Discard Discard Discard Discard
------+------+------+------+--------+-------+-------+-------+--------
0/1     2      2      0      1        0       0       2       3
```

output definitions

Slot/Port	Interface slot and port number.
PADI Rx	Valid PADI (PPPoE Active Discovery Initiation) packets received on the client port.
PADR Rx	Valid PADR (PPPoE Active Discovery Request) packets received on the client port.

output definitions (continued)

PADT Rx	Valid PADT (PPPoE Active Discovery Terminate) packets received on the client port.
PADI Discard	Invalid (malformed or PDU length exceeds 1484) PADI packets received on the client port or no enabled trust port in the same VLAN as the client port.
PADR Discard	Invalid (malformed or PDU length exceeds 1500) PADR packets received on client port or no enabled trust port in the same VLAN as the client port.
PADT Discard	Invalid (malformed or PDU length exceeds 1500) PADT packets received on client port or no enabled trust port in the same VLAN as the client port.
PADO Discard	Total PADO (PPPoE Active Discovery Offer) packets received on the client port.
PADS Discard	Total PADS (PPPoE Active Discovery Session-confirmation) packets received on the client port.

Release History

Release 6.4.5; command introduced.

Related Commands

clear pppoe-ia statistics	Clears the statistics for all the physical or link-aggregate ports, a single port or a link aggregate port, or a range of physical ports for PPPoE-IA.
show pppoe-ia configuration	Displays the global configuration for PPPoE-IA.

MIB Objects

```
alaPPPoEIAStatsTable
   alaPPPoEIAStatsIfIndex
   alaPPPoEIAStatsPADIRxCounter
   alaPPPoEIAStatsPADRRxCounter
   alaPPPoEIAStatsPADTRxCounter
   alaPPPoEIAStatsPADIRxDiscardCounter
   alaPPPoEIAStatsPADRRxDiscardCounter
   alaPPPoEIAStatsPADTRxDiscardCounter
   alaPPPoEIAStatsPADORxDiscardCounter
   alaPPPoEIAStatsPADSRxDiscardCounter
```

14 GVRP Commands

The GARP VLAN Registration Protocol (GVRP) facilitates control of virtual local area networks (VLANs) within a larger network. It is an application of General Attribute Registration Protocol (GARP) that provides the VLAN registration service. The GARP provides a generic framework whereby devices in a bridged LAN can register and de-register attribute values, such as VLAN identifiers.

GVRP is compliant with 802.1q and dynamically learns and further propagates VLAN membership information across a bridged network. It dynamically maintains and updates the registration and de-registration of VLANs and prunes unnecessary broadcast and unicast traffic. Through propagation of GVRP information, a switch can continuously update its knowledge on the set of VLANs that currently have active nodes and on ports through which those nodes can be reached.

A summary of the available commands is listed here:

gvrp
gvrp port
gvrp transparent switching
gvrp maximum vlan
gvrp registration
gvrp applicant
gvrp timer
gvrp restrict-vlan-registration
gvrp restrict-vlan-advertisement
gvrp static-vlan restrict
clear gvrp statistics
show gvrp statistics
show gvrp last-pdu-origin
show gvrp configuration
show gvrp configuration port
show gvrp configuration linkagg/port
show gvrp timer

gvrp

Enables GVRP on the switch globally.

gvrp

no gvrp

Syntax Definitions

N/A

Defaults

By default, GVRP is disabled on the switch.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to disable GVRP globally on the switch.
- Disabling GVRP globally will delete all the learned VLANs.
- GVRP is supported only when the switch is operating in the flat Spanning Tree mode; it is not supported in the 1x1 mode.

Examples

```
-> gvrp
-> no gvrp
```

Release History

Release 6.2.1; command was introduced.

Related Commands

show gvrp configuration	Displays the global configuration for GVRP.

MIB Objects

```
dot1qGvrpStatus
```

gvrp port

Enables GVRP on a specific port or an aggregate of ports on the switch.

gvrp {linkagg *agg_num* | **port** *slot/port***}**

no gvrp {linkagg *agg_num* | **port** *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).
agg_num	The number corresponding to the aggregate group.

Defaults

By default, GVRP is disabled on the ports.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to disable GVRP on the specified ports.
- GVRP can be enabled on ports regardless of whether it is globally enabled or not. However, for the port to become an active participant, you should enable GVRP globally on the switch.
- When GVRP is globally enabled on the switch and is not enabled on the port, that port is excluded from the GVRP process.
- GVRP can be enabled only on fixed ports, 802.1 Q ports, and aggregate ports. Other ports (mirror ports, aggregable ports, mobile ports, and MSTI Trunking ports) do not support GVRP.
- To use the *agg_num* parameter, the link aggregate group should be created and enabled.

Examples

```
-> gvrp port 3/2
-> no gvrp port 3/2
-> gvrp linkagg 2
```

Release History

Release 6.2.1; command was introduced.

Related Commands

show gvrp configuration port	Displays the GVRP configuration for all the ports.
show gvrp configuration linkagg/port	Displays the GVRP configuration for a specific port or an aggregate of ports.

MIB Objects

```
dot1qPortVlanTable
   dot1qPortGvrpStatus
```

gvrp transparent switching

Enables transparent switching on the switch. When transparent switching is enabled, the switch propagates GVRP information to other switches but does not register itself in the GVRP process.

gvrp transparent switching

no gvrp transparent switching

Syntax Definitions

N/A

Defaults

By default, transparent switching is disabled on the switch.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to disable transparent switching on the device.
- If GVRP is globally disabled and transparent switching is enabled, the router will flood the GVRP messages.
- If GVRP is globally disabled and transparent switching is disabled, the router will discard the GVRP messages.
- If GVRP is globally enabled transparent switching will not have any effect on the functional behavior of the device.

Examples

```
-> gvrp transparent switching
-> no gvrp transparent switching
```

Release History

Release 6.2.1; command was introduced.
Release 6.3.1; support for OmniSwitch chassis-based switches added.

Related Commands

show gvrp configuration	Displays the global configuration for GVRP.

MIB Objects

```
alaGvrpTransparentSwitching
```

gvrp maximum vlan

Configures the maximum number of dynamic VLANs that can be created by GVRP.

gvrp maximum vlan *vlanlimit*

Syntax Definitions

vlanlimit	The maximum number of VLANs to be created by GVRP. The valid range is 32–4094.

Defaults

parameter	default
vlanlimit	256

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- This command can be used even when GVRP is not enabled on the switch. However, GVRP should be enabled on the switch for creating dynamic VLANs.
- If the VLAN limit to be set is less than the current number of dynamically learnt VLANs, then the new configuration will take effect only after the GVRP is disabled and enabled again on the switch. If this operation is not done, the VLANs learnt earlier will be maintained.

Examples

```
-> gvrp maximum vlan 100
```

Release History

Release 6.2.1; command was introduced.

Related Commands

show gvrp configuration	Displays the global configuration for GVRP.

MIB Objects

```
alaGvrpMaxVlanLimit
```

gvrp registration

Configures the GVRP registration mode for a specific port or an aggregate of ports.

gvrp registration {normal | **fixed** | **forbidden} {linkagg** *agg_num* | **port** *slot/port***}**

no gvrp registration {linkagg *agg_num* | **port** *slot/port***}**

Syntax Definitions

normal	Specifies that both registration and de-registration of VLANs are allowed. VLANs can be mapped either dynamically (through GVRP) or statically (through management application) on such a port.
fixed	Specifies that only static mapping of VLANs is allowed on the port but de-registration of previously created dynamic or static VLANs is not allowed.
forbidden	Specifies that dynamic VLAN registration or de-registration is not allowed on the port. Any dynamic VLAN created earlier will be de-registered.
agg_num	The number corresponding to the aggregate group.
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).

Defaults

parameter	default
normal | fixed | forbidden	**normal**

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to set the registration mode to the default value.
- GVRP should be enabled on the port before configuring the GVRP registration mode.
- The registration mode for the default VLANs of all the ports in the switch will be set to fixed.
- To use the *agg_num* parameter, the link aggregate group should be created and enabled.

Examples

```
-> gvrp registration forbidden port 3/2
-> no gvrp registration port 3/2
```

Release History

Release 6.2.1; command was introduced.

Related Commands

show gvrp configuration linkagg/port	Displays the GVRP configuration for a specific port or an aggregate of ports.

MIB Objects

```
alaGvrpPortConfigtable
   alaGvrpPortConfigRegistrarMode
```

gvrp applicant

Configures the applicant mode of a specific port or an aggregate of ports on the switch. The applicant mode determines whether or not GVRP PDU exchanges are allowed on a port depending on the Spanning Tree state of the port.

gvrp applicant {participant | non-participant | active} {linkagg *agg_num* | **port** *slot/port***}**

no gvrp applicant {linkagg *agg_num* | **port** *slot/port***}**

Syntax Definitions

participant	Specifies that GVRP PDU exchanges are only allowed when the port is in the STP forwarding state.
non-participant	Specifies that no GVRP PDU exchanges are allowed on the port, regardless of the STP status of the port.
active	Specifies that GVRP PDU exchanges are allowed when the port is either in the STP forwarding or STP blocking state.
agg_num	The number corresponding to the aggregate group.
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).

Defaults

parameter	default
participant | non-participant | active	**participant**

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to set the applicant mode to the default value.
- GVRP should be enabled on the port before configuring the GVRP applicant mode.
- To use the *agg_num* parameter, the link aggregate group should be created and enabled.

Examples

```
-> gvrp applicant active port 2/2
-> no gvrp applicant port 2/2
```

Release History

Release 6.2.1; command was introduced.

Related Commands

show gvrp configuration linkagg/port	Displays the GVRP configuration for a specific port or an aggregate of ports.

MIB Objects

```
alaGvrpPortConfigtable
   alaGvrpPortConfigApplicantMode
```

gvrp timer

Configures the Join, Leave, or LeaveAll timer values for the switch ports.

gvrp timer {join | leave | leaveall} *timer-value* **{linkagg** *agg_num* | **port** *slot/port***}**

no gvrp timer {join | leave | leaveall} {linkagg *agg_num* | **port** *slot/port***}**

Syntax Definitions

join	Specifies the value of the Join timer in milliseconds.
leave	Specifies the value of the Leave timer in milliseconds.
leaveall	Specifies the value of the LeaveAll timer in milliseconds.
timer-value	The value of the specified timer in milliseconds. The valid range is 1–2,147,483,647 for Join timer, 3–2,147,483,647 for Leave timer, and 3–2,147,483,647 for LeaveAll timer.
agg_num	The number corresponding to the aggregate group.
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).

Defaults

parameter	default
timer-value **(join)**	600 ms
timer-value **(leave)**	1800 ms
*timer-value (***leaveall)**	30000 ms

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to set the timer for a particular slot or port to the default value.
- GVRP should be enabled on the port before configuring the timer value for that port.
- Leave timer value should be greater than or equal to three times the Join timer value.
- Leaveall timer value should be greater than or equal to the Leave timer value.
- To use the *agg_num* parameter, the link aggregate group should be created and enabled.

Examples

```
-> gvrp timer join 300 port 3/2
-> no gvrp timer join 3/2
-> gvrp timer leave 900 port 3/2
-> no gvrp timer leave port 3/2
-> gvrp timer leaveall 950 port 3/2
-> no gvrp timer leaveall port 3/2
```

Release History

Release 6.2.1; command was introduced.

Related Commands

show gvrp timer	Displays the timer values configured for all the ports or a specific port.
show gvrp configuration linkagg/port	Displays the GVRP configuration for a specific port or an aggregate of ports.

MIB Objects

```
alaGvrpPortConfigTable
   alaGvrpPortConfigJoinTimer
   alaGvrpPortConfigLeaveTimer
   alaGvrpPortConfigLeaveAllTimer
```

gvrp restrict-vlan-registration

Restricts GVRP processing from dynamically registering the specified VLAN(s) on the switch.

gvrp restrict-vlan-registration {linkagg *agg_num* | **port** *slot/port***}** *vlan-list*

no gvrp restrict-vlan-registration {linkagg *agg_num* | **port** *slot/port***}** *vlan-list*

Syntax Definitions

agg_num	The number corresponding to the aggregate group.
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).
vlan-list	The VLAN ID or the VLAN ID range (e.g., 1-10).

Defaults

By default, GVRP dynamic VLAN registration is not restricted.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to allow registration of dynamic VLAN IDs through GVRP processing.
- GVRP should be enabled on the port before restricting dynamic VLAN registrations on that port.
- This command can be used only if the GVRP registration mode is set to normal.
- If the specified VLAN already exists on the switch, the VLAN is mapped to the receiving port.
- To use the *agg_num* parameter, the link aggregate group should be created and enabled.

Examples

```
-> gvrp restrict-vlan-registration port 3/1 5
-> no gvrp restrict-vlan-registration port 3/1 5
-> gvrp restrict-vlan-registration port 3/1 6-10
-> no gvrp restrict-vlan-registration port 3/1 6-10
```

Release History

Release 6.2.1; command was introduced.

Related Commands

gvrp registration	Configures the GVRP registration mode for the switch ports.
show gvrp configuration linkagg/port	Displays the GVRP configuration for a specific port or an aggregate of ports.

MIB Objects

```
alaGvrpPortConfigTable
   alaGvrpPortConfigRestrictedRegistrationBitmap
   alaGvrpPortConfigAllowRegistrationBitmap
   alaGvrpPortConfigRegistrationBitmap
```

gvrp restrict-vlan-advertisement

Restricts the advertisement of VLANs on a specific port or an aggregate of ports.

gvrp restrict-vlan-advertisement {linkagg *agg_num* | **port** *slot/port***}** *vlan-list*

no gvrp restrict-vlan-advertisement {linkagg *agg_num* | **port** *slot/port***}** *vlan-list*

Syntax Definitions

agg_num	The number corresponding to the aggregate group.
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).
vlan-list	The VLAN ID or the VLAN ID range (e.g., 1-10).

Defaults

By default, VLAN advertisement is not restricted.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to allow the propagation of VLANs.
- GVRP should be enabled on the port before restricting VLAN advertisements on that port.
- This command affects the GVRP processing only if the applicant mode is set to participant or active.
- To use the *agg_num* parameter, the link aggregate group should be created and enabled.

Examples

```
-> gvrp restrict-vlan-advertisement port 3/1 4
-> no gvrp restrict-vlan-advertisement port 3/1 4
-> gvrp restrict-vlan-advertisement port 3/1 6-9
-> no gvrp restrict-vlan-advertisement port 3/1 6-9
-> gvrp restrict-vlan-advertisement linkagg 3 10
-> no gvrp restrict-vlan-advertisement linkagg 3 10
```

Release History

Release 6.2.1; command was introduced.

Related Commands

gvrp applicant	Configures the applicant mode for the switch port.
show gvrp configuration linkagg/port	Displays the GVRP configuration for a specific port or an aggregate of ports.

MIB Objects

```
alaGvrpPortConfigTable
   alaGvrpPortConfigRestrictedApplicantBitmap
   alaGvrpPortConfigAllowApplicantBitmap
   alaGvrpPortConfigApplicantBitmap
```

gvrp static-vlan restrict

Restricts a port from becoming a member of a statically created VLAN or a range of VLANs.

gvrp static-vlan restrict {linkagg *agg_num* | **port** *slot/port***}** *vlan-list*

no gvrp static-vlan restrict {linkagg *agg_num* | **port** *slot/port***}** *vlan-list*

Syntax Definitions

agg_num	The number corresponding to the aggregate group.
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).
vlan-list	The VLAN ID or the VLAN ID range (e.g., 1-10).

Defaults

By default, ports are assigned to the static VLAN based on GVRP PDU processing.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to set the specified port and VLAN to the default value.
- GVRP should be enabled on the port before restricting static VLAN registrations on that port.
- This command does not apply to dynamic VLANs.
- To use the *agg_num* parameter, the link aggregate group should be created and enabled.

Examples

```
-> gvrp static-vlan restrict port 3/2 5
-> no gvrp static-vlan restrict port 3/2 5
-> gvrp static-vlan restrict port 3/2 6-9
-> no gvrp static-vlan restrict port 3/2 6-9
-> gvrp static-vlan restrict linkagg 3 4-5
-> no gvrp static-vlan aggregate linkagg 3 4-5
```

Release History

Release 6.2.1; command was introduced.

Related Commands

show gvrp configuration linkagg/port	Displays the GVRP configuration for a specific port or an aggregate of ports.

MIB Objects

```
alaGvrpPortConfigTable
   alaGvrpPortConfigRegistrationToStaticVlan
   alaGvrpPortConfigRegistrationToStaticVlanLearn
   alaGvrpPortConfigRegistrationToStaticVlanRestrict
```

clear gvrp statistics

Clears GVRP statistics for all the ports, an aggregate of ports, or a specific port.

clear gvrp statistics [linkagg *agg_num* | **port** *slot/port***]**

Syntax Definitions

agg_num	The number corresponding to the aggregate group.
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).

Defaults

By default, the GVRP statistics are deleted for all the ports.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

Use the *agg_num* or *slot/port* parameter with this command to clear GVRP statistics for a specific port.

Examples

```
-> clear gvrp statistics port 3/2
```

Release History

Release 6.2.1; command was introduced.

Related Commands

show gvrp statistics	Displays the GVRP statistics or all the ports, an aggregate of ports, or a specific port.

MIB Objects

```
   alaGvrpGlobalClearStats
alaGvrpPortStatsTable
   alaGvrpPortStatsClearStats
```

show gvrp statistics

Displays the GVRP statistics for all the ports, an aggregate of ports, or a specific port.

show gvrp statistics [linkagg *agg_num* | **port** *slot/port***]**

Syntax Definitions

agg_num	The number corresponding to the aggregate group.
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).

Defaults

By default, the GVRP statistics are displayed for all ports.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

Use the *agg_num* or *slot/port* parameter with this command to display GVRP statistics for a specific port.

Examples

```
-> show gvrp statistics port 1/21
Port 1/21:
  Join Empty Received     : 8290,
  Join In Received        : 1526,
  Empty Received          : 0,
  Leave Empty Received    : 1,
  Leave In Received       : 0,
  Leave All Received      : 283,
  Join Empty Transmitted  : 826,
  Join In Transmitted     : 1532,
  Empty Transmitted       : 39,
  Leave Empty Transmitted : 0,
  Leave In Transmitted    : 0,
  Leave All Transmitted   : 296,
  Failed Registrations    : 0,
  Garp PDU Received       : 1160,
  Garp PDU Transmitted    : 957,
  Garp Msgs Received      : 10100,
  Garp Msgs Transmitted   : 2693,
  Invalid Msgs Received   : 0


-> show gvrp statistics
Port 1/1:
  Join Empty Received     : 0,
  Join In Received        : 0,
  Empty Received          : 0,
  Leave Empty Received    : 0,
```

```
  Leave In Received       : 0,
  Leave All Received      : 0,
  Join Empty Transmitted  : 0,
  Join In Transmitted     : 0,
  Empty Transmitted       : 0,
  Leave Empty Transmitted : 0,
  Leave In Transmitted    : 0,
  Leave All Transmitted   : 0,
  Failed Registrations    : 0,
  Garp PDU Received       : 0,
  Garp PDU Transmitted    : 0,
  Garp Msgs Received      : 0,
  Garp Msgs Transmitted   : 0,
  Invalid Msgs Received   : 0


Port 1/2:
  Join Empty Received     : 8330,
  Join In Received        : 1526,
  Empty Received          : 0,
  Leave Empty Received    : 1,
  Leave In Received       : 0,
  Leave All Received      : 284,
  Join Empty Transmitted  : 830,
  Join In Transmitted     : 1532,
  Empty Transmitted       : 39,
  Leave Empty Transmitted : 0,
  Leave In Transmitted    : 0,
  Leave All Transmitted   : 297,
  Failed Registrations    : 0,
  Garp PDU Received       : 1165,
  Garp PDU Transmitted    : 962,
  Garp Msgs Received      : 10141,
  Garp Msgs Transmitted   : 2698,
  Invalid Msgs Received   : 0


Port 1/3:
  Join Empty Received     : 0,
  Join In Received        : 0,
  Empty Received          : 0,
```

output definitions

Join Empty Received	The number of Join Empty messages received.
Join In Received	The number of Join In messages received.
Empty Received	The number of Empty messages received.
Leave Empty Received	The number of Leave Empty messages received.
Leave In Received	The number of Leave In messages received.
Leave All Received	The number of Leave All messages received.
Join Empty Transmitted	The number of Join Empty messages transmitted.
Join In Transmitted	The number of Join In messages transmitted.
Empty Transmitted	The number of Empty messages transmitted.
Leave Empty Transmitted	The number of Leave Empty messages transmitted.

output definitions

Join Empty Received	The number of Join Empty messages received.
Leave In Transmitted	The number of Leave In messages transmitted.
Leave All Transmitted	The number of Leave All messages transmitted.
Failed Registrations	The number of failed registrations.
Total PDU Received	The number of total PDUs received.
Total PDU Transmitted	The number of total PDUs transmitted.
Invalid Msgs Received	The number of invalid messages received.
Total Msgs Received	The number of total messages received.
Total Msgs Transmitted	The number of total messages transmitted.

Release History

Release 6.2.1; command was introduced.
Release 6.3.1; **Total PDU Received, Total PDU Transmitted, Invalid Msgs Received, Total Msgs Received, Total Msgs Transmitted** fields are added.

Related Commands

clear gvrp statistics	Clears GVRP statistics for all the ports, an aggregate of ports, or a specific port.

MIB Objects

```
alaGvrpPortStatsTable
   alaGvrpPortStatsJoinEmptyReceived
   alaGvrpPortStatsJoinInReceived
   alaGvrpPortStatsEmptyReceived
   alaGvrpPortStatsLeaveInReceived
   alaGvrpPortStatsLeaveEmptyReceived
   alaGvrpPortStatsLeaveAllReceived
   alaGvrpPortStatsJoinEmptyTransmitted
   alaGvrpPortStatsJoinInTransmitted
   alaGvrpPortStatsEmptyTransmitted
   alaGvrpPortStatsLeaveInTransmitted
   alaGvrpPortStatsLeaveEmptyTransmitted
   alaGvrpPortStatsLeaveAllTransmitted
   dot1qPortGvrpFailedRegistrations
   alaGvrpPortStatsTotalPDUReceived
   alaGvrpPortStatsTotalPDUTransmitted
   alaGvrpPortStatsInvalidMsgsReceived
   alaGvrpPortStatsTotalMsgsReceived
   alaGvrpPortStatsTotalMsgsTransmitted
```

show gvrp last-pdu-origin

Displays the source MAC address of the last GVRP message received on a specific port or an aggregate of ports.

show gvrp last-pdu-origin {linkagg *agg_num* | **port** *slot/port***}**

Syntax Definitions

agg_num	The number corresponding to the aggregate group.
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).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show gvrp last-pdu-origin port 1/21
Last-PDU Origin : 00:d0:95:ee:f4:64
```

output definitions

Last-PDU Origin	The source MAC address of the last PDU message received on the specific port.

Release History

Release 6.2.1; command was introduced.

Related Commands

N/A

MIB Objects

```
Dot1qPortvlantable
   dot1qPortGvrpLastPduOrigin
```

show gvrp configuration

Displays the global configuration for GVRP.

show gvrp configuration

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show gvrp configuration
GVRP Enabled                    : yes,
Transparent Switching Enabled   : no,
Maximum VLAN Limit              : 256
```

output definitions

GVRP Enabled	Indicates whether or not GVRP is globally enabled.
Transparent Switching Enabled	Indicates whether transparent switching is enabled (**Yes**) or disabled (**No**). When enabled, GVRP messages are flooded even if GVRP is disabled for the switch.
Maximum VLAN Limit	The maximum number of VLANs that can be learned by GVRP in the system.

Release History

Release 6.2.1; command was introduced.

Related Commands

gvrp	Enables GVRP on the device globally.
gvrp transparent switching	Enables transparent switching on the device.
gvrp maximum vlan	Configures the maximum number of dynamic VLANs that can be learned by GVRP.

MIB Objects

```
dot1qGvrpStatus
alaGvrpTransparentSwitching
alaGvrpMaxVlanLimit
```

show gvrp configuration port

Displays the GVRP configuration status for all the ports.

show gvrp configuration port

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show gvrp configuration port
  Port     GVRP Status
--------+---------------
   1/1     Disabled
   1/2     Disabled
   1/3     Disabled
   1/4     Disabled
   1/5     Disabled
   1/6     Disabled
   1/7     Disabled
   1/8     Disabled
   1/9     Enabled
   1/10    Disabled
   1/11    Disabled
   1/12    Disabled
   1/13    Disabled
   1/14    Disabled
   1/15    Disabled
   1/16    Disabled
   1/17    Disabled
   1/18    Disabled
   1/19    Disabled
   1/20    Disabled
   1/21    Enabled
   1/22    Disabled
   1/23    Disabled
   1/24    Disabled
   1/25    Disabled
   1/26    Disabled
   1/27    Disabled
   1/28    Disabled
```

```
1/29    Disabled
1/30    Disabled
1/31    Enabled
1/32    Disabled
1/33    Disabled
1/34    Disabled
1/35    Disabled
1/36    Disabled
1/37    Disabled
1/38    Disabled
1/39    Disabled
1/40    Disabled
1/41    Disabled
1/42    Disabled
1/43    Disabled
1/44    Disabled
1/45    Disabled
1/46    Disabled
1/47    Disabled
1/48    Disabled
1/49    Disabled
1/50    Disabled
```

output definitions

Port	Displays the slot/port number.
GVRP Status	Indicates if GVRP is **Enabled** or **Disabled** on the port.

Release History

Release 6.2.1; command was introduced.

Related Commands

gvrp port	Enables GVRP on a specific port or an aggregate of ports on the switch.
show gvrp configuration linkagg/port	Displays the GVRP configuration for a specific port or an aggregate of ports.

MIB Objects

```
Dot1qportvlantable
   dot1qPortGvrpStatus
```

show gvrp configuration linkagg/port

Displays the GVRP configuration for a specific port or an aggregate of ports.

show gvrp configuration {linkagg *agg_num* | **port** *slot/port***}**

Syntax Definitions

agg_num	The number corresponding to the aggregate group.
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).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show gvrp configuration port 1/21
Port 1/21:
  GVRP Enabled          : yes,
  Registrar Mode        : normal,
  Applicant Mode        : participant,
  Join Timer (msec)     : 600,
  Leave Timer (msec)    : 1800,
  LeaveAll Timer (msec) : 30000,
  Legacy Bpdu           : disabled

VLAN Memberships:
VLAN Id           Static        Restricted      Restricted
                Registration    Registration    Applicant
---------------+---------------+---------------+-----------
      1          LEARN           FALSE           FALSE
      2          LEARN           FALSE           FALSE
     11          LEARN           FALSE           FALSE
     12          LEARN           FALSE           FALSE
     13          LEARN           FALSE           FALSE
     14          LEARN           FALSE           FALSE
     15          LEARN           FALSE           FALSE
     16          LEARN           FALSE           FALSE
     17          LEARN           FALSE           FALSE
     18          LEARN           FALSE           FALSE
     19          LEARN           FALSE           FALSE
     20          LEARN           FALSE           FALSE
     51          RESTRICT        FALSE           FALSE
     52          RESTRICT        FALSE           FALSE
```

```
53          LEARN           TRUE            FALSE
54          LEARN           TRUE            FALSE
55          LEARN           FALSE           TRUE
56          LEARN           FALSE           TRUE
57          LEARN           FALSE           FALSE
58          LEARN           FALSE           FALSE
59          LEARN           FALSE           FALSE
60          LEARN           FALSE           FALSE
```

output definitions

GVRP Enabled	Indicates whether or not GVRP is globally enabled (**Yes** or **No**).
Registrar Mode	Indicates the registrar mode (**NORMAL**, **FIXED**, or **FORBIDDEN**) of the port.
Applicant Mode	Indicates the applicant mode (**PARTICIPANT, NON-PARTICIPANT**, or **ACTIVE**) of the port.
Join Timer	Displays the Join timer value.
Leave Timer	Displays the Leave timer value.
LeaveAll Timer	Displays the LeaveAll timer value.
Legacy Bpdu	Indicates the status of conventional/customer BPDU processing on network ports (**ENABLED** or **DISABLED**).
VLAN Id	The numerical VLAN ID.
Static Registration	Indicates if the port is restricted (**RESTRICT**) or not restricted (**LEARN**) from becoming a member of the static VLAN.
Restricted Registration	Indicates if the VLAN is restricted (**TRUE**) or not restricted (**FALSE**) from dynamic registration on the port.
Restricted Applicant	Indicates if the restricted applicant mode is enabled (**TRUE**) or not (**FALSE**).

Release History

Release 6.2.1; command was introduced.

Related Commands

gvrp port	Enables GVRP on a specific port or an aggregate of ports on the switch.
gvrp registration	Configures the GVRP registration mode for a specific port or an aggregate of ports.
gvrp applicant	Configures the applicant mode of a specific port or an aggregate of ports on the switch.
gvrp timer	Configures the Join, Leave, or LeaveAll timer values for the switch ports.
gvrp restrict-vlan-registration	Restricts GVRP processing from dynamically registering the specified VLAN(s) on the switch.
gvrp restrict-vlan-advertisement	Restricts the advertisement of VLANs on a specific port or an aggregate of ports.
gvrp static-vlan restrict	Restricts a port from becoming a member of a statically created VLAN or a range of VLANs.
show gvrp configuration port	Displays the GVRP configuration status for all the ports.

MIB Objects

```
Dot1qportvlantable
   dot1qPortGvrpLastPduOrigin
   dot1qPortGvrpStatus
alaGvrpPortConfigTable
   alaGvrpPortConfigRegistrarMode
   alaGvrpPortConfigApplicantMode
   alaGvrpPortConfigJoinTimer
   alaGvrpPortConfigLeaveTimer
   alaGvrpPortConfigLeaveAllTimer
   alaGvrpPortConfigRestrictedRegistrationBitmap
   alaGvrpPortConfigRegistrationToStaticVlan
   alaGvrpPortConfigPropagateDynamicNonGvrpVlan
```

show gvrp timer

Displays the timer values configured for all the ports or a specific port.

show gvrp timer [[join | leave | leaveall] {linkagg *agg_num* | **port** *slot/port***}]**

Syntax Definitions

join	Displays the Join timer value.
leave	Displays the Leave timer value.
leaveall	Displays the LeaveAll timer value.
agg_num	The number corresponding to the aggregate group.
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).

Defaults

By default the timer values configured on all the ports are displayed.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **join**, **leave**, or **leaveall** parameter with this command to view the specific timer values configured on all the ports.
- Use the *agg_num* or *slot/port* parameter with this command to display the timer values configured for a specific port.

Examples

```
-> show gvrp timer
Legend : All timer values are in milliseconds
  Port     Join Timer    Leave Timer    LeaveAll Timer
--------+-------------+-------------+--------------
   1/1     600           1800           30000
   1/2     600           1800           30000
   1/3     600           1800           30000
   1/4     600           1800           30000
   1/5     600           1800           30000
   1/6     600           1800           30000
   1/7     600           1800           30000
   1/8     600           1800           30000
   1/9     600           1800           30000
   1/10    600           1800           30000
   1/11    600           1800           30000
   1/12    600           1800           30000
   1/13    600           1800           30000
   1/14    600           1800           30000
   1/15    600           1800           30000
```

```
   1/16    600           1800           30000
   1/17    600           1800           30000
   1/18    600           1800           30000
   1/19    600           1800           30000
   1/20    600           1800           30000
   1/21    600           1800           30000
   1/22    600           1800           30000
   1/23    600           1800           30000
   1/24    600           1800           30000
   1/25    600           1800           30000
   1/26    600           1800           30000
   1/27    600           1800           30000
   1/28    600           1800           30000
   1/29    600           1800           30000
   1/30    600           1800           30000
   1/31    600           1800           30000
   1/32    600           1800           30000
   1/33    600           1800           30000
   1/34    600           1800           30000
   1/35    600           1800           30000
   1/36    600           1800           30000
   1/37    600           1800           30000
   1/38    600           1800           30000
   1/39    600           1800           30000
   1/40    600           1800           30000
   1/41    600           1800           30000
   1/42    600           1800           30000
   1/43    600           1800           30000
   1/44    600           1800           30000
   1/45    600           1800           30000
   1/46    600           1800           30000
   1/47    600           1800           30000
   1/48    600           1800           30000
   1/49    600           1800           30000
   1/50    600           1800           30000

-> show gvrp timer port 1/21
Join Timer (msec)     : 600,
Leave Timer (msec)    : 1800,
LeaveAll Timer (msec) : 30000

-> show gvrp timer join port 1/21
Join Timer (msec) : 600

-> show gvrp timer leave port 1/21
Leave Timer (msec) : 1800

-> show gvrp timer leaveall port 1/21
LeaveAll Timer (msec) : 30000


-> show gvrp timer join
Legend : All timer values are in milliseconds
  Port     Join Timer
--------+----------------
   1/1     600
   1/2     600
   1/3     600
```

```
   1/4     600
   1/5     600
   1/6     600
   1/7     600
   1/8     600
   1/9     600
   1/10    600
   1/11    600
   1/12    600
   1/13    600
   1/14    600
   1/15    600
   1/16    600
   1/17    600
   1/18    600
   1/19    600
   1/20    600
   1/21    600
   1/22    600
   1/23    600
   1/24    600
   1/25    600
   1/26    600
   1/27    600
   1/28    600
   1/29    600
   1/30    600
   1/31    600
   1/32    600
   1/33    600
   1/34    600
   1/35    600
   1/36    600
   1/37    600
   1/38    600
   1/39    600
   1/40    600
   1/41    600
   1/42    600
   1/43    600
   1/44    600
   1/45    600
   1/46    600
   1/47    600
   1/48    600
   1/49    600
   1/50    600

-> show gvrp timer leave
Legend : All timer values are in milliseconds
  Port     Leave Timer
--------+----------------
   1/1     1800
   1/2     1800
   1/3     1800
   1/4     1800
   1/5     1800
   1/6     1800
```

```
   1/7     1800
   1/8     1800
   1/9     1800
   1/10    1800
   1/11    1800
   1/12    1800
   1/13    1800
   1/14    1800
   1/15    1800
   1/16    1800
   1/17    1800
   1/18    1800
   1/19    1800
   1/20    1800
   1/21    1800
   1/22    1800
   1/23    1800
   1/24    1800
   1/25    1800
   1/26    1800
   1/27    1800
   1/28    1800
   1/29    1800
   1/30    1800
   1/31    1800
   1/32    1800
   1/33    1800
   1/34    1800
   1/35    1800
   1/36    1800
   1/37    1800
   1/38    1800
   1/39    1800
   1/40    1800
   1/41    1800
   1/42    1800
   1/43    1800
   1/44    1800
   1/45    1800
   1/46    1800
   1/47    1800
   1/48    1800
   1/49    1800
   1/50    1800

-> show gvrp timer leaveall
Legend : All timer values are in milliseconds
  Port     LeaveAll Timer
--------+----------------
   1/1     30000
   1/2     30000
   1/3     30000
   1/4     30000
   1/5     30000
   1/6     30000
   1/7     30000
   1/8     30000
   1/9     30000
```

```
1/10    30000
1/11    30000
1/12    30000
1/13    30000
1/14    30000
1/15    30000
1/16    30000
1/17    30000
1/18    30000
1/19    30000
1/20    30000
1/21    30000
1/22    30000
1/23    30000
1/24    30000
1/25    30000
1/26    30000
1/27    30000
1/28    30000
1/29    30000
1/30    30000
1/31    30000
1/32    30000
1/33    30000
1/34    30000
1/35    30000
1/36    30000
1/37    30000
1/38    30000
1/39    30000
1/40    30000
1/41    30000
1/42    30000
1/43    30000
1/44    30000
1/45    30000
1/46    30000
1/47    30000
1/48    30000
1/49    30000
1/50    30000
```

output definitions

Port	Displays the slot/port number.
Join Timer	Displays the Join timer value in milliseconds.
Leave Timer	Displays the Leave timer value in milliseconds.
LeaveAll Timer	Displays the LeaveAll timer value in milliseconds.

Release History

Release 6.2.1; command was introduced.

Related Commands

gvrp timer	Configures the Join, Leave, or LeaveAll timer values for the switch ports.

MIB Objects

```
alaGvrpPortConfigTable
   alaGvrpPortConfigJoinTimer
   alaGvrpPortConfigLeaveTimer
   alaGvrpPortConfigLeaveAllTimer
```

15 MVRP Commands

MVRP (Multiple VLAN Registration Protocol) provides a mechanism for maintaining the contents of Dynamic VLAN Registration Entries for each VLAN, and for propagating the information they contain to other Bridges. MVRP uses MRP (Multiple Registration Protocol) as the underlying mechanism, for the maintenance and propagation of the VLAN information.

MVRP acts as an MRP application, sending and receiving MVRP information encapsulated in an Ethernet frame on a specific MAC address. MVRP allows both end stations and Bridges in a Bridged Local Area Network to issue and revoke declarations relating to membership of VLANs. Note that if MVRP is configured on a switch, GVRP cannot be configured on that switch.

A summary of the available commands is listed here:

vlan registration-mode
mvrp
mvrp port
mvrp linkagg
mvrp transparent-switching
mvrp maximum vlan
mvrp registration
mvrp applicant
mvrp timer join
mvrp timer leave
mvrp timer leaveall
mvrp timer periodic-timer
mvrp periodic-transmission
mvrp restrict-vlan-registration
mvrp restrict-vlan-advertisement
mvrp static-vlan-restrict
show mvrp configuration
show mvrp port
show mvrp linkagg
show mvrp timer
show mvrp statistics
show mvrp last-pdu-origin
show vlan registration-mode
show mvrp vlan-restrictions
show vlan mvrp
mvrp clear-statistics

vlan registration-mode

Configures VLAN dynamic registration mode to either GVRP or MVRP and deletes all static configuration of previous mode along with the dynamic data.

vlan registration-mode {gvrp | mvrp}

Syntax Definitions

gvrp	Dynamic registration protocol mode is GVRP.
mvrp	Dynamic registration protocol mode is MVRP.

Defaults

parameter	default
gvrp| mvrp	**mvrp**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Before configuring MVRP, change the VLAN registration mode to MVRP.
- When the mode is changed from MVRP to GVRP or GVRP to MVRP, all static and dynamic configurations of the previous mode is deleted.
- An INFO message “All [GVRP/MVRP] static and dynamic configurations has been deleted” is given to the user on changing the mode from GVRP to MVRP.
- On configuring the same mode, no INFO message is given to the user.
- While running in MVRP mode, all GVRP configurations is rejected and when in GVRP mode, all MVRP configuration is rejected.
- Even though the default mode of the switch is MVRP, when you are upgrading the image from a previous release which does not support MVRP, the GVRP commands is accepted by the switch. The VLAN registration mode is internally changed to GVRP.

Examples

```
-> vlan registration-mode mvrp
INFO: All GVRP configurations and learnings have been deleted.

-> vlan registration-mode gvrp
INFO: All MVRP configurations and learnings have been deleted.
```

Release History

Release 6.4.3; command was introduced.

Related Commands

show vlan registration-mode	Displays the VLAN registration operational mode.

MIB Objects

```
alaVlanRegistrationProtocolType
```

mvrp

Enables or disables MVRP globally on the switch.

mvrp {enable | disable}

Syntax Definitions

enable	Enables MVRP globally on the switch.
disable	Disables MVRP globally on the switch.

Defaults

By default, MVRP is disabled on the switch.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Disabling MVRP globally will delete all the MVRP learned VLANs.
- MVRP is supported only when the switch is operating in the flat Spanning Tree mode and it is not supported in the 1x1 mode.

Examples

```
-> mvrp enable
-> mvrp disable
```

Release History

Release 6.4.3; command was introduced.

Related Commands

vlan registration-mode	Configures VLAN dynamic registration mode to either GVRP or MVRP and deletes all static configuration of previous mode along with the dynamic data.
show mvrp configuration	Displays the global configuration for MVRP.

MIB Objects

`alaMvrpGlobalStatus`

mvrp port

Enables or disables MVRP on specific ports on the switch.

mvrp port *slot/port* **[–** *port2***] {enable | disable}**

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (For example, 3/1 specifies port 1 on slot 3).
enable	Enables MVRP on a port.
disable	Disables MVRP on a port.

Defaults

By default, mvrp is disabled on all the ports.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- MVRP can be enabled on switch ports regardless of whether it is globally enabled on the switch. However, for the port to become an active participant in the MVRP operation, MVRP has to be enabled globally on the switch.
- When MVRP is globally enabled on the switch and is not enabled on the port, that port is excluded from the MVRP protocol operation.
- MVRP can be enabled only on fixed ports, 802.1 Q ports, aggregate ports, and VLAN Stacking Network ports. Other ports (mirroring ports, aggregable ports, mobile ports, VPLS Access ports, VLAN Stacking User ports) do not support MVRP.
- MVRP should not be enabled on ERP ring ports.

Examples

```
-> mvrp port 1/2 enable
-> mvrp port 1/2 disable
-> mvrp port 1/1-10 enable
-> mvrp port 1/1-10 disable
```

Release History

Release 6.4.3; command was introduced.

Related Commands

show mvrp port	Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.
show mvrp statistics	Displays the MVRP statistics for all the ports, aggregates, or specific ports.

MIB Objects

```
alaMvrpPortConfigTable
   alaMvrpPortStatus
```

mvrp linkagg

Enables or disables MVRP on specific aggregates on the switch.

mvrp linkagg *agg_num* **[-***agg_num2***] {enable | disable}**

Syntax Definitions

agg_num	The number corresponding to the aggregate group.
enable	Enables MVRP on a port.
disable	Disables MVRP on a port.

Defaults

By default, mvrp is disabled on all the ports.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- MVRP can be enabled on switch ports regardless of whether it is globally enabled on the switch. However, for the port to become an active participant in the MVRP operation, MVRP has to be enabled globally on the switch.
- When MVRP is globally enabled on the switch and is not enabled on the port, that port is excluded from the MVRP protocol operation.
- MVRP can be enabled only on fixed ports, 802.1 Q ports, aggregate ports, and VLAN Stacking Network ports. Other ports (mirroring ports, aggregable ports, mobile ports, VPLS Access ports, VLAN Stacking User ports) do not support MVRP.
- To use the *agg_num* parameter, the link aggregate group has to be created.
- MVRP not supported on VFL aggregate. If mvrp is configured on a vfl linkagg, an error message is displayed informing that the port is an VFL aggregate.

Examples

```
-> mvrp linkagg 10 enable
-> mvrp linkagg 10 disable
-> mvrp linkagg 2-5 enable
-> mvrp linkagg 1-5 disable
```

Release History

Release 6.4.3; command was introduced.

Related Commands

show mvrp port	Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.
show mvrp statistics	Displays the MVRP statistics for all the ports, aggregates, or specific ports.

MIB Objects

```
alaMvrpPortConfigTable
   alaMvrpPortStatus
```

mvrp transparent-switching

Enables or disables transparent switching on the switch. When transparent switching is enabled, the switch propagates MVRP information to other switches but does not participate in the MVRP protocol.

mvrp transparent-switching {enable | disable}

Syntax Definitions

enable	Enables transparent switching globally on a switch.
disable	Disables transparent switching globally on a switch.

Defaults

By default, transparent switching is disabled on the switch.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- If MVRP is globally disabled and transparent switching is enabled, the switch floods the MVRP messages.
- If MVRP is globally disabled and transparent switching is disabled, the switch discards the MVRP messages.
- If MVRP is globally enabled, transparent switching has no effect on the functional behavior of the switch.

Examples

```
-> mvrp transparent-switching enable
-> mvrp transparent-switching disable
```

Release History

Release 6.4.3; command was introduced.

Related Commands

show mvrp configuration	Displays the global configuration for MVRP.

MIB Objects

```
alaMvrpTransparentSwitching
```

mvrp maximum vlan

Configures the maximum number of dynamic VLANs that can be created by MVRP.

mvrp maximum vlan *vlanlimit*

Syntax Definitions

vlanlimit	The maximum number of VLANs to be created by MVRP. The valid range is 32–4094.

Defaults

The default value is 256.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- This command can be used even when MVRP is not enabled on the switch. However, MVRP has to be enabled on the switch for creating dynamic VLANs.
- If the VLAN limit to be set is less than the current number of dynamically learnt VLANs, then the new configuration takes effect only after the MVRP is disabled and enabled again on the switch. If this operation is not done, the VLANs learnt earlier is retained.

Examples

```
-> mvrp maximum vlan 100
```

Release History

Release 6.4.3; command was introduced.

Related Commands

show mvrp configuration	Displays the global configuration for MVRP.
show vlan mvrp	Displays the list of VLANS learned through MVRP and their details.

MIB Objects

```
alaMvrpMaxVlanLimit
```

mvrp registration

Configures the MVRP registration mode for specific ports or aggregates.

mvrp {port *slot/port* **[–** *port2***] | linkagg** *agg_num* **[-***agg_num2***]} registration {normal | fixed | forbidden}**

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (For example, 3/1 specifies port 1 on slot 3).
agg_num	The number corresponding to the aggregate group.
normal	Specifies that both registration and de-registration of VLANs are allowed. VLANs can be mapped either dynamically (through MVRP) or statically (through management application) on such a port.
fixed	Specifies that only static mapping of VLANs is allowed on the port but de-registration of previously created dynamic or static VLANs is not allowed.
forbidden	Specifies that dynamic VLAN registration or de-registration is not allowed on the port. Any dynamic VLAN created earlier is deregistered.

Defaults

parameter	default
normal | fixed | forbidden	**normal**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

To use the *agg_num* parameter, the link aggregate group has to be created and enabled.

Examples

```
-> mvrp port 1/2 registration forbidden
-> mvrp port 1/5 registration normal
-> mvrp linkagg 10 registration fixed
-> mvrp linkagg 20 registration forbidden
-> mvrp port 2/5-10 registration normal
```

Release History

Release 6.4.3; command was introduced.

Related Commands

show mvrp port	Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.
show mvrp linkagg	Displays the MVRP configurations for all the link aggregates, including timer values, registration and applicant modes.

MIB Objects

```
alaMvrpPortConfigTable
   alaMvrpPortConfigRegistrarMode
```

mvrp applicant

Configures the applicant mode of specific ports on the switch. The applicant mode determines whether MVRP PDU exchanges are allowed on a port depending on the Spanning Tree state of the port.

mvrp {port *slot/port* **[–** *port2***] | linkagg** *agg_num* **[-***agg_num2***]} applicant {participant | non-participant | active}**

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (For example, 3/1 specifies port 1 on slot 3).
agg_num	The number corresponding to the aggregate group.
participant	Specifies that MVRP PDU exchanges are only allowed when the port is in the STP forwarding state.
non-participant	Specifies that MVRP PDU's are not sent in this mode and PDU's received are processed and learning happens as expected.
active	Specifies that MVRP PDU exchanges are allowed when the port is in the STP forwarding state or STP blocking state.This is applicable for both advertisement and registration.

Defaults

parameter	default
participant | non-participant | active	**active**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

To use the *agg_num* parameter, the link aggregate group has to be created and enabled.

Examples

```
-> mvrp port 1/2 applicant active
-> mvrp port 1/3 applicant participant
-> mvrp port 1/4 applicant non-participant
-> mvrp linkagg 10 applicant active
-> mvrp linkagg 15 applicant participant
-> mvrp linkagg 20 applicant non-participant
```

Release History

Release 6.4.3; command was introduced.

Related Commands

show mvrp port	Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.
show mvrp linkagg	Displays the MVRP configurations for all the link aggregates, including timer values, registration and applicant modes.

MIB Objects

```
alaMvrpPortConfigtable
   alaMvrpPortConfigApplicantMode
```

mvrp timer join

Specifies the join time interval between transmit opportunities for the dynamically registering VLANs on the switch.

mvrp {port *slot/port* **[–** *port2***] | linkagg** *agg_num* **[-***agg_num2***]} timer join** *timer-value*

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (For example, 3/1 specifies port 1 on slot 3).
agg_num	The number corresponding to the aggregate group.
timer-value	Specifies the value of the join timer in milliseconds.The valid range is 250 milliseconds to 1073741773 milliseconds.

Defaults

parameter	default
timer-value	*600 milliseconds*

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use default timer settings unless there is a compelling reason to change the settings. Modifying timers to inappropriate values might cause an imbalance in the operation of MVRP.
- To use the *agg_num* parameter, the link aggregate group has to be created and enabled.

Examples

```
-> mvrp port 1/2 timer join 600
-> mvrp port 1/2-12 timer join 600
-> mvrp linkagg 3 timer join 600
-> mvrp linkagg 3-6 timer join 600
```

Release History

Release 6.4.3; command was introduced.

Related Commands

show mvrp timer	Displays the timer values configured for all the ports or a specific port.
show mvrp port	Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.

MIB Objects

```
alaMvrpPortConfigTable
   alaMvrpPortConfigJoinTimer
   alaMvrpPortConfigLeaveTimer
   alaMvrpPortConfigLeaveAllTimer
   alaMvrpPortConfigPeriodicTimer
```

mvrp timer leave

Specifies the period of time that the switch has to wait in the Leave state before changing to the unregistered state.

mvrp {port *slot/port* **[–** *port2***] | linkagg** *agg_num* **[-***agg_num2***]} timer leave** *timer-value*

Syntax Definitions

slot	The slot number for the module.
port	The physical port number on the module.
agg_num	The number corresponding to the aggregate group.
timer-value	Specifies the value of the Leave Timer in milliseconds. The valid range is 750 milliseconds to 2147483647 milliseconds.

Defaults

parameter	default
timer-value	*1800 milliseconds*

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use default timer settings unless there is a compelling reason to change the settings. Modifying timers to inappropriate values might cause an imbalance in the operation of MVRP.
- Leave timer value has to be greater than or equal to twice the Join timer value, plus six times the timer resolution (that is, 16.66 milliseconds). Leave timer has to be at least be greater than twice the join timer plus100 milliseconds.
- To use the *agg_num* parameter, the link aggregate group has to be created and enabled.

Examples

```
-> mvrp port 1/2 timer leave 1800
-> mvrp port 1/2-12 timer leave 1800
-> mvrp linkagg 3 timer leave 1800
-> mvrp linkagg 3-6 timer leave 1800
```

Release History

Release 6.4.3; command was introduced.

Related Commands

show mvrp timer	Displays the timer values configured for all the ports or a specific port.
show mvrp port	Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.

MIB Objects

```
alaMvrpPortConfigTable
   alaMvrpPortConfigJoinTimer
   alaMvrpPortConfigLeaveTimer
   alaMvrpPortConfigLeaveAllTimer
   alaMvrpPortConfigPeriodicTime
```

mvrp timer leaveall

Specifies the frequency with which the LeaveAll messages are communicated.

mvrp {port *slot/port* **[–** *port2***] | linkagg** *agg_num* **[-***agg_num2***]} timer leaveall** *timer-value*

Syntax Definitions

slot	The slot number for the module.
port	The physical port number on the module.
agg_num	The number corresponding to the aggregate group.
timer-value	Specifies the value of the LeaveAll Timer in milliseconds. The valid range is 750 milliseconds to 2147483647 milliseconds.

Defaults

parameter	default
timer-value	*30000 milliseconds*

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use default timer settings unless there is a compelling reason to change the settings. Modifying timers to inappropriate values might cause an imbalance in the operation of MVRP.
- Leaveall timer value has to be greater than or equal to the Leave timer value. It is recommended to have the leaveall timer 15 times greater than the leave timer.
- To use the *agg_num* parameter, the link aggregate group has to be created and enabled.

Examples

```
-> mvrp port 1/2 timer leaveall 30000
-> mvrp port 1/2-12 timer leaveall 30000
-> mvrp linkagg 3 timer leaveall 30000
-> mvrp linkagg 3-6 timer leaveall 30000
```

Release History

Release 6.4.3; command was introduced.

Related Commands

show mvrp timer	Displays the timer values configured for all the ports or a specific port.
show mvrp port	Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.

MIB Objects

```
alaMvrpPortConfigTable
   alaMvrpPortConfigJoinTimer
   alaMvrpPortConfigLeaveTimer
   alaMvrpPortConfigLeaveAllTimer
   alaMvrpPortConfigPeriodicTimer
```

mvrp timer periodic-timer

Specifies the MVRP periodic-timer time interval for the dynamically registering VLANs on the switch.

mvrp {port *slot/port* **[–** *port2***] | linkagg** *agg_num* **[-***agg_num2***]} timer periodic-timer** *timer-value*

Syntax Definitions

slot	The slot number for the module.
port	The physical port number on the module.
agg_num	The number corresponding to the aggregate group.
timer-value	Specifies the value of the Periodic Timer in seconds. The valid range is between 1 to 2147483647 milliseconds.

Defaults

parameter	default
timer-value	*1 second*

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use default timer settings unless there is a compelling reason to change the settings. Modifying timers to inappropriate values might cause an imbalance in the operation of MVRP.
- To use the *agg_num* parameter, the link aggregate group has to be created and enabled.

Examples

```
-> mvrp port 1/2 timer periodic-timer 1
-> mvrp port 1/2 timer periodic-timer 1
-> mvrp linkagg 3 timer periodic-timer 1
-> mvrp linkagg 3-6 timer periodic-timer 1
```

Release History

Release 6.4.3; command was introduced.

Related Commands

show mvrp timer	Displays the timer values configured for all the ports or a specific port.
show mvrp port	Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.

MIB Objects

```
alaMvrpPortConfigTable
   alaMvrpPortConfigJoinTimer
   alaMvrpPortConfigLeaveTimer
   alaMvrpPortConfigLeaveAllTimer
   alaMvrpPortConfigPeriodicTimer
```

mvrp periodic-transmission

Enables the periodic transmission status on a port or aggregate of ports.

mvrp {port *slot/port* **[–** *port2***] | linkagg** *agg_num* **[-***agg_num2***]} periodic-transmission {enable|disable}**

Syntax Definitions

slot	The slot number for the module.
port	The physical port number on the module.
agg_num	The number corresponding to the aggregate group.
enable	Enables periodic transmission status on a port.
disable	Disables periodic transmission status on a port.

Defaults

By default, periodic-transmission status would be disabled on all the ports.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

To use the *agg_num* parameter, the link aggregate group has to be created and enabled.

Examples

```
-> mvrp port 1/2 periodic-transmission enable
-> mvrp port 1/2 periodic-transmission disable
-> mvrp linkagg 10 periodic-transmission enable
-> mvrp linkagg 10 periodic-transmission disable
```

Release History

Release 6.4.3; command was introduced.

Related Commands

show mvrp port	Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.
show mvrp linkagg	Displays the MVRP configurations for all link aggregates, including timer values, registration and applicant modes.

MIB Objects

```
alaMvrpPortConfigTable
   alaMvrpPortConfigPeriodicTransmissionStatus
```

mvrp restrict-vlan-registration

Restricts MVRP processing from dynamically registering the specified VLAN or VLANs on the switch.

mvrp {port *slot/port* **[–** *port2***] | linkagg** *agg_num* **[-***agg_num2***]} restrict-vlan-registration vlan** *vlan-list*

no mvrp {port *slot/port* **[–** *port2***] | linkagg** *agg_num* **[-***agg_num2***]} restrict-vlan-registration vlan** *vlan-list*

Syntax Definitions

slot	The slot number for the module.
port	The physical port number on the module.
agg_num	The number corresponding to the aggregate group.
vlan-list	The VLAN ID or the VLAN ID range (For example, 1-10).

Defaults

By default, MVRP dynamic VLAN registrations are not restricted.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to allow registration of dynamic VLAN IDs through MVRP processing.
- If the specified VLAN exists on the switch, the VLAN is mapped to the receiving port.
- To use the *agg_num* parameter, the link aggregate group has to be created and enabled.

Examples

```
-> mvrp port 1/2 restrict-vlan-registration vlan 5
-> no mvrp port 1/2 restrict-vlan-registration vlan 5
-> mvrp linkagg 10 restrict-vlan-registration vlan 6-10
-> no mvrp port 3/1 restrict-vlan-registration vlan 6-10
```

Release History

Release 6.4.3; command was introduced.

Related Commands

show mvrp port	Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.
show mvrp linkagg	Displays the MVRP configurations for all link aggregates, including timer values, registration and applicant modes.

MIB Objects

```
alaMvrpPortRestrictVlanConfigTable
   alaMvrpPortRestrictRowStatus
   alaMvrpPortRestrictVlanAttributeType
   alaMvrpPortRestrictVlanID
```

mvrp restrict-vlan-advertisement

Restricts the advertisement of VLANs on a specific port or an aggregate of ports.

mvrp {port *slot/port* **[–***port2***] | linkagg** *agg_num* **[-***agg_num2***]} restrict-vlan-advertisement**

vlan *vlan-list*

no mvrp {| port *slot/port* **[–***port2***] | linkagg** *agg_num* **[-***agg_num2***]} restrict-vlan-advertisement**

vlan *vlan-list*

Syntax Definitions

slot	The slot number for the module.
port	The physical port number on the module.
agg_num	The number corresponding to the aggregate group.
vlan_list	The list of VLAN IDs or the VLAN ID range (For example, 1-10).

Defaults

By default, MVRP VLAN advertisement is not restricted.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- This command affects the MVRP processing only if the applicant mode is set to participant or active.
- Use the **no** form of this command to allow the propagation of VLANs.
- To use the *agg_num* parameter, the link aggregate group has to be created and enabled.

Examples

```
-> mvrp port 1/2 restrict-vlan-advertisement vlan 5
-> no mvrp port 1/2 restrict-vlan-advertisement vlan 5
-> mvrp linkagg 10 restrict-vlan-advertisement vlan 6-10
-> no mvrp port 1/2 restrict-vlan-advertisement vlan 6-10
-> no mvrp port 1/1-2 restrict-vlan-advertisement vlan 6-10
```

Release History

Release 6.4.3; command was introduced.

Related Commands

mvrp applicant	Configures the applicant mode of specific ports on the switch. The applicant mode determines whether MVRP PDU exchanges are allowed on a port depending on the Spanning Tree state of the port.
mvrp timer join	Configures the applicant mode of specific link aggregates on the switch. The applicant mode determines whether MVRP PDU exchanges are allowed on a port depending on the Spanning Tree state of the port.
show mvrp port	Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.
show mvrp linkagg	Displays the MVRP configurations for all the link aggregates, including timer values, registration and applicant modes.

MIB Objects

```
alaMvrpPortRestrictVlanConfigTable
   alaMvrpPortRestrictRowStatus
   alaMvrpPortRestrictVlanAttributeType
   alaMvrpPortRestrictVlanID
```

mvrp static-vlan-restrict

Restricts a port from becoming a member of a statically created VLAN or a range of VLANs.

mvrp {linkagg *agg_num* **[-***agg_num2***] | port** *slot/port* **[–** *port2***]} static-vlan-restrict vlan** *vlan-list*

no mvrp {linkagg *agg_num* **[-***agg_num2***] | port** *slot/port* **[–** *port2***]} static-vlan-restrict vlan** *vlan-list*

Syntax Definitions

agg_num	The number corresponding to the aggregate group.
slot	The slot number for the module.
port	The physical port number on the module.
vlan_list	The list of VLAN IDs or the VLAN ID range (For example, 1-10).

Defaults

By default, ports are assigned to the static VLAN based on MVRP PDU processing.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- This command applies only to static VLANs and does not apply to dynamic VLANs.
- Use the **no** form of this command to set the specified port and VLAN to the default value.
- Use the *agg_num* or *slot/port* parameter with this command to display GVRP statistics for a specific port.

Examples

```
-> mvrp port 1/2 static-vlan-restrict vlan 5
-> no mvrp port 1/2 static-vlan-restrict vlan 5
-> mvrp port 1/2 static-vlan-restrict vlan 6-9
-> no mvrp port 1/2 static-vlan-restrict vlan 6-9
-> mvrp linkagg 3 static-vlan-restrict vlan 4-5
-> no mvrp linkagg 3 static-vlan-restrict aggregate vlan 4-5
```

Release History

Release 6.4.3; command was introduced.

Related Commands

show mvrp port	Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.
show mvrp linkagg	Displays the MVRP configurations for all the link aggregates, including timer values, registration and applicant modes.

MIB Objects

```
alaMvrpPortRestrictVlanConfigTable
   alaMvrpPortRestrictRowStatus
   alaMvrpPortRestrictVlanAttributeType
   alaMvrpPortRestrictVlanID
   alaMvrpPortConfigRegistrationToStaticVlan
   alaMvrpPortConfigRegistrationToStaticVlanLearn
   alaMvrpPortConfigRegistrationToStaticVlanRestrict
```

show mvrp configuration

Displays the global configuration for MVRP.

show mvrp configuration

Syntax Definitions

NA

Defaults

NA

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

NA

Examples

```
-> show mvrp configuration
MVRP Enabled                  : yes,
Transparent Switching Enabled : no,
Maximum VLAN Limit            : 256
```

output definitions

MVRP Enabled	Indicates whether MVRP is globally enabled.
Transparent Switching Enabled	Indicates whether transparent switching is enabled (**Yes**) or disabled (**No**). When enabled, MVRP messages are flooded even if MVRP is disabled for the switch.
Maximum VLAN Limit	The maximum number of VLANs that can be learned by MVRP in the system.

Release History

Release 6.4.3; command was introduced.

Related Commands

mvrp	Enables or disables MVRP globally on the switch.
vlan registration-mode	Configures VLAN dynamic registration mode to either GVRP or MVRP and deletes all static configuration of previous mode along with the dynamic data.
mvrp port	Enables or disables transparent switching on the switch. When transparent switching is enabled, the switch propagates MVRP information to other switches but does not participate in the MVRP protocol.
mvrp maximum vlan	Configures the maximum number of dynamic VLANs that can be created by MVRP.

MIB Objects

```
alaMvrpGlobalStatus
alaMvrpTransparentSwitching
alaMvrpMaxVlanLimit
```

show mvrp port

Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.

show mvrp port {*slot/port* **[-***port2***]} [enabled | disabled]**

Syntax Definitions

slot	The slot number for the module.
port	The physical port number on the module.
enabled	To display only the enabled ports.
disabled	To display only the disabled ports.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show mvrp port enabled

Port  Join      Leave LeaveAll Periodic  Registration  Applicant          Periodic Tx Status
      Timer     Timer  Timer    Timer    Mode           Mode
      (msec)    (msec) (msec)   (sec)
----+----------+-----------+---------------+---------------+------------+-------
1/1    600    1800    30000   2     fixed        active          enabled
1/2   600    1800    30000   2     fixed        active          enabled
1/7   600    1800    30000   2     fixed        active          enabled
1/8   600    1800    30000   2     fixed        active          enabled
2/24  600    1800    30000   2     fixed        active          enabled

-> show mvrp port disabled
Port  Join      Leave LeaveAll Periodic  Registration  Applicant          Periodic Tx Status
      Timer     Timer  Timer    Timer    Mode           Mode
      (msec)    (msec) (msec)   (sec)
----+----------+-----------+---------------+---------------+------------+-------
1/9   600     1800  30000    2     fixed        active           enabled
1/10  600     1800  30000    2     fixed        active           enabled
2/1   600     1800  30000    2     fixed        active           enabled
2/2   600     1800  30000    2     fixed        active           enabled
….
2/24  600     1800 30000    2       fixed        active           enabled
```

```
-> show mvrp port

Port Status    Join      Leave LeaveAll Periodic  Registration  Applicant       Periodic
               Timer     Timer  Timer    Timer    Mode           Mode           Tx Status
               (msec)    (msec) (msec)   (sec)
----+----------+-----------+--------------+--------------+-----------+-------
1/1  disabled 600     1800  30000    2     fixed        participant  enabled
1/2  enabled  600     1800  30000    2     fixed        participant  enabled
1/3  enabled  600     1800  30000    2     fixed        active       enabled
1/4  enabled  600     1800  30000    2     fixed        active       enabled
2/24 enabled  600     1800  30000    2     fixed        active       enabled


-> show mvrp port 1/1-3

Port Status    Join      Leave LeaveAll Periodic  Registration  Applicant       Periodic
               Timer     Timer  Timer    Timer    Mode           Mode           Tx Status
               (msec)    (msec) (msec)   (sec)
----+----------+-----------+--------------+--------------+-----------+-------
1/1  disabled 600     1800  30000    2     fixed        participant  enabled
1/2  enabled  600     1800  30000    2     fixed        participant  enabled
1/3  enabled  600     1800  30000    2     fixed        participant  enabled

-> show mvrp port 1/1

MVRP Enabled : no,
Registrar Mode : normal,
Applicant Mode : participant,
Join Timer (msec) : 600,
Leave Timer (msec) : 1800,
LeaveAll Timer (msec) : 30000,
Periodic Timer (sec) : 1,
Periodic Tx Status : enabled

-> show mvrp port 1/1 enabled
ERROR: MVRP is disabled on port 1/1
```

output definitions

Port	Displays the slot/port number.
Join Timer	Displays the value of Join Timer in milliseconds.
Leave Timer	Displays the value of the Leave Timer in milliseconds.
LeaveALL Timer	Displays the value of the LeaveAll Timer in milliseconds.
Periodic Timer	Displays the value of the Periodic Timer in seconds.
Registration Mode	Indicates the registration mode of the port. • **Normal**: Registrar responds normally to incoming MRP messages. • **Fixed**: Registrar ignores all MRP messages and remains in the IN state for all the dynamic VLAN-port associations. • **Forbidden**: Registrar ignores all MRP messages and remains in MT State.

output definitions (continued)

Applicant Mode	Indicates the applicant mode of the port. • **Participant**: MVRP PDU exchanges are only allowed when the port is in the STP forwarding state. • **Non-participant**: MVRP PDU's are not sent in this mode and PDU's received are processed and learning happens as expected. • **Active**: MVRP PDU exchanges are allowed when the port is in the STP forwarding state or STP blocking state.
Periodic Tx Status	The transmission status of MVRP, **enabled** or **disabled**.

Release History

Release 6.4.3; command was introduced.

Related Commands

mvrp port	Enables or disables MVRP on specific ports on the switch.
mvrp transparent-switching	Enables or disables MVRP on specific aggregates on the switch
vlan registration-mode	Configures VLAN dynamic registration mode to either GVRP or MVRP and deletes all static configuration of previous mode along with the dynamic data.

MIB Objects

```
alaMvrpPortConfigTable
   alaMvrpPortStatus
   alaMvrpPortConfigRegistrarMode
   alaMvrpPortConfigApplicantMode
   alaMvrpPortConfigJoinTimer
   alaMvrpPortConfigLeaveTimer
   alaMvrpPortConfigLeaveAllTimer
   alaMvrpPortConfigPeriodicTimer
   alaMvrpPortConfigPeriodicTransmissionStatus
```

show mvrp linkagg

Displays the MVRP configurations for linkaggs, including timer values, registration and applicant modes.

show mvrp linkagg [*agg_num* **[-***agg_num2***]} [enabled | disabled]**

Syntax Definitions

agg_num	The number corresponding to the aggregate group.
enabled	To display only the enabled ports.
disabled	To display only the disabled ports.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show mvrp linkagg 1-3

Port Status    Join      Leave LeaveAll Periodic  Registration  Applicant       Periodic
               Timer     Timer  Timer    Timer    Mode           Mode           Tx Status
               (msec)    (msec) (msec)   (sec)
----+----------+-----------+--------------+---------------+------------+-------
0/1  enabled  600     1800  30000    2     fixed        participant  enabled
0/2  enabled  600     1800  30000    2     fixed        participant  enabled
0/3  enabled  600     1800  30000    2     fixed        participant  enabled

-> show mvrp linkagg 1
MVRP Enabled           : yes,
Registrar Mode         : normal,
Applicant Mode         : participant,
Join Timer (msec)      : 600,
Leave Timer (msec)     : 1800,
LeaveAll Timer (msec)  : 30000,
Periodic Timer (sec)   : 1,
Periodic Tx Status     : enabled

-> show mvrp linkagg 1 disabled
ERROR: MVRP is enabled on linkagg 0/1
```

Note. In the following command output, the MVRP status is not displayed as the command is only for enabled ports/linkagg.

```
-> show mvrp linkagg 10 enabled
Registrar Mode        : normal,
Applicant Mode        : participant,
Join Timer (msec)     : 600,
Leave Timer (msec)    : 1800,
LeaveAll Timer (msec) : 30000,
Periodic Timer (sec)  : 1,
Periodic Tx status    : disabled

-> show mvrp linkagg 128 disabled
ERROR: Port 0/128 is a VFL aggregate. MVRP not supported on VFL aggregate
```

output definitions

Port	Displays the slot/port number.
Join Timer	Displays the value of Join Timer in milliseconds.
Leave Timer	Displays the value of the Leave Timer in milliseconds.
LeaveALL Timer	Displays the value of the LeaveAll Timer in milliseconds.
Periodic Timer	Displays the value of the Periodic Timer in seconds.
Registration Mode	Indicates the registration mode of the port. • **Normal**: Registrar responds normally to incoming MRP messages. • **Fixed**: Registrar ignores all MRP messages and remains in the IN state for all the dynamic VLAN-port associations. • **Forbidden**: Registrar ignores all MRP messages and remains in MT State.
Applicant Mode	Indicates the applicant mode of the port. • **Participant**: MVRP PDU exchanges are only allowed when the port is in the STP forwarding state. • **Non-participant**: MVRP PDU's are not sent in this mode and PDU's received are processed and learning happens as expected. • **Active**: MVRP PDU exchanges are allowed when the port is in the STP forwarding state or STP blocking state.
Periodic Tx Status	The transmission status of MVRP, **enabled** or **disabled**.

Release History

Release 6.4.3; command was introduced.

Related Commands

mvrp port	Enables or disables MVRP on specific ports on the switch.
mvrp transparent-switching	Enables or disables MVRP on specific aggregates on the switch
vlan registration-mode	Configures VLAN dynamic registration mode to either GVRP or MVRP and deletes all static configuration of previous mode along with the dynamic data.

MIB Objects

```
alaMvrpPortConfigTable
   alaMvrpPortStatus
   alaMvrpPortConfigRegistrarMode
   alaMvrpPortConfigApplicantMode
   alaMvrpPortConfigJoinTimer
   alaMvrpPortConfigLeaveTimer
   alaMvrpPortConfigLeaveAllTimer
   alaMvrpPortConfigPeriodicTimer
   alaMvrpPortConfigPeriodicTransmissionStatus
```

show mvrp timer

Displays the timer values configured for all the ports or a specific port.

show mvrp {port *slot/port* **[–** *port2***] | linkagg** *agg_num* **[-***agg_num2***]} timer {join | leave | leaveall | periodic-timer}**

Syntax Definitions

slot	The slot number for the module.
port	The physical port number on the module.
agg_num	The number corresponding to the aggregate group.
join	To display only the join timer.
leave	To display only the leave timer.
leaveall	To display only the leaveall timer.
periodic-timer	To display only the periodic-timer.

Defaults

NA

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **join**, **leave**, **leaveall**, or **periodic-timer** parameter with this command to view the specific timer values configured on all the ports.
- Use the *agg_num* or *slot/port* parameter with this command to display the timer values configured for a specific port.

Examples

```
-> show mvrp timer
Port    Join Timer     Leave Timer    LeaveAll Timer   Periodic Timer
        (msec)         (msec)          (sec)             (msec)
--------+--------------+--------------+---------------+----------------
1/1      600            1800            30000             2
1/2      600            1800            30000             5
1/3      600            1800            30000             1
1/4      600            1800            30000             1
-> show mvrp port 1/21 timer
Join Timer (msec)      : 600,
Leave Timer (msec)     : 1800,
LeaveAll Timer (msec)  : 30000,
Periodic-Timer (sec)   : 1

-> show mvrp port 1/21 timer join
```

```
Join Timer (msec)      : 600

-> show mvrp port 1/21 timer leave
Leave Timer (msec)     : 1800

-> show mvrp port 1/21 timer leaveall
LeaveAll Timer (msec)  : 30000

-> show mvrp port 1/21 timer periodic-timer
Periodic-Timer (sec)   : 1

-> show mvrp timer join
Legend : All timer values are in milliseconds
Port      Join Timer
--------+----------------
1/1       600
1/2       600
1/3       600

-> show mvrp timer leaveall
Legend : All timer values are in milliseconds
Port     LeaveAll Timer
--------+----------------
1/1      1800
1/2      1800
1/3      1800

-> show mvrp timer leaveall
Legend : All timer values are in milliseconds
Port      LeaveAll Timer
--------+----------------
1/1       30000
1/2       30000
1/3       30000

-> show mvrp timer periodic-timer
Port      Periodic Timer
--------+----------------
1/1        1
1/2        1
1/3        1
```

output definitions

Port	Displays the slot/port number.
Join Timer	Displays the value of Join Timer in milliseconds.
Leave Timer	Displays the value of the Leave Timer in milliseconds.
LeaveALL Timer	Displays the value of the LeaveAll Timer in milliseconds.
Periodic Timer	Displays the value of the Periodic Timer in seconds.

Release History

Release 6.4.3; command was introduced.

Related Commands

mvrp timer join	Specifies the join time interval between transmit opportunities for the dynamically registering VLANs on the switch.
mvrp timer leave	Specifies the period of time that the switch has to wait in the Leave state before changing to the unregistered state.
mvrp timer leaveall	Specifies the frequency with which the LeaveAll messages are communicated.
mvrp timer periodic-timer	Specifies the MVRP periodic-timer time interval for the dynamically registering VLANs on the switch.
show mvrp port	Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.

MIB Objects

```
alaMvrpPortConfigTable
   alaMvrpPortConfigJoinTimer
   alaMvrpPortConfigLeaveTimer
   alaMvrpPortConfigLeaveAllTimer
   alaMvrpPortConfigPeriodicTimer
```

show mvrp statistics

Displays the MVRP statistics for all the ports, aggregates, or specific ports.

show mvrp {port *slot/port* **[–** *port2***] | linkagg** *agg_num* **[-***agg_num2***] } statistics**

Syntax Definitions

slot	The slot number for the module.
port	The physical port number on the module.
agg_num	The number corresponding to the aggregate group.

Defaults

NA

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- If no port or link aggregate is specified the MVRP statistics are displayed for all ports.
- Use the *agg_num* or *slot/port* parameter with this command to display the MVRP statistics for a specific port.

Examples

```
-> show mvrp port 1/21 statistics
Port 1/21:
New Received           : 0,
Join In Received       : 1526,
Join Empty Received    : 8290,
Leave Received         : 0,
In Received            : 1,
Empty Received         : 0,
Leave All Received     : 283,
New Transmitted        : 826,
Join In Transmitted    : 1532,
Jon Empty Transmitted  : 39,
Leave Transmitted      : 0,
In Transmitted         : 0,
Empty Transmitted      : 296,
LeaveAll Transmitted   : 23,
Failed Registrations   : 0,
Total Mrp PDU Received  : 1160,
Total Mrp PDU Transmitted : 957,
Total Mrp Msgs Received : 10100,
Total Mrp Msgs Transmitted : 2693,
Invalid Msgs Received  : 0
```

```
-> show mvrp statistics
Port 1/1:
New Received           : 0,
Join In Received       : 1526,
Join Empty Received    : 8290,
Leave Received         : 0,
In Received            : 1,
Empty Received         : 0,
Leave All Received     : 283,
New Transmitted        : 826,
Join In Transmitted    : 1532,
Jon Empty Transmitted  : 39,
Leave Transmitted      : 0,
In Transmitted         : 0,
Empty Transmitted      : 296,
LeaveAll Transmitted   : 23,
Failed Registrations   : 0,
Total Mrp PDU Received  : 1160,
Total Mrp PDU Transmitted : 957,
Total Mrp Msgs Received : 10100,
Total Mrp Msgs Transmitted : 2693,
Invalid Msgs Received  : 0

Port 1/2:
New Received           : 0,
Join In Received       : 1526,
Join Empty Received    : 8290,
Leave Received         : 0,
In Received            : 1,
Empty Received         : 0,
Leave All Received     : 283,
New Transmitted        : 826,
Join In Transmitted    : 1532,
Jon Empty Transmitted  : 39,
Leave Transmitted      : 0,
In Transmitted         : 0,
Empty Transmitted      : 296,
LeaveAll Transmitted   : 23,
Failed Registrations   : 0,
Total Mrp PDU Received  : 1160,
Total Mrp PDU Transmitted : 957,
Total Mrp Msgs Received : 10100,
Total Mrp Msgs Transmitted : 2693,
Invalid Msgs Received  : 0
```

output definitions

New Received	The number of new MVRP messages received on the switch.
Join In Received	The number of MVRP Join In messages received on the switch
Join Empty Received	The number of MVRP Join Empty messages received on the switch.
Leave In Received	The number of MVRP Leave In messages received on the switch.
In Received	The total MVRP messages received on the switch.
Empty Received	The number of MVRP Empty messages received on the switch.
Leave All Received	The number of MVRP Leave All messages received on the switch.
New Transmitted	The number of new MVRP messages sent by the switch.

output definitions (continued)

Join In Transmitted	The number of MVRP Join In messages sent by the switch
Join Empty Transmitted	The number of MVRP Join Empty messages sent by the switch.
Leave Transmitted	The number of MVRP Leave messages sent by the switch.
In Transmitted	The number of MVRP In messages sent by the switch.
Empty Transmitted	The number of MVRP empty messages sent by the switch.
LeaveAll Transmitted	The number of Leave All messages sent by the switch.
Failed Registrations	The number of failed registrations.
Total Mrp PDU Received	The number of total MRP PDUs received by the switch.
Total Mrp Msgs Received	The number of total MRP messages received by the switch.
Total Mrp Msgs Transmitted	The number of total MRP messages sent by the switch.
Invalid Msgs Received	The number of invalid messages received by the switch.

Release History

Release 6.4.3; command was introduced.

Related Commands

show mvrp configuration	Clears MVRP statistics for all the ports, an aggregate of ports, or a specific port.
show mvrp port	Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.
show mvrp linkagg	Displays the MVRP configuration for a specific port or an aggregate of ports.

MIB Objects

```
alaMvrpPortStatsTable
   alaMvrpPortStatsNewReceived,
   alaMvrpPortStatsJoinInReceived,
   alaMvrpPortStatsJoinEmptyReceived,
   alaMvrpPortStatsLeaveReceived,
   alaMvrpPortStatsInReceived,
   alaMvrpPortStatsEmptyReceived,
   alaMvrpPortStatsLeaveAllReceived,
   alaMvrpPortStatsNewTransmitted,
   alaMvrpPortStatsJoinInTransmitted,
   alaMvrpPortStatsJoinEmptyTransmitted,
   alaMvrpPortStatsLeaveTransmitted,
   alaMvrpPortStatsInTransmitted,
   alaMvrpPortStatsEmptyTransmitted,
   alaMvrpPortStatsLeaveAllTransmitted,
   alaMvrpPortStatsTotalPDUReceived,
   alaMvrpPortStatsTotalPDUTransmitted,
   alaMvrpPortStatsTotalMsgsReceived,
   alaMvrpPortStatsTotalMsgsTransmitted,
   alaMvrpPortStatsInvalidMsgsReceived,
   alaMvrpPortFailedRegistrations
```

show mvrp last-pdu-origin

Displays the source MAC address of the last MVRP message received on specific ports or aggregates.

show mvrp {port *slot/port* **[–** *port2***] | linkagg** *agg_num* **[-***agg_num2***]} last-pdu-origin**

Syntax Definitions

slot	The slot number for the module.
port	The physical port number on the module.
agg_num	The number corresponding to the aggregate group.

Defaults

NA

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

None

Examples

```
-> show mvrp port 1/1-3 last-pdu-origin
Port     Last PDU Origin
--------+------------------
1/1      00:d0:95:ee:f4:64
1/2      00:d0:95:ee:f4:65
1/3      00:d0:95:ee:f4:66

->show mvrp port 1/21 last-pdu-origin
Port     Last PDU Origin
--------+------------------
1/1      00:d0:95:ee:f4:64
```

output definitions

Port	Displays the slot/port number.
Last PDU origin	The source MAC address of the last PDU message received on the specific port.

Release History

Release 6.4.3; command was introduced.

Related Commands

show mvrp linkagg	Displays the MVRP configuration for a specific port or an aggregate of ports.
show mvrp port	Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.

MIB Objects

```
alaMvrpPortStatsTable
   alaMvrpPortLastPduOrigin
```

show vlan registration-mode

Displays the VLAN registration operational mode.

show vlan registration-mode

Syntax Definitions

NA

Defaults

NA

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

None

Examples

```
-> show vlan registration-mode
VLAN dynamic registration mode : mvrp
```

output definitions

VLAN dynamic registration mode	Displays the VLAN dynamic registration mode, mvrp or **gvrp**.

Release History

Release 6.4.3; command was introduced.

Related Commands

vlan registration-mode	Configures VLAN dynamic registration mode to either GVRP or MVRP and deletes all static configuration of previous mode along with the dynamic data.

MIB Objects

```
alaVlanDynamicRegistrationProtocolType
```

show mvrp vlan-restrictions

Displays the VLAN MVRP configuration on a specific port or an aggregate of ports.

show mvrp {port *slot/port* **[–** *port2***] | linkagg** *agg_num* **[-***agg_num2***]} vlan-restrictions**

Syntax Definitions

agg_num	The number corresponding to the aggregate group.
slot	The slot number for the module.
port	The physical port number on the module.

Defaults

NA

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the *agg_num* or *slot/port* parameter with this command to display the MVRP statistics for a specific port.

Examples

```
-> show mvrp port 1/21 vlan-restrictions
VLAN Id             Static      Restricted      Restricted
                 Registration   Registration    Applicant
--------------+--------------+--------------+-----------
     1               LEARN          FALSE         FALSE
     2               LEARN          FALSE         FALSE
     3               LEARN          FALSE         FALSE
     4               LEARN          FALSE         FALSE
     5               LEARN          FALSE         FALSE
     6               LEARN          FALSE         FALSE
     7               LEARN          FALSE         FALSE
    11               RESTRICT       FALSE         FALSE
    12               RESTRICT       FALSE         FALSE
    53               LEARN          TRUE          FALSE
    55               LEARN          FALSE         TRUE
```

output definitions

VLAN ID	The VLAN identification number for a preconfigured VLAN that handles the MVRP traffic for this port.
Static Registration	Indicates if the port is restricted (**RESTRICT**) or not restricted (**LEARN**) from becoming a member of the static VLAN.
Restricted Registration	Indicates if the VLAN is restricted (**TRUE**) or not restricted (**FALSE**) from dynamic registration on the port.
Restricted Applicant	Indicates if the VLAN is restricted for advertisement from the port (**TRUE**) or not (**FALSE**).

Release History

Release 6.4.3; command was introduced.

Related Commands

show mvrp port	Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.
show mvrp linkagg	Displays the MVRP configuration for a specific port or an aggregate of ports.

MIB Objects

```
alaMvrpPortConfigTable
   alaMvrpPortConfigRestrictedRegistrationBitmap
   alaMvrpPortConfigRestrictedApplicantBitmap
   alaMvrpPortConfigRegistrationToStaticVlan
```

show vlan mvrp

Displays the list of VLANS learned through MVRP and their details.

show vlan mvrp [vlan-id | vlan-range]

Syntax Definitions

vlan-id	VLAN ID number you want to display (1-4094)
vlan-range	The VLAN ID range (For example, 1-10)

Defaults

NA

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

None

Examples

```
-> show vlan mvrp
                        stree     mble
vlan  type admin oper 1x1   flat  auth  ip  ipx  tag  name
----+-----+-----+----+-----+--------+-------+------+-----+-----+-----------
5     mvrp  on    on   on    on   off   NA  off  off  MVRP1
6     mvrp  on    on   off   off  off   NA  off  off  MVRP12
```

output definitions

VLAN	The VLAN ID. Use the **vlan** command to create or remove VLANs.
Type	The type of VLAN (**std**, **vstk**, **gvrp**, **mvrp**, or **ipmv**)
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.
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 (For example, router interfaces, Spanning Tree) are applied to ports and traffic flow. A VLAN has to have an enabled administrative status before it can become operationally enabled.
stree lxl	Specifies that the MVRP status for the VLAN applies when the switch is running in the 1x1 MVRP mode.

output definitions (continued)

stree Flat	Specifies that the MVRP status for the VLAN applies when the switch is running in the flat MVRP mode.
Auth	VLAN Authentication status: **on** (enabled) or **off** (disabled). Use the **vlan authentication** command to change the VLAN Authentication status.
IP	IP router interface status: **on** (IP interface exists for the VLAN) or **off** (no IP router interface exists for the VLAN). Use **the ip interface command** to define an IP router interface for a VLAN.
mble Tag	Mobile tagging status: **on** (enabled); **off** (disabled). Configured through the **vlan mobile-tag** command.
Name	The user-defined text description for the VLAN. By default, the VLAN ID is specified for the VLAN description.

Release History

Release 6.4.3; command was introduced.

Related Commands

mvrp maximum vlan	Configures the maximum number of dynamic VLANs that can be created by MVRP.

MIB Objects

```
vlanMgrVlan
vlanTable
   vlanNumber
   vlanDescription
   vlanAdmStatus
   vlanOperStatus
   vlanStatus
   vlanStpStatus
   vlanAuthentStatus
   vlanIpAddress
   vlanIpMask
   vlanIpEnacp
   vlanIpForward
   vlanIpStatus
   vlanTagMobilePortStatus
```

mvrp clear-statistics

Clears MVRP statistics for all the ports, an aggregate of ports, or a specific port.

mvrp [port *slot/port* **[–***port2***] | linkagg** *agg_num* **[-***agg_num2***]] clear-statistics**

Syntax Definitions

slot	The slot number for the module.
port	The physical port number on the module.
agg_num	The number corresponding to the aggregate group.

Defaults

If no ports are specified, the MVRP statistics are deleted for all the ports.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the *agg_num* or *slot/port* parameter with this command to clear MVRP statistics for a specific port.

Examples

```
-> mvrp clear-statistics
-> mvrp port 1/2 clear-statistics
-> mvrp linkagg 10 clear-statistics
```

Release History

Release 6.4.3; command was introduced.

Related Commands

show mvrp statistics	Displays the MVRP statistics for all the ports, aggregates, or specific ports.

MIB Objects

```
alaMvrpGlobalClearStats
   alaMvrpPortStatsTable
   alaMvrpPortStatsClearStats
```

16 802.1AB Commands

Alcatel-Lucent 802.1AB is an IEEE standard for exchanging information with neighboring devices and maintaining a database of the information. The information is exchanged using the LLDPDU (Link Layer Discovery Protocol Data Unit) in TLV (Time, Length, Value) format. This chapter details configuring and monitoring 802.1AB on a switch.

Alcatel-Lucent version of 802.1AB complies with the IEEE 802.1AB-2005 Station and Media Access Control Discovery and ANSI-TIA 1057-2006 Link Layer Discovery Protocol for Media End Point Devices.

MIB information for the 802.1AB commands is as follows:

Filename: IEEE_LLDP_Base.mib
Module: LLDP-MIB

Filename: IEEE_LLDP_Dot1.mib
Module: LLDP-EXT-DOT1-MIB

Filename: IEEE_LLDP_Dot3.mib
Module: LLDP-EXT-DOT3-MIB

Filename: ANSI_TIA_LLDP_MED.mib
Module: LLDP-EXT-DOT3-MIB

Link Layer Discovery Protocol (LLDP) Security Mechanism in AOS prevents rogue LLDP agent from being connected to OmniSwitch. This ensures secured access to the device and the network.

LLDP Security Mechanism ensures having only one trusted LLDP agent on a network port. When more than one LLDP agent is learned on a port, the port is moved to violation state.

MIB information for the LLDP commands is as follows:

Filename: AlcatelINDLLDP.mib
Module: LLDP (IEEE802.1ab)

A summary of the available commands is listed here.

LLDP	**lldp destination mac-address** **lldp transmit fast-start-count** **lldp transmit interval** **lldp transmit hold-multiplier** **lldp transmit delay** **lldp reinit delay** **lldp network-policy** **lldp med network-policy** **lldp notification interval** **lldp lldpdu** **lldp notification** **lldp tlv management** **lldp tlv dot1** **lldp tlv dot3 mac-phy** **lldp tlv med** **show lldp config** **show lldp network-policy** **show lldp med network-policy** **show lldp system-statistics** **show lldp statistics** **show lldp local-system** **show lldp local-port** **show lldp local-management-address** **show lldp remote-system** **show lldp remote-system med**
LLDP Security Mechanism	**lldp trust-agent** **lldp trust-agent violation-action** **show lldp trusted remote-agent** **show lldp trust-agent**

Configuration procedures for 802.1AB are explained in the “Configuring 802.1AB” chapter of the *OmniSwitch AOS Release 6 Network Configuration Guide*.

lldp destination mac-address

Sets the lldp destination mac-address sent in LLPDUs.

lldp destination mac-address {nearest-bridge | nearest-edge}

Syntax Definitions

nearest-bridge	Specifies the destination mac-address as 01:80:C2:00:00:0E.
nearest-edge	Specifies the destination mac-address as 01:20: DA: 02:01:73.

Defaults

parameter	default
mac-address	**nearest-bridge**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

The **nearest-edge** MAC address is used in conjunction with the Auto Download Configuration feature to advertise the management VLAN.

Examples

```
-> lldp destination mac-address nearest-edge
-> lldp destination mac-address nearest-bridge
```

Release History

Release 6.4.4; command introduced.

Related Commands

show lldp local-system	Displays local system information.

MIB Objects

```
lldpDestMac
```

lldp transmit fast-start-count

Configures the fast start count for an LLDP Media Endpoint Device (MED).The fast start count specifies the number of LLDPDUs to be sent as soon as a MED is detected by the switch. The LLDPDUs contain the LLDP MED Network Policy TLVs.

lldp transmit fast-start-count *num*

Syntax Definitions

num	Specifies the number of LLDPDUs to send when a MED is detected. The valid range is 1–10.

Defaults

parameter	default
num	3

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

The LLDP MED fast start is only applicable when the MED is detected by the switch.

Examples

```
-> lldp transmit fast-start-count 4
```

Release History

Release 6.4.3; command introduced.

Related Commands

lldp network-policy	Configures a MED Network Policy on the switch for a specific application type.
lldp med network-policy	Associates an existing MED Network Policy with one or more LLDP ports.
show lldp local-system	Displays local system information.

MIB Objects

```
lldpXMedFastStartRepeatCount
```

lldp transmit interval

Sets the transmit time interval for LLDPDUs. This is the amount of time the switch waits between each transmission of an LLDPDU.

lldp transmit interval *seconds*

Syntax Definitions

seconds	The transmit interval value, in seconds. The valid range is 5–32768.

Defaults

parameter	default
seconds	30

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- This command applies only to LLDP-enabled ports.
- LLDP also multiplies the transmit time interval by the transmit hold multiplier to determine the time to live (TTL) value that is advertised in the LLDPDU.

Examples

```
-> lldp transmit interval 40
```

Release History

Release 6.3.1; command introduced.

Related Commands

lldp transmit hold-multiplier	Sets the transmit hold multiplier value. This value is used to calculate the Time To Live (TTL) value that is advertised in an LLDPDU.
show lldp local-system	Displays local system information.

MIB Objects

```
lldpConfiguration
   lldpMessageTxInterval
```

lldp transmit hold-multiplier

Sets the transmit hold multiplier value. This value is used to calculate the Time To Live (TTL) value that is advertised in an LLDPDU.

lldp transmit hold-multiplier *num*

Syntax Definitions

num	The transmit hold multiplier value. The valid range is 2–10.

Defaults

parameter	default
num	4

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- This command applies only to LLDP-enabled ports.
- LLDP multiples the transmit hold multiplier by the transmit interval value to determine the TTL value that is advertised in an LLDPDU.

Examples

```
-> lldp transmit hold-multiplier 6
```

Release History

Release 6.3.1; command introduced.

Related Commands

lldp transmit interval	Sets the transmit time interval for LLDPDUs. This is the amount of time the switch waits between each transmission of an LLDPDU.
show lldp local-system	Displays local system information.

MIB Objects

```
lldpConfiguration
   lldpMessageTxHoldMultiplier
```

lldp transmit delay

Sets the minimum amount of time that must elapse between successive LLDPDUs that are transmitted as the result of a value or status change in the LLDP local systems MIB.

lldp transmit delay *seconds*

Syntax Definitions

seconds	The transmit delay value, in seconds. The valid range is 1–8192.

Defaults

parameter	default
seconds	2

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- This command applies only to LLDP-enabled ports.
- The following formula determines the recommended transmit delay value:

  1 <= transmit delay <= (0.25 * transmit interval).

Examples

```
-> lldp transmit delay 20
```

Release History

Release 6.3.1; command introduced.

Related Commands

lldp transmit interval	Sets the transmit time interval for LLDPDUs. This is the amount of time the switch waits between each transmission of an LLDPDU.
show lldp local-system	Displays local system information.

MIB Objects

```
lldpConfiguration
   lldpTxDelay
```

lldp reinit delay

Sets the amount of time that must elapse before an LLDP port is re-initialized after the status for the port was disabled.

lldp reinit delay *seconds*

Syntax Definitions

seconds	The re-initialize value, in seconds. The valid range is 1–10.

Defaults

parameter	default
seconds	2

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

This command applies only to LLDP-enabled ports.

Examples

```
-> lldp reinit delay 4
```

Release History

Release 6.3.1; command introduced.

Related Commands

lldp transmit delay	Sets the minimum time interval between successive LLDPDUs that are transmitted as the result of a value or status change in the LLDP local systems MIB.
show lldp local-system	Displays local system information.

MIB Objects

```
lldpConfiguration
   lldpReinitDelay
```

lldp notification interval

Sets the amount of time that must elapse before an LLDP notification about a remote systems MIB change is generated.

lldp notification interval *seconds*

Syntax Definitions

seconds	The notification time interval, in seconds. The valid range is 5–3600.

Defaults

parameter	default
seconds	5

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- This command applies only to LLDP-enabled ports that also have the LLDP notification status enabled.
- Within a given notification time interval, generating more than one notification event is not allowed.

Examples

```
-> lldp notification interval 25
```

Release History

Release 6.3.1; command introduced.

Related Commands

lldp notification	Enables or disables the LLDP notification status for one or more switch ports. LLDP notifications are sent when there is a change to the remote systems MIB.
show lldp local-system	Displays local system information.

MIB Objects

```
lldpConfiguration
   lldpNotificationInterval
```

lldp lldpdu

Configures the LLDPDU status for one or more switch ports. The status determines if the specified switch ports will transmit, receive, transmit and receive, or drop LLDPDUs.

lldp {*slot/port* **|** *slot* **| chassis} lldpdu {tx | rx | tx-and-rx | disable}**

Syntax Definitions

slot/port	Slot number for the module and physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
slot	The slot number for a specific module.
chassis	All ports on the switch.
tx	Transmits LLDPDUs.
rx	Receives LLDPDUs.
tx-and-rx	Transmits and receives LLDPDUs.
disable	Disables the LLDPDU status.

Defaults

parameter	default
tx | rx | tx-and-rx | disable	**tx-and-rx**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- If the LLDPDU status is disabled, LLDPDUs are not transmitted and any that are received are dropped.
- Using the *slot* or **chassis** parameter with this command overrides the existing status configuration for any individual ports on the specified slot number or for all ports on the switch.

Examples

```
-> lldp 1/2 lldpdu tx-and-rx
-> lldp 3 lldpdu rx
-> lldp chassis lldpdu disable
```

Release History

Release 6.3.1; command introduced.

Related Commands

lldp notification	Enables or disables the LLDP notification status for one or more switch ports. LLDP notifications are sent when there is a change to the remote systems MIB.
show lldp local-port	Displays information about local system ports.
show lldp config	Displays the general LLDP configuration information for LLDP ports.

MIB Objects

```
lldpPortConfigTable
   lldpPortConfigPortNum
   lldpPortConfigAdminStatus
```

lldp notification

Enables or disables the LLDP notification status for one or more switch ports. LLDP notifications are sent when there is a change to the remote systems MIB.

lldp {*slot/port* **|** *slot* | **chassis} notification {enable | disable}**

Syntax Definitions

slot/port	The slot number for the module and physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
slot	The slot number for a specific module.
chassis	All switch ports.
enable	Enables the notification of local system MIB changes.
disable	Disables the notification.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The LLDPDU administrative status must be in the receive state before using this command.
- Using the *slot* or **chassis** parameter with this command overrides the existing notification status configuration for any individual ports on the specified slot number or for all ports on the switch.

Examples

```
-> lldp 1/2 notification enable
-> lldp 1 notification disable
```

Release History

Release 6.3.1; command introduced.

Related Commands

lldp notification interval	Sets the time interval that must elapse before a notification about the local system MIB change is generated.
lldp lldpdu	Configures the LLDPDU status for one or more switch ports. The status determines if the specified switch ports will transmit, receive, transmit and receive, or drop LLDPDUs.

MIB Objects

```
lldpPortConfigTable
   lldpPortConfigPortNum
   lldpPortConfigNotificationEnable
```

lldp network-policy

Configures a local Network Policy on the switch for a specific application type.

lldp network-policy *policy_id* - [*policy_id2*] **application {voice | voice-signaling | guest-voice | guest-voice-signaling | softphone-voice | video-conferencing | streaming-video | video-signaling} vlan {untagged | priority-tag |** *vlan-id***} [l2-priority** *802.1p_value***] [dscp** *dscp_value***]**

no lldp network-policy *policy_id* - [*policy_id2*]

Syntax Definitions

policy_id - [*policy_id2*]	A network policy identifier (0-31) which is associated to a port.
voice	Specifies a voice application type.
voice-signaling	Specifies a voice-signaling application type.
guest-voice	Specifies a guest-voice application type.
guest-voice-signaling	Specifies a guest-voice-signaling application type.
softphone-voice	Specifies a softphone-voice application type.
video-conferencing	Specifies a video-conferencing application type.
streaming-video	Specifies a streaming-video application type.
video-signaling	Specifies a video-signaling application type.
untagged	Specifies that a VLAN port is untagged.
priority-tag	Specifies the internal priority that would be assigned to the VLAN**.**
vlan_id	VLAN identifier. Valid range is 1–4094.
802.1p_value	The Layer-2 priority value assigned to the VLAN. Valid range is 0–7.
dscp_value	Priority value assigned to the DSCP (Differentiated Service Code Point) header. Valid range is 0–63.

Defaults

parameter	default
802.1p_value	**0**
dscp_value	**0**

- By default the VLAN ID is configured in the voice network profile.
- By default the 802.1p_value is 5 for voice application.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove the configured network policy from the system.
- When a network policy is deleted, all the associated values and port bindings are also deleted.
- A maximum of 32 network policies can be configured on a single VLAN.
- Once a policy is created, the application type, VLAN ID, 802.1p, and DSCP values can be modified.
- If a network policy ID is bound to a port, it cannot be modified.
- Use a hyphen to specify a range of Policy IDs and a space to separate multiple Policy IDs in the command.
- The range for Policy IDs is supported only with the **no** form of this command.

Examples

```
-> lldp network-policy 10 application voice vlan 20
-> lldp network-policy 11 application guest-voice-signaling vlan untagged
l2-priority 3
-> lldp network-policy 20 application voice vlan priority-tag dscp 39
-> lldp network-policy 20 application voice-signaling vlan 23 l2-priority 2 dscp 43
-> no lldp network-policy 10
-> no lldp network-policy 10-20
```

Release History

Release 6.4.3; command introduced.

Related Commands

lldp tlv med	Configures whether or not LLDP-MED TLVs are included in transmitted LLDPDUs.
show lldp network-policy	Displays the network policy details for a given policy ID.
show lldp med network-policy	Displays the network policy configured on a slot or port. If no option is specified, network policies configured on all ports of the chassis are displayed.

MIB Objects

```
aLldpXMedLocMediaPolicyTable
   alaLldpXMedLocMediaPolicyId
   alaLldpXMedLocMediaPolicyAppType
   alaLldpXMedLocMediaPolicyVlanType
   alaLldpXMedLocMediaPolicyVlanID
   alaLldpXMedLocMediaPolicyPriority
   alaLldpXMedLocMediaPolicyDscp
   alaLldpXMedLocMediaPolicyUnknown
   alaLldpXMedLocMediaPolicyTagged
   alaLldpXMedLocMediaPolicyRowStatus
```

lldp med network-policy

Associates an existing network policy to a port, slot, or chassis.

lldp {*slot/port* **|** *slot* | **chassis} med network-policy** *policy_id* - [*policy_id2*]

no lldp {*slot/port* **|** *slot* | **chassis} med network-policy** *policy_id* - [*policy_id2*]

Syntax Definition

slot/port	The slot number for the module and physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
slot	The slot number for a specific module.
chassis	All switch ports.
policy_id - [*policy_id2*]	A network policy identifier (0–31).

Defaults

NA

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to disassociate a network policy from a port.
- The network policy should already be configured in the system before associating it with a port.
- A maximum of 8 network policies can be associated to a port.
- Two or more network policy IDs with the same application type cannot be associated to a port.

Examples

```
-> lldp chassis med network-policy 22
-> lldp 1 med network-policy 1-4 5 6
-> lldp 2/3 med network-policy 12
-> no lldp 2/3 med network-policy 12
```

Release History

Release 6.4.3; command introduced.

Related Commands

lldp tlv med	Configures whether or not LLDP-MED TLVs are included in transmitted LLDPDUs.
show lldp network-policy	Displays the MED Network Policy details for a given policy ID.
show lldp med network-policy	Displays the network policy configured on a slot or port. If no option is specified, network policies configured on all ports of the chassis are displayed.

MIB Objects

```
alaLldpXMedLocMediaPolicyPortTable
   alaLldpXMedLocMediaPolicyPortIfIndex
   alaLldpXMedLocMediaPolicyId
   alaLldpXMedLocMediaPolicyPortRowStatus
```

lldp tlv management

Specifies the switch to control per port management TLVs to be incorporated in the LLDPDUs.

lldp {*slot/port* **|** *slot* **| chassis} tlv management {port-description | system-name | system-description | system-capabilities | management-address} {enable | disable}**

Syntax Definitions

slot/port	Slot number for the module and physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
slot	The slot number for a specific module.
port-description	Enables or disables the transmission of port description TLV in LLDPDU.
system-name	Enables or disables the transmission of system name TLV in LLDPDU.
system-description	Enables or disables transmission of system description TLV in LLDPDU.
system-capabilities	Enables or disables transmission of system capabilities TLV in LLDPDU.
management-address	Enables or disables transmission of management address on per port.
enable	Enables management TLV LLDPDU transmission.
disable	Disables management TLV LLDPDU transmission.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The LLDPDU must be enabled and set to transmit before using this command.
- Using the *slot* or **chassis** parameter with this command overrides the existing configuration for any individual ports on the specified slot number or for all ports on the switch.

Examples

```
-> lldp 1/2 tlv management port-description enable
-> lldp 2 tlv management management-address enable
-> lldp 3 tlv management system-name disable
```

Release History

Release 6.3.1; command introduced.

Related Commands

lldp lldpdu	Specifies the switch to control the transmission and the reception of LLDPDUs for a particular chassis, a slot, or a port.
show lldp local-system	Displays local system information.
show lldp local-port	Displays local port information.
show lldp remote-system	Displays port information of remote system.

MIB Objects

```
lldpPortConfigTable
   lldpLocPortPortNum
   lldpPortConfigTLVsTxEnable
lldpConfigManAddrTable
   lldpConfigManAddrPortsTxEnable
```

lldp tlv dot1

Specifies the switch to control per port 802.1 TLVs to be incorporated in the LLDPDUs.

lldp {*slot/port* **|** *slot* **| chassis} tlv dot1 {port-vlan | vlan-name} {enable | disable}**

Syntax Definitions

slot/port	Slot number for the module and physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
slot	The slot number for a specific module.
port-vlan	Enables or disables transmission of port VLAN TLV in LLDPDU.
vlan-name	Enables or disables transmission of VLAN name TLV in LLDPDU.
enable	Enables 802.1 TLV LLDPDU transmission.
disable	Disables 802.1 TLV LLDPDU transmission.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The LLDPDU must be enabled and set to transmit before using this command.
- Using the *slot* or **chassis** parameter with this command overrides the existing configuration for any individual ports on the specified slot number or for all ports on the switch.
- If one TLV is included then the other TLV is automatically included when you use this command.

Examples

```
-> lldp 5/1 tlv dot1 port-vlan enable
-> lldp 3 tlv dot1 vlan-name enable
-> lldp 3 tlv dot1 vlan-name disable
```

Release History

Release 6.3.1; command introduced.

Related Commands

lldp tlv management	Specifies the switch to control per port management TLVs to be incorporated in the LLDPDUs.
show lldp statistics	Displays per port statistics.
show lldp local-port	Displays per port information.

MIB Objects

```
lldpPortConfigTable
   lldpPortConfigPortNum
lldpXdot1ConfigPortVlanTable
   lldpXdot1ConfigPortVlanTxEnable
lldpXdot1ConfigVlanNameTable
   lldpXdot1ConfigVlanNameTxEnable
```

lldp tlv dot3 mac-phy

Configures whether or not 802.3 TLVs are included in transmitted LLDPDUs.

lldp {*slot/port* **|** *slot* | **chassis} tlv dot3 mac-phy {enable | disable}**

Syntax Definitions

slot/port	Slot number for the module and physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
slot	The slot number for a specific module.
chassis	All ports on the switch.
enable	Enables the transmission of 802.3 TLVs in LLDPDUs.
disable	Disables the transmission of 802.3 TLVs in LLDPDUs.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The ports specified with this command must already be configured to transmit LLDPDUs.
- Using the *slot* or **chassis** parameter with this command overrides the existing configuration for any individual ports on the specified slot number or for all ports on the switch.

Examples

```
-> lldp 2/4 tlv dot3 mac-phy enable
-> lldp 2 tlv dot3 mac-phy disable
```

Release History

Release 6.3.1; command introduced.

Related Commands

lldp lldpdu	Configures the LLDPDU status for one or more switch ports. The status determines if the specified switch ports will transmit, receive, transmit and receive, or drop LLDPDUs.
lldp tlv management	Configures whether or not management TLVs are included in transmitted LLDPDUs.
lldp tlv dot1	Configures whether or not 802.1 TLVs are included in transmitted LLDPDUs.
show lldp statistics	Displays per port statistics.

MIB Objects

```
lldpPortConfigTable
   lldpPortConfigPortNum
lldpXdot3PortConfigTable
   lldpXdot3PortConfigTLVsTxEnable
```

lldp tlv med

Configures whether or not LLDP-MED TLVs are included in transmitted LLDPDUs.

lldp {*slot/port* **|** *slot* **| chassis} tlv med {power | capability | network policy} {enable | disable}**

Syntax Definitions

slot/port	Slot number for the module and physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
slot	The slot number for a specific module.
chassis	All ports on the switch.
power	Includes the extended POE TLV in transmitted LLDPDUs.
capability	Includes the Capabilities TLV in transmitted LLDPDUs.
network policy	Includes the Network Policy TLV in transmitted LLDPDUs.
enable	Enables the transmission of LLDP-MED TLV in LLDPDUs.
disable	Disables the transmission of LLDP-MED TLV in LLDPDUs.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The ports specified with this command must already be configured to transmit LLDPDUs.
- Using the *slot* or **chassis** parameter with this command overrides the existing configuration for any individual ports on the specified slot number or for all ports on the switch.
- The **lldp tlv med power** version of this command applies only to PoE units.
- Before enabling the Power MED TLV, use the **lanpower start** command to activate PoE on a port or on all ports in a specific slot.

Examples

```
-> lldp 4/4 tlv med power enable
-> lldp 4/3 tlv med capability enable
-> lldp 4 tlv med power disable
-> lldp 4 tlv med network-policy enable
-> lldp chassis tlv med network-policy enable
```

Release History

Release 6.3.1; command introduced.
Release 6.4.3; **network policy** option added.

Related Commands

lldp lldpdu	Configures the LLDPDU status for one or more switch ports. The status determines if the specified switch ports will transmit, receive, transmit and receive, or drop LLDPDUs.
lldp tlv management	Configures whether or not management TLVs are included in transmitted LLDPDUs.
lldp tlv dot1	Configures whether or not 802.1 TLVs are included in transmitted LLDPDUs.
lldp tlv dot3 mac-phy	Configures whether or not 802.3 TLVs are included in transmitted LLDPDUs.
show lldp med network-policy	Displays the MED Network Policy configuration.

MIB Objects

```
lldpPortConfigTable
   lldpPortConfigPortNum
lldpXMedPortConfigTable
   lldpXMedPortConfigTLVsTxEnable
```

show lldp config

Displays the general LLDP configuration information for LLDP ports.

show lldp {*slot* | *slot/port***} config**

Syntax Definitions

slot	The slot number for a specific module.
slot/port	Slot number for the module and physical port number on that module (for example, 3/1 specifies port 1 on slot 3).

Defaults

By default, a list of all LLDP ports with their configuration parameters is displayed.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the *slot/port* or *slot* parameter to display information for a specific port or for all ports on a specific module.

Examples

```
-> show lldp config
----------+-----------------------------------------+-----------------+-------
          |  Admin   |  Notify  |  Std TLV |   Mgmt   |  802.1   |  802.3 |   MED
 Slot/Port|  Status  |   Trap   |   Mask   | Address  |   TLV    |   Mask |   Mask
----------+----------+----------+----------+----------+----------+------+------
   2/1      Rx + Tx    Disabled     0x00     Disabled   Disabled     0x00 0x00
   2/2      Rx + Tx    Disabled     0x00     Disabled   Disabled     0x00 0x00
   2/3      Rx + Tx    Disabled     0x00     Disabled   Disabled     0x00 0x00
   2/4      Rx + Tx    Disabled     0x00     Disabled   Disabled     0x00 0x00
   2/5      Rx + Tx    Disabled     0x00     Disabled   Disabled     0x00 0x00
```

output definitions

Slot/Port	The LLDP slot and port number.
Admin Status	Indicates the Administrative status of the LLDP port.The options are - **Disabled**, **Rx**, **Tx**, and **Rx+Tx**.
Notify Trap	Indicates if the Notify Trap feature is disabled or enabled on a particular port
Std TLV Mask	The standard TLV mask set for the port.
Mgmt Address	Indicates whether transmission of the per port IPv4 management address is enabled or disabled.
802.1 TLV	Indicates whether 802.1 TLV status is enabled or disabled on the LLDP port.

output definitions

802.3 Mask	The standard 802.3 mask set for the port.
MED Mask	The standard MED mask set for the port.

Release History

Release 6.4.3; command introduced.

Related Commands

lldp lldpdu	Configures the LLDPDU status for one or more switch ports. The status determines if the specified switch ports will transmit, receive, transmit and receive, or drop LLDPDUs.
lldp notification	Enables or disables the LLDP notification status for one or more switch ports. LLDP notifications are sent when there is a change to the remote systems MIB.
lldp tlv management	Specifies the switch to control per port management TLVs to be incorporated in the LLDPDUs.
lldp tlv dot3 mac-phy	Configures whether or not 802.3 TLVs are included in transmitted LLDPDUs.

MIB Objects

```
lldpPortConfigTable
   lldpPortConfigPortNum
   lldpPortConfigAdminStatus
   lldpPortConfigNotificationEnable
   lldpLocPortPortNum
   lldpPortConfigTLVsTxEnable
lldpConfigManAddrTable
   lldpConfigManAddrPortsTxEnable
lldpXdot3PortConfigTable
   lldpXdot3PortConfigTLVsTxEnable
```

show lldp network-policy

Displays the MED Network Policy details for a given policy ID.

show lldp network-policy [*policy_id***]**

Syntax Definitions

policy_id	Policy identifier for a network policy definition. Valid range is between 0 and 31.

Defaults

By default, all configured policies are displayed.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Network policy should be configured on the system before using this command.
- Enter a policy ID with this command to display information for a specific policy.

Examples

```
-> show lldp network-policy
Legend: 0 Priority Tagged Vlan
        - Untagged Vlan

Network         Application       Vlan    Layer2   DSCP
Policy ID        Type              Id    Priority  Value
-----------+----------------------+------+--------+-------
     1      voice                   4000   7        33
    12      guest-voice                -   -        44
    21      streaming-voice            0   4        11
    31      guest-voice-signaling     23   2        1

-> show lldp network-policy 1
Legend: 0 Priority Tagged Vlan
        - Untagged Vlan

Network         Application       Vlan    Layer2   DSCP
Policy ID        Type              Id    Priority  Value
-----------+----------------------+------+--------+-------
     1      voice                   4000   7        33
```

output definitions

Network Policy ID	Policy identifier for a network policy definition.
Application Type	Indicates the type of application configured on the port or VLAN.
VLAN ID	The VLAN ID assigned to the port on which the network policy is configured.
Layer2 Priority	Layer 2 priority to be used for the specified application type.
DSCP Value	DSCP value to be used to provide Diffserv node behavior for the specified application type.

Release History

Release 6.4.3; command introduced.

Related Commands

lldp network-policy	Configures a local network policy on a switch for an application type.

MIB Objects

```
alaLldpXMedLocMediaPolicyTable
   alaLldpXMedLocMediaPolicyId
   alaLldpXMedLocMediaPolicyAppType
   alaLldpXMedLocMediaPolicyVlanType
   alaLldpXMedLocMediaPolicyVlanId
   alaLldpXMedLocMediaPolicyPriority
   alaLldpXMedLocMediaPolicyDscp
   alaLldpXMedLocMediaPolicyUnknown
   alaLldpXMedLocMediaPolicyTagged
```

show lldp med network-policy

Displays the network policy configured on a slot or port. If no option is specified, network policies configured on all ports of the chassis are displayed.

show lldp [*slot* | *slot/port***] med network-policy**

Syntax Definitions

slot	Specifies the slot number on a specific module or chassis.
slot/port	Specifies the slot number for the module and physical port number on that module (for example 3/1 specifies port 1 of slot 3).

Defaults

By default, all ports with associated policies are displayed.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Network policy should be configured on the system before using this command.
- Enter a slot or slot/port number with this command to display information for a specific slot or port.

Examples

```
-> show lldp med network-policy

  slot/port         Network Policy ID
-------------+------------------------
    1/1            1 3 5 7 21 23 30 31
    1/2            1 2 3 4 7 8 9 10
    .
    .
    .
    2/1            1 3 5
    .
    .

-> show lldp 1/1 med network-policy

Legend: 0 Priority Tagged Vlan
        - Untagged Vlan

Slot/    Network         Application       Vlan    Layer2   DSCP
 Port    Policy ID        Type              Id    Priority  Value
-------+-----------+---------------------+------+--------+-------
  1/1        1       guest-voice-signaling  -      -        0
```

output definitions

Slot/Port	Slot number for the module and physical port number on that module.
Network Policy ID	Policy identifier for a network policy definition.
Application Type	Indicates the type of application configured on the port or VLAN.
VLAN ID	The VLAN ID assigned to the port on which the network policy is configured.
Layer2 Priority	Layer 2 priority to be used for the specified application type.

Release History

Release 6.4.3; command introduced.

Related Commands

lldp tlv med	Configures whether or not LLDP-MED TLVs are included in transmitted LLDPDUs.
lldp network-policy	Configures a local network policy on a switch for an application type.

MIB Objects

```
alaLldpXMedLocMediaPolicyPortTable
   alaLldpXMedLocMediaPolicyPortIfIndex
   alaLldpXMedLocMediaPolicyId
```

show lldp system-statistics

Displays system-wide statistics.

show lldp system-statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show lldp system-statistics
 Local LLDP Agent System Statistics:
  Remote Systems Last Change  = 0 days 0 hours 3 minutes and 10 seconds,
  Remote Systems MIB Inserts  = 2,
  Remote Systems MIB Deletes  = 0,
  Remote Systems MIB Drops    = 0,
  Remote Systems MIB Age Outs = 0
```

output definitions

Remote Systems Last Change	The last change recorded in the tables associated with the remote system.
Remote Systems MIB Inserts	The total number of complete inserts in the tables associated with the remote system.
Remote Systems MIB Deletes	The total number of complete deletes in tables associated with the remote system.
Remote Systems MIB Drops	The total number of LLDPDUs dropped because of insufficient resources.
Remote Systems MIB Age Outs	The total number of complete age-outs in the tables associated with the remote system.

Release History

Release 6.3.1; command introduced.

Related Commands

lldp notification	Enables or disables the LLDP notification status for one or more switch ports. LLDP notifications are sent when there is a change to the remote systems MIB.
lldp notification interval	Sets the amount of time that must elapse before an LLDP notification about a remote systems MIB change is generated.

MIB Objects

```
lldpStatistics
   lldpStatsRemTablesLastChangeTime
   lldpStatsRemTablesInserts
   lldpStatsRemTablesDeletes
   lldpStatsRemTablesDrops
   lldpStatsRemTablesAgeouts
```

show lldp statistics

Displays per port statistics.

show lldp [*slot*|*slot/port***] statistics**

Syntax Definitions

slot	The slot number for a specific module.
slot/port	Slot number for the module and physical port number on that module (for example, 3/1 specifies port 1 on slot 3).

Defaults

By default, statistics are displayed for all LLDP ports.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Enter a slot or slot/port number to display statistics for a specific slot or port.
- If the statistics are zero they are not displayed.

Examples

```
-> show lldp statistics
----------+--------------------------------------+--------------------+----------
       |           LLDPDU                      |     TLV      | Device
 Slot/Port|  Tx         Rx       Errors    Discards |  Unknown   Discards | Ageouts
----------+--------+----------+----------+----------+----------+----------+-----
  1/23       52          0          0          0          0          0          0
  2/47       50         50          0          0          0          0          0
  2/48       50         50          0          0          0          0          0
```

output definitions

Slot/Port	Slot number for the module and physical port number on that module.
LLDPDU Tx	The total number of LLDPDUs transmitted on the port.
LLDPDU Rx	The total number of valid LLDPDUs received on the port.
LLDPDU Errors	The total number of invalid LLDPDUs discarded on the port.
LLDPDU Discards	The total number of LLDPDUs discarded on the port.
TLV Unknown	The total number of unrecognized LLDP TLVs on the port.
TLV Discards	The total number of LLDP TLVs discarded on the port.
Device Ageouts	The total number of complete age-outs on the port.

Release History

Release 6.3.1; command introduced.

Related Commands

lldp lldpdu	Configures the LLDPDU status for one or more switch ports. The status determines if the specified switch ports will transmit, receive, transmit and receive, or drop LLDPDUs.
lldp tlv management	Specifies the switch to control per port management TLVs to be incorporated in the LLDPDUs.

MIB Objects

```
lldpStatsTxPortTable
   lldpStatsTxPortNum
   lldpStatsTxPortFramesTotal
lldpStatsRxPortTable
   lldpStatsRxPortNum
   lldpStatsRxPortFramesDiscardedTotal
   lldpStatsRxPortFramesErrors
   lldpStatsRxPortFramesTotal
   lldpStatsRxPortTLVsDiscardedTotal
   lldpStatsRxPortTLVsUnrecognizedTotal
   lldpStatsRxPortAgeoutsTotal
```

show lldp local-system

Displays local system information.

show lldp local-system

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show lldp local-system
Local LLDP Agent System Data:
  Chassis ID Subtype          = 4 (MAC Address),
  Chassis ID                  = 00:d0:95:e9:c9:2e,
  System Name                 = OS6850E,
  System Description          = 6.3.1.636.R01 Development, September 07, 2007.,
  Capabilities Supported       = Bridge, Router,
  Capabilities Enabled         = Bridge, Router,
  LLDPDU Transmit Interval    = 30 seconds,
  TTL Hold Multiplier         = 4,
  LLDPDU Transmit Delay       = 2 seconds,
  Reintialization Delay       = 2 seconds,
  MIB Notification Interval = 5 seconds,
  Fast Start Count            = 4,
  Management Address Type     = 1 (IPv4),
  Management IP Address       = 10.255.11.100,
```

output definitions

Chassis ID Subtype	The subtype that describe chassis ID.
Chassis ID	The chassis ID (MAC address).
System Name	The name of the system.
System Description	The description of the system.
Capabilities Supported	The capabilities of the system.
Capabilities Enabled	The enabled capabilities of the system.
LLDPDU Transmit Interval	The LLDPDU transmit interval.
TTL Hold Multiplier	The hold multiplier used to calculate TTL.

output definitions (continued)

LLDPDU Transmit Delay	The minimum transmit time between successive LLDPDUs.
Reintialization Delay	The minimum time interval before the reinitialization of local port objects between port status changes.
MIB Notification Interval	The minimum time interval between consecutive notifications of local system MIB change.
Fast Start Count	Specifies the number of LLDPDUs to be sent as soon as a MED is detected by system.
Management Address Type	The type of management address used in LLDPDU.
Management IP Address	The management IP address. This will be the Loopback0 IP address if configured, otherwise it is the first IP interface configured on the switch.

Release History

Release 6.3.1; command introduced.
Release 6.4.3; **Fast Start Count** field added to output.

Related Commands

lldp transmit fast-start-count	Configures the fast start count for an LLDP Media Endpoint Device (MED).The fast start count specifies the number of LLDPDUs to be sent as soon as a MED is detected by the switch. The LLDPDUs contain the LLDP MED Network Policy TLVs.
lldp reinit delay	Sets the amount of time that must elapse before an LLDP port is re-initialized after the status for the port was disabled.
lldp transmit hold-multiplier	Sets the transmit hold multiplier value. This value is used to calculate the Time To Live (TTL) value that is advertised in an LLDPDU.
lldp transmit delay	Sets the minimum amount of time that must elapse between successive LLDPDUs that are transmitted as the result of a value or status change in the LLDP local systems MIB.

MIB Objects

```
lldpLocalSystemData
   lldpLocChassisIdSubtype
   lldpLocChassisId
   lldpLocSysName
   lldpLocSysDesc
   lldpLocSysCapSupported
   lldpLocSysEnabled
lldpPortConfigTable
   lldpMessageTxInterval
   lldpMessageTXHoldMultiplier
   lldpTxDelay
   lldpReinitDelay
   lldpNotificationInterval
lldpLocManAddrTable
   lldpLocManAddrSubtype
   lldpLocManAddr
```

```
lldpXMedFastStartRepeatCount
```

show lldp local-port

Displays local LLDP port information.

show lldp [*slot/port* **|** *slot***] local-port**

Syntax Definitions

slot/port	Slot number for the module and physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
slot	The slot number for a specific module.

Defaults

By default, a list of all LLDP ports is displayed.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the *slot/port* or *slot* parameter to display information for a specific port or for all ports on a specific module.

Examples

```
-> show lldp local-port
Local Slot 1/Port 1 LLDP Info:
  Port ID                     = 1001 (Locally assigned),
  Port Description            = Alcatel 1/1 6.3.1.636.R01,
Local Slot 1/Port 2 LLDP Info:
  Port ID                     = 1002 (Locally assigned),
  Port Description            = Alcatel 1/2 6.3.1.636.R01,
.
.
.
Local Slot 2/Port 48 LLDP Info:
  Port ID                     = 2048 (Locally assigned),
  Port Description            = Alcatel 2/48 6.3.1.636.R01,
```

output definitions

Port ID	The port ID (Port MAC).
Port Description	The description of the port (which includes the port number and the AOS version).

Release History

Release 6.3.1; command introduced.

Related Commands

lldp tlv management	Specifies the switch to control per port management TLVs to be incorporated in the LLDPDUs.
lldp tlv dot1	Specifies the switch to control per port 802.1 TLVs to be incorporated in the LLDPDUs.

MIB Objects

```
lldpLocPortTable
   lldpLocPortNum
   lldpLocPortIdsubtype
   lldpLocPortId
   lldpLocPortDesc
```

show lldp local-management-address

Displays the local management address information.

show lldp local-management-address

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show lldp local-management-address
Local LLDP Agent Management Address:
  Management Address Type     = 1 (IPv4),
  Management IP Address       = 10.255.11.100
```

output definitions

Management Address Type	The address type used to define the interface number (IPv4 or IPv6).
Management IP Address	The management IP address. The Loopback0 IP address is configured for the management IP address to be transmitted.

Release History

Release 6.3.1; command introduced.

Related Commands

lldp tlv management	Specifies the switch to control per port management TLVs to be incorporated in the LLDPDUs.
show lldp local-system	Displays local system information.

MIB Objects

```
lldpLocManAddrTable
   lldpLocManAddrLen
   lldpLocManAddrIfSubtype
   lldpLocManAddrIfId
```

show lldp remote-system

Displays remote system information for a single port or all ports on a slot.

show lldp [*slot/port* **|** *slot***] remote-system**

Syntax Definitions

slot/port	Slot number for the module and physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
slot	The slot number for a specific module.

Defaults

By default, a list of all LLDP ports is displayed.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the *slot/port* or *slot* parameter to display information for a specific port or for all ports on a specific module.

Examples

```
-> show lldp remote-system
Remote LLDP Agents on Local Slot/Port 1/22:
  Remote ID 1:
    Chassis ID Subtype          = 4 (MAC Address),
    Chassis ID                  = 00:d0:95:ea:7c:3a,
    Port ID Subtype             = 3 (MAC address),
    Port ID                     = 00:d0:95:ea:7c:45,
    Port Description            = (null),
    System Name                 = (null),
    System Description          = (null),
    Capabilities Supported      = Bridge, Router,
    Capabilities Enabled        = Bridge, Router,
    MED Device Type             = Network Connectivity,
    MED Capabilities            = Capabilities | Power via MDI-PSE (09),
    MED Extension TLVs Present  = Network Policy, Inventory Management,
    Remote port MAC/PHY AutoNeg = Supported, Enabled, Capability 0x6c01,
    Mau Type=1000BaseTFD - Four-pair Category 5 UTP, full duplex mode
```

output definitions

Remote LLDP Agents on Local Slot/Port	The Slot number to which the remote system entry is associated and the physical port number on that module.
Chassis ID Subtype	The sub type that describes chassis ID.
Chassis ID	The chassis ID (MAC address).
Port ID Subtype	The sub type that describes port ID

output definitions (continued)

Port ID	The port ID (Port MAC).
Port Description	The description of the port (which includes the port number and the AOS version).
System Name	The name of the system.
System Description	The description of the system.
Capabilities Supported	The capabilities of the system such as bridge or router.
Capabilities Enabled	The enabled capabilities of the system.
MED Device Type	The type of device such as Network Connectivity or Endpoint Device.
MED Capabilities	MED capabilities supported.
MED Extension TLVs Present	MED Extension TLVs present.
Remote port MAC/PHY AutoNeg	The MAC/PHY settings of the remote port such as speed, duplex, and auto-negotiation.

Release History

Release 6.3.1; command introduced.
Release 6.3.4; **remote-system** parameter was introduced.

Related Commands

show lldp local-port	Displays per port information.
show lldp local-system	Displays local system information.

MIB Objects

```
lldpRemTable
   lldpRemLocalPortNum
   lldpRemChassisIdSubtype
   lldpRemChassisId
   lldpRemPortIdSubtype
   lldpRemPortId
   lldpRemPortDesc
   lldpRemSysName
   lldpRemSysDesc
   lldpRemSysCapSupported
   lldpRemSysCapEnabled
   lldpRemManAddrIfSubtype
   lldpRemManAddrIfId
```

show lldp remote-system med

Displays remote system MED information for a single port or all ports on a slot.

show lldp [*slot/port* **|** *slot***] remote-system [med {network-policy | inventory}]**

Syntax Definitions

slot/port	Slot number for the module and physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
slot	The slot number for a specific module.
network-policy	Display network-policy TLVs from remote Endpoint Devices
inventory	Display inventory management TLVs from remote Endpoint Devices

Defaults

By default, a list of all LLDP ports is displayed.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the *slot/port* or *slot* parameter to display information for a specific port or for all ports on a specific module.

Examples

```
-> show lldp 1/22 remote-system med network-policy
Slot/  Remote   Application      Unknown    Tagged    Vlan     Layer2   DSCP
Port    ID         Type         Policy Flag Flag       Id     Priority  Value
------+------+--------------+-----------+---------+------+----------+------
 1/22   1        Voice(01)         Defined  Untagged   345       4        34
 1/22   2        Guest Voice(4)    Defined  Untagged    50       3        46
```

output definitions

Slot/Port	The Slot number to which the remote system entry is associated and the physical port number on that module.
Remote ID	The Index of the Remote Device.
Application Type	The Application type of the peer entity. 1. Voice 2. Voice Signaling 3. Guest Voice 4. Guest Voice Signaling 5. Softphone Voice 6. Video Conferencing 7. Streaming Video 8. Video Signaling

output definitions (continued)

Unknown Policy Flag	Whether the network policy for the specified application type is currently defined or unknown.
Tagged Flag	Whether the specified application type is using a **tagged** or an **untagged** VLAN.
VLAN ID	The VLAN identifier (VID) for the port.
Layer 2 Priority	Layer 2 priority to be used for the specified application type.
DSCP Value	DSCP value to be used to provide Diffserv node behavior for the specified application type.

```
-> show lldp 1/22 remote-system med inventory
Remote LLDP Agents on Local Slot/Port 1/22:

    Chassis 80:40:c9:e6:80:40, Port 00:80:9f:56:09:d9:
      Remote ID                     = 2,
      Hardware Revision             = "3GV23014ADCA070415",
      Firmware Revision             = "NOE 4.20.60",
      Software Revision             = "NOE 4.20.60",
      Serial Number                 = "H0400408605787",
      Manufacturer Name             = "Alcatel-Lucent Enterprise",
      Model Name                    = "IP Touch 4068 FE",
      Asset Id                      = "00:80:9f:56:09:d9",
```

output definitions

Remote ID	The Index of the Remote Device.
MED Hardware Revision	The Hardware Revision of the endpoint
MED Firmware Revision	The Firmware Revision of the endpoint.
MED Software Revision	The Software Revision of the endpoint.
MED Manufacturer Name	The Manufacturer Name of the endpoint.
MED Model Name	The Model Name of the endpoint.
MED Asset ID	The Asset ID of the endpoint.

Release History

Release 6.3.4; command introduced.

Related Commands

show lldp local-port	Displays per port information.
show lldp local-system	Displays local system information.

MIB Objects

```
lldpXMedRemMediaPolicyTable
   lldpXMedRemMediaPolicyAppType
   lldpXMedRemMediaPolicyDscp
   lldpXMedRemMediaPolicyPriority
   lldpXMedRemMediaPolicyTagged
   lldpXMedRemMediaPolicyUnknown
```

```
  lldpXMedRemMediaPolicyVlanID
lldpXMedRemInventoryTable
  lldpXMedRemAssetID
  lldpXMedRemFirmwareRev
  lldpXMedRemHardwareRev
  lldpXMedRemMfgName
  lldpXMedRemModelName
  lldpXMedRemSerialNum
  lldpXMedRemSoftwareRev
```

lldp trust-agent

Enables or disables the security mechanism globally (chassis level) or for a slot or a single port. By enabling LLDP security mechanism on a port, LLDP CMM task brings the LLDP status of the port as trusted and monitors the port for any LLDP security violation.

lldp {*slot/port***|** *slot* | **chassis} trust-agent {enable** | **disable} [chassis-id-subtype {chassis-component** | **interface-alias** | **port-component** | **mac-address** | **network-address** | **interface-name** | **locally-assigned** | **any}]**

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
slot	The slot number for the module (for example, 3 specifies slot 3)
chassis	Specifies all the ports in the chassis.
enable	Enables LLDP security mechanism.
disable	Disables LLDP security mechanism.
chassis-component	The chassis component is used for validating the remote agent.
interface-alias	The alias configured for the interface is used for validating the remote agent.
port-component	The port component is used for validating the remote agent.
mac-address	The MAC address is used for validating the remote agent.
network-address	The network address is used for validating the remote agent.
interface-name	The interface name is used for validating the remote agent.
locally-assigned	The locally assigned component is used for validating the remote agent, that is the chassis information, which can be locally assigned (the local configuration)
any	The remote agent with any chassis ID sub type is accepted as a trust agent.

Defaults

'**any**' - If the chassis ID sub type is not configured for validating the remote agent, by default, the first remote agent is accepted as a trust agent considering any of the chassis ID sub types.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- By enabling security on chassis/slot level, the ports that come under the respective level are monitored for any LLDP security violation.
- If the chassis ID sub type is not configured for validating the remote agent, then the LLDP learns the first remote agent with available chassis ID TLV (Time, Length, Value) received in the PDU.
- After a link up is received on a LLDP security enabled port, LLDP CMM waits for three times the LLDP timer interval (30 seconds). If no LLDP PDU is received after link up that has no remote agent, the port is moved to a violation state.
- If a trusted remote agent already exists, and if no LLDP remote agent is learned even after three times the LLDP timer interval (30 seconds), the port is moved to a violation state. If a new LLDP remote agent is learned after the link toggle, then the port is moved to a violation state.
- If the same chassis ID and port ID already exist in the trusted remote agent database but on a different port, then the port remote agent is learned and the port is moved to a violation state. If a new LLDP remote agent is learned on a port that has a trusted LLDP remote agent, then the port is moved to a violation state.

Examples

```
-> lldp chassis trust-agent enable

-> lldp chassis trust-agent chassis-id-subtype chassis-component
```

Release History

Release 6.4.4; command introduced.

Related Commands

lldp trust-agent violation-action	Sets the action to be performed when a violation is detected.
show lldp trusted remote-agent	Displays information on trusted remote-agents.
show lldp trust-agent	Displays information on local LLDP agent or port.

MIB Objects

```
alaLldpTrustAdminStatus
   alaLldpTrustChassisIdSubType
```

lldp trust-agent violation-action

Sets the action to be performed when a violation is detected.

lldp {*slot/port***|** *slot* **| chassis} trust-agent violation-action {trap-and-shutdown | trap | shutdown}**

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
slot	The slot number for the module (for example, 3 specifies slot 3)
chassis	All switch ports.
trap-and-shutdown	Shuts down the port and sends a trap notification when a violation is detected.
trap	Sends a trap notification when a violation is detected.
shutdown	Shuts down the port when a violation is detected.

Defaults

By default, trust agent violation action is set to ‘trap’.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- If the port is in a shutdown state, clear the violation on the port by using the command “**interfaces** *slot***[***/port***[***-port2***]] clear-violation-all**”
- Clearing the violation on a port does not clear the trusted remote agent existing on that port. To clear the trusted remote agent, disable the LLDP security mechanism on the port.
- If the port is in a shutdown state due to violation and the port link is toggled, only the link goes up. The port still remains in the violation state and the trusted remote agent existing on that port is not cleared.

Examples

```
-> lldp chassis trust-agent violation-action trap

-> lldp 3 trust-agent violation-action shutdown
```

Release History

Release 6.4.4; command introduced.

Related Commands

lldp trust-agent	Sets the status of trust admin status for a port.
show lldp trusted remote-agent	Displays information on trusted remote-agents.
show lldp trust-agent	Displays information on local LLDP agent or port.

MIB Objects

```
alaLldpTrustAction
```

show lldp trusted remote-agent

Displays information on trusted remote-agents.

show lldp [*num* | *slot/port***] trusted remote-agent**

Syntax Definitions

num	The slot number for the module (for example, 3 specifies slot 3)
slot/port	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the slot/port or slot parameter to display information for a specific port or for all ports on a specific module.
- LLDP trust agent must be enabled globally on the chassis or individually on a port in order to get the **show lldp trusted remote-agent** command output.

Examples

```
-> lldp chassis trust-agent enable

-> lldp chassis trust-agent chassis-id-subtype mac-address

-> show lldp trusted remote-agent

Trusted Remote LLDP Agents on Local Slot/Port: 1/7
  Chassis ID Subtype          = 4 (MAC Address),
  Chassis ID                  = 00:e0:b1:7a:e6:3c,
  Port ID Subtype             = 7 (Locally assigned),
  Port ID                     = 1017
```

output definitions

Trusted Remote LLDP Agents on Local Slot/Port	The slot number to which the remote trusted agent is associated and the physical port number on that module.
Chassis ID Subtype	The sub type that describes the chassis ID.
Chassis ID	The chassis ID (MAC address).
Port ID Subtype	The sub type that describes port ID.
Port ID	The port ID (Port MAC).

Release History

Release 6.4.4; command introduced.

Related Commands

lldp trust-agent	Sets the status of trust admin status for a port.
lldp trust-agent violation-action	Sets the action to be performed when a violation is detected.
show lldp trust-agent	Displays information on local LLDP agent/port.

MIB Objects

N/A

show lldp trust-agent

Displays information of the local LLDP agent or port.

show lldp [*slot* | *slot/port***] trust-agent**

Syntax Definitions

slot	The slot number for the module (for example, 3 specifies slot 3)
slot/port	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the *slot/port* or *num* (slot number) values to display information for a specific port or for all ports on a specific module.
- LLDP trust agent must be enabled globally on the chassis or individually on a port in order to get the **show lldp trust-agent** command output correctly.
- If LLDP security is disabled this command correctly displays the ‘Admin Status’ as ‘Disabled’; however the other output parameters will display their default values.

Examples

```
-> lldp chassis trust-agent enable

-> lldp chassis trust-agent chassis-id-subtype chassis-component

-> show lldp trust-agent

Slot/Port  Admin Status   Violation Action  Violation Status   Chassis Subtype
---------+--------------+-----------------+------------------+-----------------
   1/1     Enabled        Trap Only         Trusted            1(Chassis Component)
   1/2     Enabled        Trap Only         Trusted            1(Chassis Component)
   1/3     Enabled        Trap Only         Trusted            1(Chassis Component)
   1/4     Disabled       Shutdown          Violated           1(Chassis Component)
   1/5     Enabled        Shutdown          Trusted            1(Chassis Component)
   1/6     Enabled        Trap-and-Shutdown Trusted            1(Chassis Component)
   1/7     Disabled       Trap-and-Shutdown Violated           1(Chassis Component)
   1/8     Enabled        Trap Only         Trusted            1(Chassis Component)
   1/9     Enabled        Trap Only         Trusted            1(Chassis Component)
   1/10    Enabled        Trap Only         Trusted            1(Chassis Component)
```

output definitions

Slot/Port	The LLDP slot and port number.
Admin Status	Indicates the administrative status of the LLDP port, **Enabled** or **Disabled**
Violation Action	Indicates the action performed when a violation is detected. The options are - **Trap Only**, **Trap-and-Shutdown**, and **Shutdown Only**.
Violation Status	The violation status of the port, **Trusted** or **Violated**
Chassis Subtype	The sub type that describes the chassis ID.

Release History

Release 6.4.4; command introduced.

Related Commands

lldp trust-agent	Sets the status of trust admin status for a port.
lldp trust-agent violation-action	Sets the action to be performed when a violation is detected.
show lldp trusted remote-agent	Displays information on trusted remote-agents.

MIB Objects

N/A

17 Interswitch Protocol Commands

Alcatel-Lucent Interswitch Protocols (AIP) are used to discover and advertise adjacent switch information. Only one protocol is supported:

- Alcatel-Lucent 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 is 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-Lucent 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 17-5).

Examples

```
-> amap discovery 1200
-> amap discovery time 600
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

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 17-3) has expired.

Examples

```
-> amap common 1200
-> amap common time 600
```

Release History

Release 6.1; 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 the 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 6400, 6850E, 6855, 9000E

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 6.1; 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 the active Spanning Tree ports in the common transmission state.

18 SIP Commands

SIP Snooping feature address the key challenge of real time delivery and monitoring requirements for media streams from SIP devices. SIP snooping feature provides plug and play support to the device, where it automatically identifies the ports used. It also enhances the security of device.

SIP Snooping prioritizes voice and video traffic over non-voice traffic. To summarize, SIP Snooping:

- Identifies and marks the SIP and its corresponding media streams. Each media stream contains Real Time Protocol (RTP) and Real Time Control Protocol (RTCP) flows. Marking is done using the DSCP field in the IP header.
- Provides user configured QOS treatment for SIP/RTP/RTCP traffic flows based on its marking.
- Also snoops voice quality metrics of media streams from their RTCP packets and displays them to the user with knowledge of media reception quality in real time and helps to diagnose the problems on their quality. Also in addition, trap will be generated when voice quality parameters like Jitter, Round trip time, Packet-lost, R-factor and MOS values of media streams crosses user configured threshold.

Note. SIP Snooping is not supported in OS 6400 and OS 6855 –P14/C14

This chapter includes descriptions of SIP commands.

MIB information for SIP commands is as follows:

Filename: AlcatelIND1SIPSnooping.MIB
Module: ALCATEL-IND1-CHASSIS-MIB

A summary of the available commands is listed here:

---

sip-snooping enable
sip-snooping port enable
sip-snooping mode
sip-snooping trusted server
sip-snooping sip-control
sip-snooping sos-call number
sip-snooping sos-call dscp
sip-snooping udp port
sip-snooping tcp port
sip-snooping threshold
sip-snooping logging-threshold num-of-calls
show sip-snooping call-records
clear sip-snooping statistics
show sip-snooping config
show sip-snooping ports
show sip-snooping statistics
show qos dscp-table

---

sip-snooping enable

Enables or disables the SIP snooping on the switch.

sip-snooping {enable | disable}

Syntax Definitions

enable	Enables SIP snooping
disable	Disables SIP snooping

Defaults

By default, SIP-snooping is disabled on the switch.

Platforms Supported

OmniSwitch 6850E,9000E,6855-U24X

Usage Guidelines

- If SIP snooping is disabled at a port level, enabling SIP snooping globally will not override the configuration of that port.
- If SIP-snooping is disabled and enabled, it is mandatory that the phones re-register for successful DSCP marking.

Examples

```
-> sip-snooping enable
-> sip-snooping disable
```

Release History

Release 6.4.5; command was introduced.

Related Commands

sip-snooping port enable	Configures the status of SIP snooping on a single port, a range of ports, or on a link aggregate of ports.
show sip-snooping ports	Shows the SIP snooping port level data.
show sip-snooping config	

MIB Objects

`aluSIPSnoopingStatus`

sip-snooping port enable

Configures the status of SIP snooping on a single port, a range of ports, or on a link aggregate.

sip-snooping[{port *slot/port1***[**-*port2***] | linkagg** *linkagg_num***] {enable|disable}**

Syntax Definitions

slot/port1	The slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
-port2	The last port number in a range of ports that you want to configure on the same slot (e.g, 3/1-4 specifies ports 1, 2, 3, and 4 on slot 3).
linkagg_num	Specifies the link aggregate port ID.
enable	Enables SIP snooping to mirror all SIP PDU that ingress on that port
disable	Disables SIP snooping and will not mirror SIP PDU that ingress on that port.

Defaults

By default, SIP-snooping is disabled on the switch.

Platforms Supported

OmniSwitch 6850E,9000E,6855-U24X

Usage Guidelines

- Use this command for port/linkagg level SIP Snooping configuration on the switch.
- SIP snooping must be enabled globally to activate port/linkagg level configuration.
- Even after SIP snooping is globally disabled, port/linkagg level configuration is saved. This configuration will be used when SIP snooping is enabled globally again.
- Port level configuration is not allowed of a member port of a linkagg.
- If a port join a linkagg, port level configuration is overridden by linkagg configuration. Port level configuration will be activated if it leaves the linkagg.

Examples

```
-> sip-snooping port 1/5-6 enable
-> sip-snooping linkagg 10 enable
```

Release History

Release 6.4.5; command was introduced.

Related Commands

show sip-snooping ports	Shows the SIP snooping port level data.

MIB Objects

```
aluSIPSnoopingSlotPortIndex
   aluSIPSnoopingLinkAgg
   aluSIPSnoopingPortStatus
   aluSIPSnoopingRowStatus
```

sip-snooping mode

Configure port/linkagg mode of SIP snooping on the switch.

sip-snooping[{port *slot/port* **[-port2] | linkagg** *agg_num* **mode {force-edge | force-non-edge | automatic}**

Syntax Definitions

slot/port1[-port2]	The slot and port number (3/1). Use a hyphen to specify a range of ports and/or a space to specify multiple port entries (3/1-10 4/1 4/5 5/10).
agg_num	The link aggregate ID number.
force-edge	Media TCAM entries to be created for dialogs that transverse the specific port
force-non-edge	No Media TCAM entries for dialogs that transverse the specific port.
automatic	Sets to default mode. The port's edge/non-edge mode is derived by the switch/router based on LLDP received or not on the port.

Defaults

parameter	default
mode	automatic

Platforms Supported

OmniSwitch 6850E,9000E,6855-U24X

Usage Guidelines

- Use this command for port/linkagg level SIP Snooping configuration on the switch.
- Force-edge-port/force-nonedge-port option to overwrite default port mode learnt by either received or not received switch/router capability through LLDP.
- Port level configuration is not allowed of a member port of a linkagg.
- If a port joins a linkagg, port level configuration is overridden by linkagg configuration. Port level configuration will be activated if it leaves the linkagg.

Examples

```
-> sip-snooping port 1/5-6 mode force-edge
-> sip-snooping linkagg 1 mode force-non-edge
```

Release History

Release 6.4.5; command was introduced.

Related Commands

show sip-snooping ports	Shows the SIP snooping port level data.

MIB Objects

```
aluSIPSnoopingSlotPortIndex
   aluSIPSnoopingLinkAgg
   aluSIPSnoopingPortMode
   aluSIPSnoopingRowStatus
```

sip-snooping trusted server

Configure the IP addresses of the trusted servers on a switch.

sip-snooping trusted-server [*ip_address1 ip_address2 ip_address ...ip_address8***]**
no sip-snooping trusted-server *all*
no sip-snooping trusted-server [*ip_address***]**

Syntax Definitions

ip_address1**[-***ip_address2***]**	The IP Addresses of the trusted-server.
all	Specifies all the IP addresses.

Defaults

By default, no trusted servers are configured.
All SIP based calls using any call server will be supported.

Platforms Supported

OmniSwitch 6850E,9000E,6855-U24X

Usage Guidelines

- This command is used to configure the IP addresses of the trusted servers. If trusted server is configured, then only the calls initiated through those servers will be supported.
- A maximum of 8 trusted servers can be configured.
- If no trust servers are configured, all SIP based calls using any call server will be supported.
- Use "**No**" form of the command to remove any trusted IP or all trusted IPs, which were configured earlier.
- No command is used to remove all trusted server IP configured earlier

Examples

```
-> sip-snooping trusted-server 192.254.32.22 192.254.32.33
-> no sip-snooping trusted-server 192.254.32.22
-> no sip-snooping trusted-server all
```

Release History

Release 6.4.5; command was introduced.

Related Commands

show sip-snooping config	Shows the configuration done for SIP snooping.

MIB Objects

```
aluSIPSnoopingSIPTrustedServerIPAddress1
aluSIPSnoopingSIPTrustedServerIPAddress2
aluSIPSnoopingSIPTrustedServerIPAddress3
aluSIPSnoopingSIPTrustedServerIPAddress4
aluSIPSnoopingSIPTrustedServerIPAddress5
aluSIPSnoopingSIPTrustedServerIPAddress6
aluSIPSnoopingSIPTrustedServerIPAddress7
aluSIPSnoopingSIPTrustedServerIPAddress8
```

sip-snooping sip-control

Configures SIP control DSCP marking.

sip-snooping sip-control dscp *num*

sip-snooping sip-control no dscp

Syntax Definitions

num	The DSCP number.

Defaults

By default no marking/priotizing or rate limit is performed. The packet gets its priority as normal packet. Either from the qos port configuration (trust the packet DSCP or untrusted) or from a user configured policy.

Platforms Supported

OmniSwitch 6850E,9000E,6855-U24X

Usage Guidelines

- This command is used for the SIP control DSCP marking. A in-built rate limiter of 1 mbps is configured to rate limit SIP PDUs being marked by the switch.
- The allowed DSCP range is 0-63.
- Use **no** form of the command is to set default mode.

Examples

```
-> sip-snooping sip-control dscp 40
-> sip-snooping sip-control no dscp
```

Release History

Release 6.4.5; command was introduced.

Related Commands

show sip-snooping config	Shows the configuration done for SIP snooping.

MIB Objects

```
aluSIPSnoopingSIPControlDSCP
```

sip-snooping sos-call number

Configures the SOS call strings in SIP snooping.

sip-snooping sos-call number <*string1*> <*string2*> **…** <*string4*>
no sip-snooping sos-call number <*string*>
no sip-snooping sos-call number all

Syntax Definitions

<*string1*> **…** <*string4*> Specifies the SOS call number.

Defaults

None

Platforms Supported

OmniSwitch 6850E,9000E,6855-U24X

Usage Guidelines

- This command is used for the configuration of the SOS call strings. A maximum of 4 SOS call strings can be configured for an exact match on the “to” URI (user part only)
- No support of regular expression. If no string is specified, no SOS call can be identified in the system.
- Use **NO** form of this command to remove an already configured sos-call string.

Examples

```
-> sip-snooping sos-call number “911” “2233”
-> no sip-snooping sos-call number “911”
-> no sip-snooping sos-call number all
```

Release History

Release 6.4.5; command was introduced.

Related Commands

show sip-snooping config Shows the configuration done for SIP snooping.

MIB Objects

```
aluSIPSnoopingSOSCallNumber1
aluSIPSnoopingSOSCallNumber2
aluSIPSnoopingSOSCallNumber3
aluSIPSnoopingSOSCallNumber4
```

sip-snooping sos-call dscp

Configures the SOS-Call RTP/RTCP DSCP Marking.

sip-snooping sos-call dscp *num*

Syntax Definitions

num	Specifies the DSCP number.

Defaults

The default configuration is 46 EF.

Platforms Supported

OmniSwitch 6850E,9000E,6855-U24X

Usage Guidelines

- This command is used for the configuration of the SOS-Call RTP/RTCP DSCP Marking. An in-built rate limiter of 128 kbps is configured to rate limit uni direction media stream being marked by the switch.
- SOS calls are identified only for the Audio media type. All other media type calls to be considered normal calls.

Examples

```
-> sip-snooping sos-call dscp 56
```

Release History

Release 6.4.5; command was introduced.

Related Commands

show sip-snooping config	Shows the configuration done for SIP snooping.

MIB Objects

`aluSIPSnoopingSOSCallDSCP`

sip-snooping udp port

Configures the UDP port for SIP Snooping.

sip-snooping udp-port <*udp-port1*> < *udp-port 2*> **...** < *udp-port 8*>
no sip-snooping udp-port <*udp-port*>
no sip-snooping udp-port all

Syntax Definitions

< *udp-port 1*> **...** < *udp-port 8*> Specifies the SIP snooping UDP port.

Defaults

By default no UDP ports and SIP mirroring is performed with the method name and SIP2.0 strings.

Platforms Supported

OmniSwitch 6850E,9000E,6855-U24X

Usage Guidelines

- A maximum of 8 UDP ports can be configured on a switch.
- Use **NO** form of this command to remove any UDP port configured earlier.

Examples

```
-> sip-snooping udp-port 5260 5060
-> no sip-snooping udp-port 5260
-> no sip-snooping udp-port all
```

Release History

Release 6.4.5; command was introduced.

Related Commands

show sip-snooping config Shows the configuration done for SIP snooping.

MIB Objects

```
aluSIPSnoopingSIPUDPPort1
aluSIPSnoopingSIPUDPPort2
aluSIPSnoopingSIPUDPPort3
aluSIPSnoopingSIPUDPPort4
aluSIPSnoopingSIPUDPPort5
aluSIPSnoopingSIPUDPPort6
aluSIPSnoopingSIPUDPPort7
aluSIPSnoopingSIPUDPPort8
```

sip-snooping tcp port

Configure the Server listening TCP ports for SIP Snooping.

sip-snooping tcp-port <*tcp-port1*> < *tcp-port 2*> **...** < *tcp-port 8*>
no sip-snooping tcp-port <*tcp-port*>
no sip-snooping tcp-port all

Syntax Definitions

< *tcp-port 1*> **...** < *tcp-port 8*> Specifies the SIP snooping TCP port.

Defaults

By default, TCP port is 5260.

Platforms Supported

OmniSwitch 6850E,9000E,6855-U24X

Usage Guidelines

- A maximum of 8 TCP ports can be configured on a switch.
- The default port will be overwritten, if the user configures any other port.
- Use **NO** form of this command to remove any TCP port configured earlier.

Examples

```
-> sip-snooping tcp-port 5260 5060
-> no sip-snooping tcp-port 5260
-> no sip-snooping tcp-port all
```

Release History

Release 6.4.5; command was introduced.

Related Commands

show sip-snooping config Shows the configuration done for SIP snooping.

MIB Objects

```
aluSIPSnoopingSIPTCPPort1
aluSIPSnoopingSIPTCPPort2
aluSIPSnoopingSIPTCPPort3
aluSIPSnoopingSIPTCPPort4
aluSIPSnoopingSIPTCPPort5
aluSIPSnoopingSIPTCPPort6
aluSIPSnoopingSIPTCPPort7
aluSIPSnoopingSIPUDPPort8
```

sip-snooping threshold

Configure the various thresholds of SIP snooping.

sip-snooping threshold {audio | video | other} {jitter *jitter_ms_num* **| packet-lost** *% num* **| round-trip-delay** *round_trip_delay_ms_num* **| R-factor** *Rfactor_num*| **MOS** *mos_num***}**

Syntax Definitions

audio	Specify threshold for audio.
video	Specify threshold for video.
other	Specify threshold for other.
jitter	Specify jitter in milliseconds.
packet-lost	Specify packet lost in percentage.
round-trip-delay	Set round trip delay in milliseconds.
R-factor	Specify R-factor number.
MOS	Specify MOS number

Defaults

parameter	default
RTCP monitoring	Enable
Jitter Threshold (audio/video/other)	50/100/100 ms
Packet-lost Threshold (audio/video/other)	10 /20/20 %
RTT Threshold (audio/video/other)	180 /250/250 ms
R-factor Threshold (audio/video/other)	70/80/80
MOS Threshold (audio/video/other)	3.6/3.0/3.0

Platforms Supported

OmniSwitch 6850E,9000E,6855-U24X

Usage Guidelines

- This command is used for the configuration of various thresholds.
- The valid range for jitter is 0-300
- The valid range for packet-loss is 0-99%.
- The allowed range for round-trip-delay is 0-500 milliseconds.
- The allowed range for R-factor is 0-100.

- The allowed range for MOS is 0-5.
- Setting value to 0 would disable threshold checking for that parameter.

Examples

```
-> sip-snooping threshold audio jitter 50
-> sip-snooping threshold audio packet-lost 10
-> sip-snooping threshold video jitter 80
-> sip-snooping threshold video round-trip-delay 180
```

Release History

Release 6.4.5; command was introduced.

Related Commands

show sip-snooping config	Shows the configuration done for SIP snooping.

MIB Objects

```
aluSIPSnoopingThresholdMedium
aluSIPSnoopingThresholdJitter
aluSIPSnoopingThresholdPacketLost
aluSIPSnoopingThresholdRoundTripDelay
aluSIPSnoopingThresholdRFactor
aluSIPSnoopingThresholdMOS
```

sip-snooping logging-threshold num-of-calls

Configures the threshold for the number of calls to be logged on to the flash file.

sip-snooping logging-threshold num-of-calls *num*

Syntax Definitions

num	Specifies the maximum number of calls to be logged.

Defaults

By default, 200 calls can be logged.

Platforms Supported

OmniSwitch 6850E,9000E,6855-U24X

Usage Guidelines

This command is used to configure the threshold for the number of calls to be logged on to the flashfile.

Examples

```
-> sip-snooping logging-threshold num-of-calls 300
```

Release History

Release 6.4.5; command was introduced.

Related Commands

show sip-snooping config	Shows the configuration done for SIP snooping.

MIB Objects

```
aluSIPSnoopingThresholdNumberOfCalls
```

show sip-snooping call-records

Displays the SIP-snooping active/ended call records.

show sip-snooping call-records {active-calls|ended-calls} [full | threshold-violation]

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E,9000E,6855-U24X

Usage Guidelines

- This command is used to show the SIP-snooping active/ended call records.

Examples

```
-> show sip-snooping call-records ended-calls full
Legend: start date time duration media-type end-reason
         call-id / from-tag / to-tag
         IP address port DSCP (forward/reverse)
         policy-rule (F/R)
         Pkt count (F/R)
         statistics min / max / avg %samples exceeding threshold (F/R)

------------------------------------------------------------------------
2012-01-30 09:12:30 UTC 9999d 02h 22m 03s Audio Normal
01234567890123456789012345678901234567890123456789012345678901234567890123 /
012345678901234567890123456789012 / 012345678901234567890123456789012
IP/DSCP 222.222.222.222 22222 63/63 111.111.111.111 11111 63/63
Policy-Rule SIP-VLAN10-Rule              SIP-VLAN10-Rule
Pkt-Count 9999999999                     9999999999
Pkt-Loss   99.9 /  99.9 /  99.9 99%       99.9 /  99.9 /  99.9 99%
Jitter    999.9 / 999.9 / 999.9 99%      999.9 / 999.9 / 999.9 99%
Delay     99999 / 99999 / 99999 99%      99999 / 99999 / 99999 99%
R-factor   99.9 / 99.9  / 99.9            99.9 / 99.9  / 99.9
MOS         4.9 / 4.9   / 4.9              4.9 / 4.9   / 4.9


2012-01-30 09:12:30 UTC 9999d 02h 22m 03s Audio Normal
1j9FpLxk3uxtm8tn@biloxi.example.com / a73kszlf / 1410948204
IP/DSCP   135.254.170.110 18888 46/32    125.54.110.110 29996 46/32
Policy-Rule SIP-Audio-SRCIP              SIP-AUDIO-VLAN100
Pkt-Count 10000                          12000
Pkt-Loss   0.9  /     0 / 2.8  0%         0   / 0      / 1   0%
Jitter      3.7 /     0 / 9    0%       0.1   / 0      / 0.2 0%
Delay      50.1 / 44    / 108
R-factor   70.1 / 55    / 77   0%        70.1 / 55    / 77   0%
```

```
MOS         4.1 / 3.9   / 4.2  0.1%       4.1 / 3.9   / 4.2  0.1%

-------------------------
Number of Call Records: 2

-> show sip-snooping call-records ended-calls
Legend: start date time duration media-type end-reason
         call-id / from-tag / to-tag
         IP address port DSCP (forward/reverse)
         policy-rule (F/R)

------------------------------------------------------------------------
2012-01-30 09:12:30 UTC 9999d 02h 22m 03s Audio Normal
01234567890123456789012345678901234567890123456789012345678901234567890123 /
01234567890123456789012345678901 / 01234567890123456789012345678901
IP/DSCP 222.222.222.222 22222 63/63 111.111.111.111 11111 63/63
Policy-Rule SIP-VLAN10-Rule              SIP-VLAN10-Rule

2012-01-30 09:12:30 UTC 9999d 02h 22m 03s Audio Normal
1j9FpLxk3uxtm8tn@biloxi.example.com / a73kszlf / 1410948204
IP/DSCP   135.254.170.110 18888 46/32    125.54.110.110 29996 46/32
Policy-Rule SIP-Audio-SRCIP              SIP-AUDIO-VLAN100

-------------------------
Number of Call Records: 2

-> show sip-snooping call-records active-calls threshold-violation
Legend: start date time duration media-type end-reason
         call-id / from-tag / to-tag
         IP address port DSCP (forward/reverse)
         policy-rule (F/R)
         statistics min / max / avg %samples exceeding threshold (F/R)

------------------------------------------------------------------------
2012-01-30 09:12:30 UTC 9999d 02h 22m 03s Audio -
1j9FpLxk3uxtm8tn@biloxi.example.com / a73kszlf / 1410948204
IP/DSCP   135.254.170.110 18888 46/32    125.54.110.110 29996 46/32
Policy-Rule SIP-AUDIO-SRCIP              SIP-AUDIO-VLAN100
MOS         4.1 / 3.9   / 4.2  0.1%       4.1 / 3.9   / 4.2  0.1%
-------------------------
Number of Call Records: 1
```

output definitions

Policy-Rule	Name of the SIP policy rule.
Pkt-Count	Packet Count in percentage for SIP Snooping.
Pkt-Loss	Packet Loss in percentage for SIP Snooping.
Jitter	Jitter threshold in millisec for SIP Snooping.
Delay	Round trip delay in millisec for SIP Snooping.
R-factor	R-Factor for SIP Snooping.
MOS	MOS for SIP Snooping multiplied by a factor of 10.
Number of Call Records	Number of call records that can be stored onto the device.

Release History

Release 6.4.5; command was introduced.

Related Commands

show sip-snooping config	Shows the configuration done for SIP snooping.

MIB Objects

```
alaQoSDSCPEntryNumber
alaQoSDSCPPriority
alaQoSDSCPDropPrecedence
```

clear sip-snooping statistics

Clears all the values of SIP snooping statistics

clear sip-snooping statistics

Syntax Definitions

statistics	Specifies SIP snooping statistics.

Defaults

N/A.

Platforms Supported

OmniSwitch 6850E,9000E,6855-U24X

Usage Guidelines

- This command is used to clear all the SIP-snooping statistics.

Examples

```
-> clear sip-snooping statistics
```

Release History

Release 6.4.5; command was introduced.

Related Commands

show sip-snooping statistics	Shows the SIP snooping statistics.

MIB Objects

```
aluSIPSnoopingClearStats
aluSIPSnoopingClearLogs
```

show sip-snooping config

Shows the configuration done for SIP snooping.

show sip-snooping config

Syntax Definitions

N/A

Defaults

N/A.

Platforms Supported

OmniSwitch 6850E,9000E,6855-U24X

Usage Guidelines

This command is used to show the configuration done for SIP-snooping.

Examples

```
-> show sip-snooping config
Sip-snooping Status : Enable,
Sip-control DSCP : 40,
SOS-Call RTP/RTCP DSCP : 35,
SOS-Call Number : 911, 2233,
Jitter Threshold (audio/video/other) : 50ms/100ms/100ms,
Packet-Lost Threshold (audio/video/other) : 10/20/20,
Round-Trip-Delay Threshold (audio/video/other) : 180ms/250ms/250ms,
R-factor Threshold (audio/video/other) : 70/80/80,
MOS Threshold (audio/video/other) :36/30/30 ,
Logging Number of calls : 200,
UDP-Port(s) : 5060, 5260
TCP-Port(s) : 5260
Trusted Server IP(s) : 192.254.32.11,192.254.32.22,192.254.32.33
```

output definitions

Sip-snooping Status	Indicates whether the SIP Snooping status is Enable or Disable.
Sip-control DSCP	Displays the SIP control DSCP value
SOS-Call RTP/RTCP DSCP	Displays the SOS-Call RTP/RTCP DSCP number.
SOS-Call Number	Displays the emergency call number.
Jitter Threshold	Displays the Jitter threshold in milliseconds.
Packet-Lost Threshold	Displays the packet lost threshold in percentage.
Round-Trip-Delay Threshold	Displays the Round-Trip-Delay threshold period in milliseconds.
R-factor Threshold	Displays the R-Factor value.
MOS Threshold	Displays the MOS for SIP Snooping multiplied by a factor of 10.

output definitions (continued)

Logging Number of calls	Displays the maximum number of calls to be logged in flash file
UDP-Ports	Displays the SIP Snooping UDP Ports.
TCP Ports	Displays the SIP Snooping TCP ports.
Trusted Server IP(s)	Displays the truster server IP addresses.

Release History

Release 6.4.5; command was introduced.

Related Commands

show sip-snooping statistics	Shows the SIP snooping statistics.
clear sip-snooping statistics	Clears all the logs of SIP snooping statistics

MIB Objects

```
aluSIPSnoopingStatus
aluSIPSnoopingSIPControlDSCP
aluSIPSnoopingSOSCallRTPDSCP
aluSIPSnoopingSOSCallNumber1
aluSIPSnoopingSOSCallNumber2
aluSIPSnoopingSOSCallNumber3
aluSIPSnoopingSOSCallNumber4
aluSIPSnoopingThresholdMedium
aluSIPSnoopingThresholdJitter
aluSIPSnoopingThresholdPacketLost
aluSIPSnoopingThresholdRoundTripDelay
aluSIPSnoopingThresholdNumberOfCalls
aluSIPSnoopingSIPTrustedServerIPAddress1
aluSIPSnoopingSIPTrustedServerIPAddress2
aluSIPSnoopingSIPTrustedServerIPAddress3
aluSIPSnoopingSIPTrustedServerIPAddress4
aluSIPSnoopingSIPTrustedServerIPAddress5
aluSIPSnoopingSIPTrustedServerIPAddress6
aluSIPSnoopingSIPTrustedServerIPAddress7
aluSIPSnoopingSIPTrustedServerIPAddress8
aluSIPSnoopingSIPUDPPort1
aluSIPSnoopingSIPUDPPort2
aluSIPSnoopingSIPUDPPort3
aluSIPSnoopingSIPUDPPort4
aluSIPSnoopingSIPUDPPort5
aluSIPSnoopingSIPUDPPort6
aluSIPSnoopingSIPUDPPort7
aluSIPSnoopingSIPUDPPort8
```

show sip-snooping ports

Shows the SIP snooping port level data.

show sip-snooping ports

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E,9000E,6855-U24X

Usage Guidelines

This command is used to show the SIP-snooping port-level data.

Examples

```
-> show sip-snooping ports
Legend : sip snooping : * status disabled (Sip-snooping globally disabled)
Port       sip-snooping         Edge/Non-edge
-----------------------------------------------------------
1/1        enable               automatic
1/2        disable              automatic
1/3        enable (*)           force-edge
1/3        enable (*)           force-non-edge
```

output definitions

Port	Displays ports configured for sip-snooping.
sip-snooping	Displays the status of sip-snooping on the port, **enable** or **disable**.
Edge/Non-edge	Displays the edge status of the port.

Release History

Release 6.4.5; command was introduced.

Related Commands

show sip-snooping statistics	Shows the SIP snooping statistics.

MIB Objects

```
aluSIPSnoopingSlotPortIndex
aluSIPSnoopingLinkAgg
```

```
aluSIPSnoopingPortStatus
aluSIPSnoopingRowStatus
```

show sip-snooping statistics

Shows the SIP snooping statistics.

show sip-snooping statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E,9000E,6855-U24X

Usage Guidelines

This command is used to show the SIP-snooping statistics.

Examples

```
-> show sip-snooping statistics
Total calls processed                  : ,
Total audio streams                    : ,
Total video streams                    : ,
Total other streams                    : ,
Total audio streams that crossed threshold       : ,
Total video streams that crossed threshold       : ,
Total other streams that crossed threshold       : ,
Active Streams that crossed threshold            : ,
Number of Active calls                 : ,
Number of active audio streams         : ,
Number of active video streams         : ,
Number of active other streams         : ,
Number of SIP packet received by hardware :
Number of SIP packet received by software :
Number of SIP packet received per method: INVITE(100) ACK(101) BYE(200)
UPDATE(40) PRACK(20)
Number of SIP response packet received:
Number of discarded/malformed/unsupported SIP packets:
Number of discarded SIP packets not from/to trusted servers:
Number of dropped SIP packet due the software error:
(NI overflow, NI/CMM, CMM overflow)
Total Emergency Calls                  :
```

output definitions

Total calls processed	Total calls processed for SIP Snooping.
Total audio streams	Displays the total audio streams.
Total video streams	Displays the total video streams.

output definitions (continued)

Total other streams	Displays the total other streams.
Total audio streams that crossed threshold	Displays the total audio streams that have exceeded threshold.
Total video streams that crossed threshold	Displays the total video streams that have exceeded threshold.
Total other streams that crossed threshold	Displays the total other streams that have exceeded threshold.
Number of Active calls	Displays the number of active calls.
Number of Active audio streams	Displays the number of active audio streams.
Number of Active video streams	Displays the number of active video streams.
Number of Active other streams	Displays the number of active other streams.
Number of SIP packet received by hardware	Displays the total SIP packet received by hardware.
Number of SIP packet received by software	Displays the total SIP packet received by software.
Number of SIP packet received by per method	Displays the method by which the SIP packet is received. The various per method are Invite, Ack, Bye, Update and Prack.
Number of SIP response packet received	Displays the total number of SIP response packet received.
Number of discarded/ malformed/unsupported SIP packets	Displays the total number of discarded, malformed or unsupported SIP packets.
Number of discarded SIP packets not from/to trusted servers	Displays the total number of discarded SIP packets not from or to trusted servers
Number of dropped SIP packet due the software error	Displays the Total number of SIP packets dropped due the software error. (i.e. NI overflow, NI/CMM, CMM overflow etc.)
Total Emergency Calls	Displays the total number of Emergency Calls.

Release History

Release 6.4.5; command was introduced.

Related Commands

clear sip-snooping statistics	Clears the SIP snooping statistics.

MIB Objects

```
aluSIPSnoopingTotalCallsProcessed
aluSIPSnoopingTotalAudioStreams
aluSIPSnoopingTotalVideoStreams
aluSIPSnoopingTotalOtherStreams
aluSIPSnoopingAudioStreamsBeyondThreshold
aluSIPSnoopingVideoStreamsBeyondThreshold
```

```
aluSIPSnoopingOtherStreamsBeyondThreshold
aluSIPSnoopingActiveStreamsBeyondThreshold
aluSIPSnoopingActiveAudioStreams
aluSIPSnoopingActiveVideoStreams
aluSIPSnoopingActiveOtherStreams
aluSIPSnoopingHardwareSIPPackets
aluSIPSnoopingSoftwareSIPPackets
aluSIPSnoopingSIPInvitePackets
aluSIPSnoopingSIPAckPackets
aluSIPSnoopingSIPByePackets
aluSIPSnoopingSIPByePackets
aluSIPSnoopingSIPUpdatePackets
aluSIPSnoopingSIPPrackPackets
aluSIPSnoopingSIPRecvdResponsePackets
aluSIPSnoopingSIPDiscardedPackets
aluSIPSnoopingSIPDiscardedNoTrustServerPackets
aluSIPSnoopingSIPDroppedSWErrorPackets
aluSIPSnoopingTotalEmergencyCalls
```

show qos dscp-table

Shows the QoS DSCP table configured.

show qos dscp-table

Syntax Definitions

N/A.

Defaults

N/A.

Platforms Supported

OmniSwitch 6850E,9000E,6855-U24X

Usage Guidelines

- This command is used to show the QoS DSCP table configured.
- This commnd functionality does not work with un-trusted port.

Examples

```
-> show qos dscp-table
DSCP           Priority      Drop-Precedence
-------------------------------------------
34              4               Low
35              4               Low
36              4               Low
37              3               Medium
```

output definitions

DSCP	Displays SIP Snooping DSCP number.
Priority	Displays the priority number of the DSCP table.
Drop-Precedence	Displays the drop precedence of the DSCP table.

Release History

Release 6.4.5; command was introduced.

Related Commands

sip-snooping threshold	Configures the priority and drop-precedence to be associated with the configured DSCP table.

MIB Objects

```
alaQoSDSCPEntryNumber
alaQoSDSCPPriority
alaQoSDSCPDropPrecedence
```

19 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.
- 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 if 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.
- Web Cache Communication Protocol (WCCP)—It provides a mechanism to redirect traffic flows to a cluster of cache servers transparently. The WCCPv2 enabled routers would redirect the traffic on configured protocol (TCP/UDP) ports to the cache engine instead of the intended hosts directly.

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 22, “RIP Commands,” Chapter 27, “OSPF Commands.” For more information on VLANs and RIP see the applicable chapter in the Configuration Guide. For more information on OSPF, see the “Configuring OSPF” chapter in the *OmniSwitch AOS Release 6 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 managed-interface** **ip interface dhcp-client** **ip interface tunnel** **ip router primary-address** **ip router router-id** **ip static-route** **ip route-pref** **ip default-ttl** **ping** **traceroute** **ip dual-hash mode** **ip directed-broadcast** **ip service** **show ip traffic** **show ip interface** **show ip managed-interface** **show ip route** **show ip route-pref** **show ip router database** **show ip emp-route** **show ip config** **show ip protocols** **show ip service**
IP Route Map Redistribution	**ip redist** **ip access-list** **ip access-list address** **ip route-map action** **ip route-map match ip address** **ip route-map match ipv6 address** **ip route-map match ip-nexthop** **ip route-map match ipv6-nexthop** **ip route-map match tag** **ip route-map match ipv4-interface** **ip route-map match ipv6-interface** **ip route-map match metric** **ip route-map match route-type** **ip route-map match protocol** **ip route-map set metric** **ip route-map set metric-type** **ip route-map set tag** **ip route-map set community** **ip route-map set local-preference** **ip route-map set level** **ip route-map set ip-nexthop** **ip route-map set ipv6-nexthop** **show ip redist** **show ip access-list** **show ip route-map**
Multiple Virtual Routing and Forwarding (VRF)	**vrf** **show vrf**
Virtual Routing and Forwarding - Route Leak	**ip export route-map** **ip import vrf** **show ip export** **show ip import** **show ip global-route-table**

ARP	**arp** **clear arp-cache** **ip dos arp-poison restricted-address** **arp filter** **clear arp filter** **show arp** **show arp summary** **show ip dynamic-proxy-arp** **show ip dos arp-poison**
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**
Web Cache Communication Protocol (WCCP)	**ip wccp admin-state** **ip wccp service-group web-cache md5** **ip wccp service-group web-cache restrict** **clear ip wccp** **show ip wccp status** **show ip wccp services** **show ip wccp cache-engines** **show ip wccp restricts** **show ip wccp service-group** **show ip wccp service-group** **show ip wccp service-group detail** **show ip wccp service-group view** **show ip wccp service-group statistics**
IP and ARP Spoofing	**ip dos anti-spoofing** **ip dos anti-spoofing arp-only** **ip dos anti-spoofing address** **ip dos anti-spoofing address arp-only** **ip dos anti-spoofing clear stats** **ip dos anti-spoofing address clear stats** **show ip dos anti-spoofing**

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* **| {rtr-port [***agg_num* | *slot/port***] rtr-vlan** *num* **[type {tagged | untagged}}] [forward | no forward] [local-proxy-arp | no local-proxy-arp] [eth2 | snap] [primary | no primary] [local-host-dbcast [enable | disable]**

no ip interface *name*

Syntax Definitions

name	Text string up to 32 characters. Use quotes around string if description contains multiple words with spaces between them (for example “Alcatel-Lucent Marketing”). This value is case sensitive.
ip_address	An IP host address (for example, 10.0.0.1, 171.15.0.20) to specify the IP router network.
subnet_mask	A valid IP address mask (for example, 255.0.0.0, 255.255.0.0) to identify the IP subnet for the interface.
admin enable	Enables the administrative status for the IP interface.
admin disable	Disables the administrative status for the IP interface.
vid	An existing VLAN ID number (1–4094).
rtr-port	The physical port associated with the IP interface (device type "RTR-PORT"). The rtr-port can be the "slot/ port" to identify the port or the "agg-num" in case of a link aggregation port. This parameter is mandatory for an RTR-PORT IP interface.
rtr-vlan	An unused VLAN on the system to be associated with this IP interface. This parameter is mandatory for an RTR-PORT IP interface.
type	Tagged or untagged, specifying whether to handle 802.1q frames or untagged frames on the specified port. This parameter is optional and defaults to type "untagged" if not specified.
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.
no local-proxy-arp	Disables Local Proxy ARP on the specified interface.
eth2	Specifies Ethernet-II encapsulation.
snap	SNAP encapsulation.
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.
local-host-dbcast enable	Accepts and processes packets destined for the directed broadcast address of the interface.
local-host-dbcast disable	Drops packets destined for the directed broadcast address of the interface.

Defaults

parameter	default
ip_address	0.0.0.0
subnet_mask	IP address class
admin [enable | disable]	**enable**
vid	none (unbound)
type	**untagged**
forward | no forward	**forward**
local-proxy-arp | no local-proxy-arp	**no local-proxy-arp**
eth2 | snap	**eth2**
primary | no primary	First interface bound to a VLAN.
local-host-dbcast [enable | disable]	**disable**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove an IP interface.
- IP multinetting is supported. As a result, it is possible to configure up to eight IP interfaces per VLAN. Each interface is configured with a different subnet, thus allowing traffic from each configured subnet to coexist on the same VLAN.
- 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. 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 to use Local Proxy ARP. The two features are independent of each other.

- 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, so it will always remain operationally active. The Loopback0 address can be configured in the same subnet as an existing IP interface.
- For setting the rtr-port IP interface, the IP interface must be associated with the rtr-port, rtr-vlan (an unused VLAN) and the type (tagged for handling 802.1q frames on the port or untagged to handle untagged frames).

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 IP1 rtr-port 1/2 rtr-vlan 20 type untagged
-> ip interface IP2 rtr-port 3 rtr-vlan 40 type tagged
```

Release History

Release 6.1; command introduced.
Release 6.4.5; **rtr-port** and **rtr-vlan** parameters added.

Related Commands

show ip interface	Displays the status and configuration of IP interfaces.

MIB Objects

```
alaIpInterfaceTable
   alaIpInterfaceName
   alaIpInterfaceAddress
   alaIpInterfaceMask
   alaIpInterfaceAdminState
   alaIpInterfaceDeviceType
   alaIpInterfaceVlanID
   alaIpInterfaceRtrPort
   alaIpInterfaceRtrPortType
   alaIpInterfaceIpForward
   alaIpInterfaceEncap
   alaIpInterfaceLocalProxyArp
   alaIpInterfacePrimCfg
   alaIpInterfaceOperState
   alaIpInterfaceOperReason
   alaIpInterfaceRouterMac
   alaIpInterfaceBcastAddr
   alaIpInterfacePrimAct
   alaIpInterfaceLocalHostDirectedBroadcast
```

ip managed-interface

Specifies the source IP address for the outgoing packets sent by the applications.

ip managed-interface {*Loopback0* | *interface-name***} application [ldap-server] [tacacs] [radius] [snmp] [sflow] [ntp] [syslog] [dns] [telnet] [ftp] [ssh] [tftp] [all]**

no ip managed-interface {*Loopback0* | *interface-name***} application [ldap-server] [tacacs] [radius] [snmp] [sflow] [ntp] [syslog] [dns] [telnet] [ftp] [ssh] [tftp] [all]**

Syntax Definitions

Loopback0	Specifies the Loopback0 IP address, if configured.
Interface-name	Specifies the name of the interface.
ldap-server	Configures the source IP address to be used by the LDAP Server.
tacacs	Configures the source IP address to be used by TACACS.
radius	Configures the source IP address to be used by RADIUS.
snmp	Configures the source IP address to be used by SNMP.
sflow	Configures the source IP address to be used by sFlow.
ntp	Configures the source IP address to be used by NTP.
syslog	Configures the source IP address to be used by Syslog.
dns	Configures the source IP address to be used by DNS.
telnet	Configures the source IP address to be used by TELNET.
ftp	Configures the source IP address to be used by FTP.
ssh	Configures the source IP address to be used by SSH.
tftp	Configures the source IP address to be used by TFTP.
all	Configures the source IP address to be used by all the application protocols.

Defaults

Application	Default behavior (selecting the source IP address)
LDAP-SERVER	Loopback0, if configured or the outgoing interface
TACACS	Outgoing interface
RADIUS	Loopback0, if configured or the outgoing interface
SNMP	Loopback0, if configured or the outgoing interface
sFlow	Loopback0, if configured or the outgoing interface
NTP	Loopback0, if configured or the outgoing interface
Syslog	Outgoing interface
DNS	Outgoing interface
Telnet	Outgoing interface
FTP	Outgoing interface
SSH	Outgoing interface
TFTP	Outgoing interface

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use this command to configure the source IP address to be used by the application to send the outgoing packets.
- Use the **no** form of this command to revert to the default behavior of choosing the source IP address.
- Use **all** in this command to configure a common source IP address to those applications that use the default source IP address.
- This command supports only the default VRF.

Examples

```
-> ip managed-interface loopback0 application ntp
-> no ip managed-interface loopback0 application ntp
```

Release History

Release 6.4.3; command introduced.

Related Commands

show ip managed-interface	Displays the application name and the corresponding interface name.
show ip interface	Displays the configuration and status of IP interfaces.
ip interface	Configures an IP interface to enable IP routing on a VLAN.

MIB Objects

```
alaIpManagedIntfTable
   AlaIpManagedIntfAppIndex
   alaIpManagedIntfEntry
   alaIpManagedIntfName
   alaIpManagedRowStatus
```

ip interface dhcp-client

Configures a DHCP client IP interface that is to be assigned an IP address from a DHCP server.

ip interface dhcp-client [vlan *vid***] [release | renew] [option-60** *opt60_string***] [admin {enable | disable}]**

no ip interface dhcp-client

Syntax Definitions

dhcp-client	Reserved IP interface name indicating this interface use DHCP to obtain an IP address from a DHCP server.
vid	An existing VLAN ID number (1–4094).
release	Releases the DHCP server assigned IP address.
renew	Renews the DHCP server assigned IP address.
opt60_string	The option-60 field value to be included in DHCP discover/request packets.
enable	Enables the administrative status for the IP interface.
disable	Disables the administrative status for the IP interface.

Defaults

parameter	default
opt60_string	OmniSwitch-xxxx (xxxx = Platform, for example, 6850E)
enable | disable	enable

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove the dhcp-client IP interface.
- Only one DHCP client IP interface can be assigned per switch but it can belong to any VLAN and any VRF instance.
- If the system name has not been configured, it will be updated using the option-12 field. If the option-12 string is greater than 19 characters the remaining characters will be truncated.
- The minimum lease time accepted on the dhcp-client interface is 5 minutes.

Examples

```
-> ip interface dhcp-client vlan 100
```

```
-> ip interface dhcp-client admin enable
-> ip interface dhcp-client release
-> ip interface dhcp-client renew
-> ip interface dhcp-client option-60 OmniSwitch
-> no ip interface dhcp-client
```

Release History

Release 6.4.3; command introduced.

Related Commands

show ip interface	Displays the status and configuration of IP interfaces.

MIB Objects

```
alaIpInterfaceTable
   alaIpInterfaceDhcpStatus
   alaIpInterfaceDhcpIpRelease
   alaIpInterfaceDhcpIpRenew
   alaIpInterfaceDhcpOption60String
```

ip interface tunnel

Configures the end points for the GRE and IPIP tunnels.

ip interface *name* **tunnel [source** *ip_address***] [destination** *ip_address***] [protocol {ipip | gre}]**

Syntax Definitions

name	Text string up to 32 characters. Use quotes around string if description contains multiple words with spaces between them (for example “Alcatel-Lucent Marketing”). This value is case sensitive.
source *ip_address*	Source IP address of the tunnel.
destination *ip_address*	Destination IP address of the tunnel.
ipip	Specifies the tunneling protocol as IPIP.
gre	Specifies the tunneling protocol as GRE.

Defaults

parameter	default
ipip | gre	**ipip**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- You can configure an interface as either a vlan or tunnel interface.
- The maximum number of GRE tunnel interfaces that can be configured on a switch is 8.
- The maximum number of IPIP tunnel interfaces that can be configured on a switch is 127 (16 on an OmniSwitch 6400).

Examples

```
-> ip interface “tnl-1” tunnel source 23.23.23.1 destination 155.2.2.2 protocol gre
-> ip interface “tnl-1” tunnel source 23.23.23.1 destination 155.2.2.2 protocol
ipip
```

Release History

Release 6.1; command introduced.
Release 6.3.1; **tunnel** parameter added.

Related Commands

show ip interface	Displays the status and configuration of IP interfaces.

MIB Objects

```
alaIpInterfaceTable
   alaIpInterfaceName
   alaIpInterfaceTunnelSrc
   alaIpInterfaceTunnelDst
   alaIpInterfaceDeviceType
```

ip router primary-address

Configures the router primary IP address. By default, the router primary address is derived from the first IP interface that becomes operational on the router.

ip router primary-address *ip_address*

Syntax Definitions

ip_address	32-bit IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The router primary address be a valid IP unicast host address.
- The router primary IP address is used by BGP to derive its unique BGP Identifier, if the router router-id is not a valid IP unicast address.
- It is recommended that the primary address be explicitly configured on dual CMM chassis or stacked routers.

Examples

```
-> ip router primary-address 172.22.2.115
```

Release History

Release 6.1; command 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 explicitly configured, the router ID defaults to the address of the first IP interface that becomes operational.

ip router router-id *ip_address*

Syntax Definitions

ip_address	32-bit IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The router ID can be any 32-bit number.
- If the router ID is not a valid IP unicast host address, the BGP identifier is derived from the router primary address.
- It is recommended that the router ID be explicitly configured on dual CMM chassis or stacked routers.
- The router ID is used by OSPF and BGP to uniquely identify the router in the network.

Examples

```
-> ip router router-id 172.22.2.115
```

Release History

Release 6.1; command 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 or recursive 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 | follows}** *ip_address* **[metric** *metric***] [tag** *tag-num***] [name** *tag-name***]**

no ip static-route *ip_address* **[mask** *mask***] {gateway | follows}** *ip_address* **[metric** *metric***][tag** *tag-num***] [name** *tag-name***]**

Syntax Definitions

ip_address	Destination IP address of the static route.
mask	Subnet mask corresponding to the destination IP address.
gateway *ip_address*	IP address of the next hop used to reach the destination IP address.
follows *ip_address*	The recursive static route follows this IP address. The recursive route will use the same gateway/nexthop that is used to reach this host address.
metric	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 1–65535.
tag-num	The tag number.
tag-name	The name of the tag.

Defaults

parameter	default
metric	1

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Static routes do not age out of the routing tables; however, they can be deleted. Use the **no** form of this command to delete a static route.
- Use the **follows** parameter to create a recursive static route. The route to this IP address can be dynamically learned.
- 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.

- 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.
- A name can be assigned to the static route to identify it quickly at a later time.
- If you want to classify certain static routes and filter them, then a tag value can be allocated to those routes and route-map match statement to filter those routes. If the tag or name value is not specified, then the previously configured values for the tag and name will remain unchanged.
- To remove the previously configured tag value, configure the same route with tag value as 0. This will be equivalent to untagging the route.
- To remove the previously configured name value, configure the static route with the name field as "". Unconfiguring the static route will delete both the tag and name values.
- To view the tag and name of the configured static routes, use the **show ip router database** command.

Examples

```
-> ip static-route 171.11.1.1 gateway 171.11.2.1
-> ip static-route 10.0.1.1/32 gateway 30.0.1.1 tag 123
-> ip static-route 10.0.2.1/32 gateway 30.0.2.1 tag 345 name RouteToServer
-> ip static-route 10.0.3.0/24 gateway 30.0.3.1 name HRDept
```

Release History

Release 6.1; command introduced.
Release 6.4.3; **follows** parameter was added.
Release 6.4.5; **tag-num** and **tag-name** parameters added.

Related Commands

show ip route	Displays the IP Forwarding table.
show ip router database	Displays the IP router database contents.

MIB Objects

```
alaIprmStaticRoute
   alaIprmStaticRouteDest
   alaIprmStaticRouteMask
   alaIprmStaticRouteNextHop
   alaIprmStaticRouteMetric
   alaIprmStaticRouteTag
   alaIprmStaticRouteName
```

ip route-pref

Configures the route preference of a router.

[vrf *name***] ip route-pref {static | rip | ospf | isisl2 | isisl1 | ibgp | ebgp | import} value**

Syntax Definitions

name	The alphanumeric name (1–20 characters) assigned to the VRF instance.
static	Configures the route preference of static routes.
ospf	Configures the route preference of OSPF routes.
isisl2	Configures the route preference of ISIS L2 routes.
isisl1	Configures the route preference of ISIS L1 routes.
rip	Configures the route preference of RIP routes.
ebgp	Configures the route preference of external BGP routes.
ibgp	Configures the route preference of internal BGP routes.
import	Configures the route preference for the routes that are imported.
value	Route preference value.

Defaults

parameter	default
static *value*	2
ospf *value*	110
isisl2 *value*	118
isisl1 *value*	115
rip *value*	120
ebgp *value*	190
ibgp *value*	200
import *value*	210

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Route preference of local routes cannot be changed.

Examples

```
-> ip route-pref ebgp 20
```

```
-> ip route-pref rip 60
-> ip route-pref import 200
```

Release History

Release 6.1.1; command introduced.
Release 6.1.3; **ebgp** and **ibgp** parameters added.
Release 6.4.5; **vrf** and **import** parameters added.

Related Commands

show ip route-pref	Displays the configured route-preference of a router.
ip import vrf	Configures a route map to import routes from GRT to the destination VRF.
show ip import	Displays the import route configuration details.

MIB Objects

```
alaIprmRtPrefTable
   alaIprmRtPrefLocal
   alaIprmRtPrefStatic
   alaIprmRtPrefOspf
   alaIprmRtPrefRip
   alaIprmRtPrefEbgp
   alaIprmRtPrefIbgp
   alaIprmRtPrefImport
```

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 6400, 6850E, 6855, 9000E

Usage Guidelines

This value represents the default value inserted into 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 6.1; command introduced.

Related Commands

show ip config	Displays IP configuration parameters.

MIB Objects

```
IpDefaultTTL
```

ping

Tests 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 IP address or hostname. The switch pings 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 in the command.

ping {*ip_address* | *hostname***} [source-interface** *ip_interface***] [[sweep-range** *start_size* | *end_size* | *diff_size***] | [count** *count***] [size** *packet_size***]] [interval** *seconds***] [timeout** *seconds***] [tos** *tos_val***] [dont-fragment] [data-pattern** *hex_string***]**

Syntax Definitions

ip_address	IP address of the system to ping.
hostname	DNS name of the system to ping.
ip_interface	IP interface name (maximum 32 characters) of the source interface.
start_size	Size of the first echo packet that is sent. The valid range is from 4 to 60000.
end_size	Maximum size of the echo packet that is sent. The range is greater than the start size and less than 60000.
diff_size	The increment factor of size for the next echo packet. The diff size must be greater than 0 and less than end size.
count	Number of packets to be transmitted. The range is between 1 and 4294967295 (0xFFFFFFFF).
packet_size	Size of the data portion of the packet sent for this ping, in bytes. The valid range is 1–60000.
interval *seconds*	The time interval in seconds with which the ICMP packets are sent out. The range is between 1 and the maximum integer value (4294967295).
timeout *seconds*	Number of seconds the program has to wait for a response before timing out.The range is between 1 and the maximum integer value (4294967295).
tos_val	Specifies the type of service for the probe. The valid range is between 0 and 255.
dont-fragment	Specifies whether the Don't Fragment (DF) bit is to be set on the ping packet. The value 1 sets the Don't Fragment bit in the packet and 0 unsets the same.
hex_string	Specifies the data pattern in a plain string of two characters. Different data patterns are used to troubleshoot framing errors and clocking problems on serial lines. For example, **ab, xy, 12** and so on.

Defaults

parameter	default
ip_interface	Outgoing IP interface as per route lookup
start_size	4
end_size	> 4
diff_size	5
count	6
packet_size	64 bytes (default 6)
interval *seconds*	1
timeout *seconds*	1
tos_val	0
dont-fragment	0
hex_string	Repeating sequence of ASCII characters from 0x4 to 0xff

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 specifying the source-interface, specify either the name of any operational interface or the Loopback0 interface. The IP address of the source interface must be reachable from the destination.
- When you specify the *sweep-range* in the **ping** command, you cannot configure the *count* and *size* parameters.
- The Don't Fragment (DF) bit must not be larger than the MTU of the IP interface.
- The command does not support Loose, Strict, and route record options.
- The command is VRF aware and is available only from CLI. It does not support IPv6.
- Ping is supported only in CLI. This command is not supported in WebView.
- The command is VRF aware and is available only from CLI. It does not support IPv6.

Examples

```
-> ping 20.1.1.2 source-interface Loopback0 interval 2 data-pattern ab sweep-range
500 1000 100 tos 7 dont-fragment

PING 20.1.1.2: 500 data bytes
508 bytes from 20.1.1.2: icmp_seq=0. time=69. ms
608 bytes from 20.1.1.2: icmp_seq=1. time=70. ms
708 bytes from 20.1.1.2: icmp_seq=2. time=69. ms
```

```
808 bytes from 20.1.1.2: icmp_seq=3. time=69. ms
908 bytes from 20.1.1.2: icmp_seq=4. time=69. ms
```

Release History

Release 6.4.1; command introduced.

Release 6.4.3; **source-interface**, **sweep-range**, **dont-fragment**, and **data-pattern** parameters were added.

Related Commands

traceroute	Finds the path taken by an IP packet from the local switch to a specified destination.

traceroute

Finds the path taken by an IP packet from the local switch to a specified destination. This command is used to discover the paths that packets take to a remote destination, as well as where routing breaks down.

traceroute {*ip_address* **|** *hostname***} [source-interface** *ip_interface***] [min-hop** *min_hop_count***] [max-hop** *max_hop_count***] [probes** *probe_count***] [time-out** *seconds***] [port-number** *port_number***]**

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.
ip_interface	IP interface name (maximum 32 characters) of the source interface.
min_hop_count	Minimum hop count for the first traceroute packet. The value must be greater than 0 and less than the max hop count.
max_hop_count	Maximum hop count for the destination address. The range is between 1 and the maximum integer value (4294967295).
probe_count	The number of probes to be sent at each TTL level hop-count. The range is between 1 and the maximum integer value (4294967295).
seconds	The period in seconds to wait for the response of each probe packet.
port_number	The destination port number used for probing packets. The value must be greater than 1024.This value is incremented by one in each probe. The valid range is between 1024 and 65535.

Defaults

parameter	default
min_hop_count	1
max_hop_count	30
probe_count	3
seconds	5 *seconds*
port_number	33334

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- When using this command, enter the name of the destination as part of the command line (either the IP address or host name).
- When specifying the source-interface, specify either the name of any operational interface or Loopback0 interface. The IP address of the source interface must be reachable from the destination.
- 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.
- Tracetoure is supported only in CLI. This command is not supported in WebView.

- The command is VRF aware and is available only from CLI. It does not support IPv6.

Examples

```
-> traceroute 192.168.1.1 max-hop 5 min-hop 1 port-number 1025 source-interface
Loopback0 timeout 5

traceroute to 192.168.1.1, 5 hops max, 40 byte packets
 1  10.135.33.1  2 ms  2 ms  11 ms
 2  10.250.2.1  6 ms  6 ms  4 ms
 3  192.168.2.2  4 ms  4 ms  3 ms
 4  192.168.1.1  3 ms  3 ms  3 ms
```

Release History

Release 6.4.1; command introduced.
Release 6.4.3; **source-interface**, **min-hop**, **probes**, **time-out**, and **port-number** parameters were added.

Related Commands

show ip route	Displays the IP Forwarding table.

ip dual-hash mode

Enable or disable the dual-hashing mode.

ip dual-hash mode {enable | disable}

Syntax Definitions

enable	Enables the dual-hash mode.
disable	Disables the dual-hash mode.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- The CLI enables dual-hash for both IPv4 as well as IPv6 multicast and unicast streams.
- Enabling dual-hash mode reduces the chances of collision. However, it does not eliminate collision.
- Dual-hash configuration is independent of VRF ID. If the value is modified from one VRF instance, its updated value is reflected in all the instances.
- Dual-hash configuration is effective only after switch reboot.

Examples

```
-> ip dual-hash mode enable
-> ip dual-hash mode disable
```

Release History

Release 6.4.5; command introduced

Related Commands

show ip config	Displays the IP configuration.

MIB Objects

```
alaIpDualHashMode
```

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 6400, 6850E, 6855, 9000E

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. Directed broadcasts must not be enabled.

Examples

```
-> ip directed-broadcast off
```

Release History

Release 6.1; command introduced.

Related Commands

show ip interface	Displays the status and configuration of IP interfaces.
show ip managed-interface	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 (SSH, telnet, FTP, and so on). Selectively enabling or disabling these types of ports provides an additional method for protecting against denial of service (DoS) attacks.

ip service {all | *service_name* **| port** *service_port***}**

no ip service {all | *service_name* **| port** *service_port***}**

Syntax Definitions

all	Configures access to all TCP/UDP ports.
service_name	The name of the TCP/UDP service to enable or disable. (Refer to the table in the following "Usage Guidelines" section for a list of supported service names.)
service_port	A TCP/UDP service port number. Configures access by port number rather than by service name. (Refer to the table in the following "Usage Guidelines" section for a list of supported service names.)

Defaults

All TCP/UDP ports are open by default.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- 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, and so on.
- Use the **all** option with this command to configure access to all well-known TCP/UDP service ports.
- To designate which port to enable or disable, specify either the name of a service or the well-known port number associated with that service. Specifying a name and a port number in a single command line is not supported.
- When using service names, it is possible to specify more than one service in a single command line by entering each service name separated by a space. See the following examples.
- When specifying a service port number, the **port** keyword is required and that only one port number is allowed in a single command.
- The following table lists the **ip service** command options for specifying TCP/UDP services and also includes the well-known port number associated with each service:

service name	port
ftp	21
ssh	22

service name	port
telnet	23
http	80
secure-http	443
avlan-http	260
avlan-secure-http	261
avlan-telnet	259
udp-relay	67
network-time	123
snmp	161
avlan-http-proxy	262

Examples

```
-> ip service all
-> ip service ftp telnet snmp
-> ip service port 261
-> no ip service ftp snmp
-> no ip service all
```

Release History

Release 6.1; command 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
```

ip redist

Controls the conditions for redistributing IPv4 routes between different protocols.

[vrf *name***] ip redist {local | static | rip | ospf | isis | bgp | import} into {rip | ospf | isis | bgp} route-map** *route-map-name* **[status {enable | disable}]**

no ip redist {local | static | rip | ospf | isis | bgp | import} into {rip | ospf | isis | bgp} [route-map *route-map-name***]**

Syntax Definitions

local	Redistributes local routes.
static	Redistributes static routes.
import	Redistibute imported routes into other routing protocols.
rip	Specifies RIP as the source or destination (into) protocol.
ospf	Specifies OSPF as the source or destination (into) protocol.
isis	Specifies IS-IS as the source or destination (into) protocol.
bgp	Specifies BGP as the source or destination (into) protocol.
route-map-name	Name of an existing route map that will control the redistribution of routes between the source and destination protocol.
enable	Enables the administrative status of the redistribution configuration.
disable	Disables the administrative status of the redistribution configuration.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a route map redistribution configuration. If a route map name is not specified, all route maps associated with the redistribution configuration are removed.
- The source and destination protocols must be loaded and enabled before redistribution occurs.
- If the metric calculated for the redistributed route, is greater than 15 (RIP_UNREACHABLE) or greater than the metric of an existing pure RIP route, the new route is not redistributed.
- Use the **ip route-map** commands described in this chapter to create a route map. Refer to the "Configuring IP" chapter in the *OmniSwitch AOS Release 6 Network Configuration Guide* for more information about how to create a route map.

- By default, import routes are least preferred.

Examples

```
-> ip redist rip into bgp route-map rip-to-bgp1
-> ip redist rip into bgp route-map rip-to-bgp2
-> no ip redist rip into bgp route-map rip-to-bgp2
-> ip redist ospf into rip route-map ospf-to-rip
-> ip redist ospf into rip route-map ospf-to-rip disable
-> ip redist import into ospf route-map R1 status enable
```

Release History

Release 6.1.3; command introduced.
Release 6.2.1; **isis** parameter support added.
Release 6.4.5; **vrf** and **import** parameters added.

Related Commands

show ip redist	Displays the route map redistribution configuration.
ip route-map action	Creates a route map and sets the status of the route map to permit or deny.
ip import vrf	Configures a route map to import routes from GRT to the destination VRF.
show ip import	Displays the import route configuration details.

MIB Objects

```
alaRouteMapRedistProtoTable
   alaRouteMapRedistSrcProtoId
   alaRouteMapRedistDestProtoId
   alaRouteMapRedistRouteMapIndex
   alaRouteMapRedistStatus
   alaRouteMapRedistAddressType
   alaRouteMapRedistRowStatus
```

ip access-list

Creates an access list for adding multiple IPv4 addresses to route maps.

ip access-list *access-list-name*

no ip access-list *access-list-name*

Syntax Definitions

access-list-name	Name of the access list (up to 20 characters).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the **no** form of this command to delete the access list.

Examples

```
-> ip access-list access1
-> no ip access-list access1
```

Release History

Release 6.1.3; command introduced.

Related Commands

ip access-list address	Adds IPv4 addresses to the specified IPv4 access list.
show ip access-list	Displays the details of the access list.

MIB Objects

```
alaRouteMapAccessListNameTable
   alaRouteMapAccessListName
   alaRouteMapAccessListNameIndex
   alaRouteMapAccessListNameAddressType
   alaRouteMapAccessListNameRowStatus
```

ip access-list address

Adds multiple IPv4 addresses to the specified IPv4 access list.

ip access-list *access-list-name* **address** *address/prefixLen* **[action {permit | deny}] [redist-control {all-subnets | no-subnets | aggregate}]**

no ip access-list *access-list-name* **address** *address/prefixLen*

Syntax Definitions

access-list-name	Name of the access list.
address/prefixLen	IP address/prefix length to be added to the access list.
permit	Permits the IP address.
deny	Denies the IP address.
all-subnets	Permits or denies all the subnet routes that match the network portion of the IP address as specified by the mask length.
no-subnets	Permits or denies only those routes that exactly match the IP address and the mask length.
aggregate	Permits an aggregate route if there are one or more routes that match or are subnets of this address.

Defaults

parameter	default
permit | **deny**	**permit**
all-subnets | **no-subnets** | **aggregate**	**all-subnets**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete the address from the access list.
- The *access-list-name* must exist before you add multiple addresses to it.
- The **action** parameters (**permit** and **deny**) determine if a route that matches the **redist-control** configuration for the IP address is allowed or denied redistribution.
- The **redist-control** parameters (**all-subnets, no-subnets**, and **aggregate**) defines the criteria used to determine if a route matches an address in the access list.
- Configuring the combination of **redist-control aggregate** with **action deny** is not allowed.

- Use this command multiple times with the same access list name to add multiple addresses to the existing access list.

Examples

```
-> ip access-list access1 address 10.0.0.0/8 action permit
-> ip access-list access1 address 11.1.0.0/16 action permit
-> ip access-list access1 address 10.1.1.0/24 redist-control aggregate
-> no ip access-list access1 address 10.0.0.0/8
```

Release History

Release 6.1.3; command introduced.

Related Commands

ip access-list	Creates an access list for adding multiple IPv4 addresses to route maps.
show ip access-list	Displays the contents of an IPv4 access list.

MIB Objects

```
alaRouteMapAccessListTable
   alaRouteMapAccessListIndex
   alaRouteMapAccessListAddress
   alaRouteMapAccessListAddressType
   alaRouteMapAccessListPrefixLength
   alaRouteMapAccessListAction
   alaRouteMapAccessListRedistControl
   alaRouteMapAccessListRowStatus
```

ip route-map action

Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.

ip route-map *route-map-name* **[sequence-number** *number***] action {permit | deny}**

no ip route-map *route-map-name* **[sequence-number** *number***]**

Syntax Definitions

route-map-name	The name of the route map (up to 20 characters).
number	A number that links together the route maps. The range is 1–100.
permit	Selects a route.
deny	Filters a route.

Defaults

parameter	default
number	50
permit | deny	**permit**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete the entire route map by specifying only the *route-map-name*.
- Use the **no** form of this command to delete a specific sequence in the route map by specifying the **sequence-number**.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- Use this command to change the status of an existing route map to permit or deny.

Examples

```
-> ip route-map route1 sequence-number 10 action permit
-> no ip route-map route1
```

Release History

Release 6.1.3; command introduced.

Related Commands

show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaRouteMapSequenceTable
   alaRouteMapSequenceIndex
   alaRouteMapSequenceNumber
   alaRouteMapSequenceAction
   alaRouteMapSequenceRowStatus
```

ip route-map match ip address

Matches the route with the specified IPv4 address or an address defined in the specified IPv4 access list.

ip route-map *route-map-name* **[sequence-number** *number***] match ip-address {***access-list-name* **|** *ip_address/prefixLen* **[redist-control {all-subnets | no-subnets | aggregate}] [permit | deny]**

no ip route-map *route-map-name* **[sequence-number** *number***] match ip-address {***access-list-name* **|** *ip_address/prefixLen* **[redist-control {all-subnets | no-subnets | aggregate}] [permit | deny]**

Syntax Definitions

route-map-name	The name of the route map (up to 20 characters).
number	A number that links together the route maps. The range is 1–100.
access-list-name	The name of an IPv4 access list that contains IPv4 addresses to match.
ip_address/prefixLen	The destination IP address along with the prefix length of the routes to be selected.
all-subnets	Selects all the subnet routes that match the network portion of the IP address as specified by the mask length.
no-subnets	Selects only those routes that exactly match the IP address and the mask length.
aggregate	Creates an aggregate route if there are one or more routes that match the IP address.
permit	Permits a route based on the IP address or prefix constrained by redist-control.
deny	Denies a route based on the IP address or prefix constrained by redist-control.

Defaults

parameter	default
number	50
permit | deny	**permit**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete the **match ip-address redist-control** parameter in the route map.
- Specify either the name of an existing IPv4 access list or an IPv4 address/prefix length with this command.

- Configuring the combination of **redist-control aggregate** with **deny** is not allowed.
- Multiple addresses in the same route map sequence are matched using the longest prefix match.
- If the best matching address is type **deny**, then the route is not selected. If the best matching address is type permit and the route map action is deny, the route is not selected.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route-map-name*, **sequence-number,** and *access-list-name* (if used) must exist before you configure this **match** criteria.

Examples

```
-> ip route-map 3 match ip-address 10.1.1.1/8 redist-control no-subnets deny
-> no ip route-map 3 match ip-address 10.1.1.1 redist-control no-subnets deny
-> ip route-map route1 sequence-number 10 match ip-address list1
-> no ip route-map route1 sequence-number 10 match ip-address list1
```

Release History

Release 6.1.3; command introduced.

Related Commands

ip route-map action	Creates a route map and sets the status of the route map to permit or deny.
ip access-list	Creates an access list for adding multiple IPv4 addresses to route maps.
ip access-list address	Adds IPv4 addresses to the specified IPv4 access list.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

ip route-map match ipv6 address

Matches the route with the specified IPv6 address or an address defined in the specified IPv6 access list.

ip route-map *route-map-name* **[sequence-number** *number***] match ipv6-address** {access-list-name | *ipv6_address/prefixLen* **[redist-control {all-subnets | no-subnets | aggregate}] [permit | deny]**

no ip route-map *route-map-name* **[sequence-number** *number***] match ipv6-address** *ipv6_address/prefix-Len* **[redist-control {all-subnets | no-subnets | aggregate}] [permit | deny]**

Syntax Definitions

route-map-name	The name of the route map (up to 20 characters).
number	A number that links together the route maps. The range is 1–100.
access-list-name	The name of an IPv4 access list that contains IPv4 addresses to match.
ipv6_address/prefixLen	The destination IPv6 address along with the prefix length of the routes to be selected.
all-subnets	Selects all the subnet routes that match the network portion of the IP address as specified by the mask length.
no-subnets	Selects only those routes that exactly match the IP address and the mask length.
aggregate	Creates an aggregate route if there are one or more routes that match the IPv6 address.
permit	Permits a route based on the IPv6 address or prefix constrained by redist-control.
deny	Denies a route based on the IPv6 address or prefix constrained by redist-control.

Defaults

parameter	default
number	50
permit | deny	**permit**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete the **match ipv6-address redist-control** parameter in the route map.
- Specify either the name of an existing IPv6 access list or an IPv6 address/prefix length with this command.

- Configuring the combination of **redist-control aggregate** with **deny** is not allowed.
- Multiple addresses in the same route map sequence are matched using the longest prefix match.
- If the best matching address is type **deny**, then the route is not selected. If the best matching address is type permit and the route map action is **deny**, the route is not selected.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route-map-name* and **sequence-number** must exist before you configure this **match** criteria.

Examples

```
-> ip route-map 3 match ipv6-address 2001::1/64 redist-control no-subnets deny
-> no ip route-map 3 match ipv6-address 2001::1/64 redist-control no-subnets deny
-> ip route-map route1 sequence-number 10 match ipv6-address list1
-> no ip route-map route1 sequence-number 10 match ipv6-address list1
```

Release History

Release 6.1.3; command introduced.

Related Commands

ip route-map action	Creates a route map and sets the status of the route map to permit or deny.
ipv6 access-list	Creates an access list for adding multiple IPv6 addresses to route maps.
ipv6 access-list address	Adds IPv6 addresses to the specified IPv6 access list.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

ip route-map match ip-nexthop

Matches any routes that have a next-hop router address permitted by the specified access list name or the IP address specified in the route map.

ip route-map *route-map-name* **[sequence-number** *number***] match ip-nexthop {***access-list-nam***e** | *ip_address/prefixLen* **[permit | deny]}**

no ip route-map *route-map-name* **[sequence-number** *number***] match ip-nexthop {***access-list-nam***e** | *ip_address/prefixLen* **[permit | deny]}**

Syntax Definitions

route-map-name	The name of the route map (up to 20 characters).
number	A number that links together the route maps. The range is 1–100.
access-list-name	The access list that matches the route nexthop IP address.
ip_address/prefixLen	The IP address along with the prefix length that matches any nexthop IP address within the specified subnet.
permit	Permits a route based on the IP nexthop.
deny	Denies a route based on the IP nexthop.

Defaults

parameter	default
number	50
permit | deny	**permit**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete the **match ip-nexthop** parameter in the route map.
- If the best matching nexthop is type deny, then the route is not selected. If the best matching nexthop is type permit and the route map action is deny, the route is not selected.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route-map-name*, **sequence-number,** and *access-list-name* must exist before you configure this **match** criteria.

Examples

```
-> ip route-map route1 sequence-number 10 match ip-nexthop list1
-> no ip route-map route1 sequence-number 10 match ip-nexthop list1
-> ip route-map route1 sequence-number 10 match ip-nexthop 10.0.0.0/8
-> no ip route-map route1 sequence-number 10 match ip-nexthop 10.0.0.0/8
```

Release History

Release 6.1.3; command introduced.

Related Commands

ip access-list	Creates an access list for adding multiple IPv4 addresses to route maps.
ip route-map action	Creates a route map and sets the status of the route map to permit or deny.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

ip route-map match ipv6-nexthop

Matches any routes that have an IPv6 next-hop router address permitted by the specified access list name or the IPv6 address specified in the route map.

ip route-map *route-map-name* **[sequence-number** *number***] match ipv6-nexthop {***access-list-name* **|** *ipv6_address/prefixLen* **[permit | deny]}**

no ip route-map *route-map-name* **[sequence-number** *number***] match ipv6-nexthop {***access-list-name* **|** *ipv6_address/prefixLen* **[permit | deny]}**

Syntax Definitions

route-map-name	The name of the route map (up to 20 characters).
number	A number that links together the route maps. The range is 1–100.
access-list-name	The access list that matches the route nexthop IPv6 address.
ipv6_address/prefixLen	The IPv6 address along with the prefix length that matches any nexthop IPv6 address within the specified subnet.
permit	Permits a route based on the IPv6 nexthop.
deny	Denies a route based on the IPv6 nexthop.

Defaults

parameter	default
number	50
permit | deny	**permit**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete the **match ipv6-nexthop** parameter in the route map.
- If the best matching nexthop is type deny, then the route is not selected. If the best matching nexthop is type permit but the route map action is deny, the route is not selected.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route-map-name*, **sequence-number,** and *access-list-name* must exist before you configure this **match** criteria.

Examples

```
-> ip route-map route1 sequence-number 10 match ipv6-nexthop list1
-> no ip route-map route1 sequence-number 10 match ipv6-nexthop list1
-> ip route-map route1 sequence-number 10 match ipv6-nexthop 2001::/64
-> no ip route-map route1 sequence-number 10 match ipv6-nexthop 2001::/64
```

Release History

Release 6.1.3; command introduced.

Related Commands

ipv6 access-list	Creates an access list for adding multiple IPv6 addresses to route maps.
ipv6 access-list address	Adds IPv6 addresses to the specified IPv6 access list.
ip route-map action	Creates a route map and sets the status of the route map to permit or deny.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

ip route-map match tag

Matches the tag value specified in the route map with the one that the routing protocol learned the route on.

ip route-map *route-map-name* **[sequence-number** *number***] match tag** *tag-number* **[name** *tag-name***]**

no ip route-map *route-map-name* **[sequence-number** *number***] match tag** *tag-number* **[name** *tag-name***]**

Syntax Definitions

route-map-name	The name of the route map (up to 20 characters).
number	A number that links together the route maps. The range is 1–100.
tag-number	The tag number.
tag-name	The name of the tag.

Defaults

parameter	default
number	50

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete the **match tag** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route-map-name* and **sequence-number** must exist before you configure this **match** criteria.

Examples

```
-> ip route-map route1 sequence-number 10 match tag 4
-> no ip route-map route1 sequence-number 10 match tag 4
```

Release History

Release 6.1.3; command introduced.
Release 6.4.5; **tag-name** parameter added.

Related Commands

ip route-map action	Creates a route map and sets the status of the route map to permit or deny.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

ip route-map match ipv4-interface

Matches the IPv4 interface name specified in the route map with the one that the routing protocol learned the route on.

ip route-map *route-map-name* **[sequence-number** *number***] match ipv4-interface** *interface-name*

no ip route-map *route-map-name* **[sequence-number** *number***] match ipv4-interface** *interface-name*

Syntax Definitions

route-map-name	The name of the route map (up to 20 characters).
number	A number that links together the route maps. The range is 1–100.
interface-name	Specifies the name of the outgoing interface of the route.

Defaults

parameter	default
number	50

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete the **match ipv4-interface** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route-map-name* and **sequence-number** must exist before you configure this **match** criteria.

Examples

```
-> ip route-map route1 sequence-number 10 match ipv4-interface int4
-> no ip route-map route1 sequence-number 10 match ipv4-interface int4
```

Release History

Release 6.1.3; command introduced.

Related Commands

ip route-map action	Creates a route map and sets the status of the route map to permit or deny.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

ip route-map match ipv6-interface

Matches the IPv6 interface name specified in the route map with the one that the routing protocol learned the route on.

ip route-map *route-map-name* **[sequence-number** *number***] match ipv6-interface** *interface-name*

no ip route-map *route-map-name* **[sequence-number** *number***] match ipv6-interface** *interface-name*

Syntax Definitions

route-map-name	The name of the route map (up to 20 characters).
number	A number that links together the route maps. The range is 1–100.
interface-name	Specifies the name of the outgoing interface of the route.

Defaults

parameter	default
number	50

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete the **match ipv6-interface** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route-map-name* and **sequence-number** must exist before you configure this **match** criteria.

Examples

```
-> ip route-map route1 sequence-number 10 match ipv6-interface int6
-> no ip route-map route1 sequence-number 10 match ipv6-interface int6
```

Release History

Release 6.1.3; command introduced.

Related Commands

ip route-map action	Creates a route map and sets the status of the route map to permit or deny.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

ip route-map match metric

Matches the metric value specified in the route map with the actual metric value of the route.

ip route-map *route-map-name* **[sequence-number** *number***] match metric** *metric* **[deviation** *deviation***]**

no ip route-map *route-map-name* **[sequence-number** *number***] match metric** *metric* **[deviation** *deviation***]**

Syntax Definitions

route-map-name	The name of the route map (up to 20 characters).
number	A number that links together the route maps. The range is 1–100.
metric	The metric value that matches a specified metric.
deviation	The deviation value. If deviation is included, the route metric can have any value within the range (metric-deviation to metric+deviation).

Defaults

parameter	default
number	50

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete the **match metric** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route-map-name* and **sequence-number** must exist before you configure this **match** criteria.

Examples

```
-> ip route-map route1 sequence-number 10 match metric 4
-> no ip route-map route1 sequence-number 10 match metric 4
```

Release History

Release 6.1.3; command introduced.

Related Commands

ip route-map action	Creates a route map and sets the status of the route map to permit or deny.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

ip route-map match route-type

Matches the specified route type with actual route type of the route.

ip route-map *route-map-name* **[sequence-number** *number***] match route-type {internal | external [type1 | type2] | level1 | level2}**

no ip route-map *route-map-name* **[sequence-number** *number***] match route-type {internal | external [type1 | type2] | level1 | level2}**

Syntax Definitions

route-map-name	The name of the route map (up to 20 characters).
number	A number that links together the route maps. The range is 1–100.
internal	Matches OSPF/BGP internal routes.
external	Matches OSPF/BGP external routes.
type1	Matches OSPF external Type-1 routes, which gives the full metric calculation for the complete path including internal as well as external cost.
type2	Matches OSPF external Type-2 routes, which gives the external redistribution metric only to the ASBR.
level1	Matches IS-IS Level-1 routes only.
level2	Matches IS-IS Level-2 routes only.

Defaults

parameter	default
number	50

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete the **match route-type** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route-map-name* and **sequence-number** must exist before you configure this **match** criteria.

Examples

```
-> ip route-map 111 sequence-number 50 match route-type internal
-> no ip route-map 111 sequence-number 50 match route-type internal
```

Release History

Release 6.1.3; command introduced.
Release 6.2.1; **level1** and **level2** parameter support added.

Related Commands

ip route-map action	Creates a route map and sets the status of the route map to permit or deny.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

ip route-map match protocol

Matches the protocol specified in the route map with the protocol of the route.

ip route-map *route-map-name* **[sequence-number** *number***] match protocol {local | static | rip | ospf | isis | bgp}**

no ip route-map *route-map-name* **[sequence-number** *number***] match protocol {local | static | rip | ospf | isis | bgp}**

Syntax Definitions

route-map-name	The name of the route map.
number	A number that links together the route maps. The range is 1–100.
local	Matches a local interface route.
static	Matches a static route.
rip	Matches a RIP route.
ospf	Matches an OSPF route.
ISIS	Matches an ISIS route.
bgp	Matches a BGP route.

Defaults

parameter	default
number	50

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete the **match protocol** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route-map-name* and **sequence-number** must exist before you configure this **match** criteria.

Examples

```
-> ip route-map route1 sequence-number 10 match protocol local
-> no ip route-map route1 sequence-number 10 match protocol local
```

Release History

Release 6.1.3; command introduced.

Related Commands

ip route-map action	Creates a route map and sets the status of the route map to permit or deny.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

ip route-map set metric

Configures the metric value of the route being distributed.

ip route-map *route-map-name* **[sequence-number** *number***] set metric** *metric*
[effect {add | subtract | replace | none}]

no ip route-map *route-map-name* **[sequence-number** *number***] set metric** *metric*
[effect {add | subtract | replace | none}]

Syntax Definitions

route-map-name	The name of the route map (up to 20 characters).
number	A number that links together the route maps. The range is 1–100.
metric	Configures the metric value of the route being distributed. A value of 0 is not allowed.
add	Adds the configured metric value to the actual metric value.
subtract	Subtracts the configured metric value from the actual metric value.
replace	Replaces the actual metric value with the configured metric value.
none	Uses the routes the actual metric value. The configured metric value is ignored. Use any value except 0.

Defaults

parameter	default
number	50

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete the **set metric** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route-map-name* and **sequence-number** must exist before you configure this **set** criteria.

Examples

```
-> ip route-map 111 sequence-number 50 set metric 30 effect add
-> no ip route-map 111 sequence-number 50 set metric 30 effect add
```

Release History

Release 6.1.3; command introduced.

Related Commands

ip route-map action	Creates a route map and sets the status of the route map to permit or deny.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

ip route-map set metric-type

Configures the metric type for the redistributed route.

ip route-map *route-map-name* **[sequence-number** *number***] set metric-type {internal | external [type1 | type2]}**

no ip route-map *route-map-name* **[sequence-number** *number***] set metric-type {internal | external [type1 | type2]}**

Syntax Definitions

route-map-name	The name of the route map (up to 20 characters).
number	A number that links together the route maps. The range is 1–100.
internal	Sets the metric type to internal for routes redistributed into BGP.
external	Sets the metric type to external for routes redistributed into BGP.
type1	Sets the metric type to external type1 for routes redistributed into OSPF, which gives the full metric calculation for the complete path including internal as well as external cost.
type2	Sets the metric type to external type2 for routes redistributed into OSPF, which gives the external redistribution metric only to the ASBR.

Defaults

parameter	default
number	50

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete the **set metric-type** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route-map-name* and **sequence-number** must exist before you configure this **set** criteria.

Examples

```
-> ip route-map 111 sequence-number 50 set metric-type internal
-> no ip route-map 111 sequence-number 50 set metric-type internal
```

Release History

Release 6.1.3; command introduced.

Related Commands

ip route-map action	Creates a route map and sets the status of the route map to permit or deny.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

ip route-map set tag

Configures the tag value of the selected routes.

ip route-map *route-map-name* **[sequence-number** *number***] set tag** *tag-number*

no ip route-map *route-map-name* **[sequence-number** *number***] set tag** *tag-number*

Syntax Definitions

route-map-name	The name of the route map (up to 20 characters).
number	A number that links together the route maps. The range is 1–100.
tag-number	Configures the tag number.

Defaults

parameter	default
number	50

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete the **set tag** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route-map-name* and **sequence-number** exist before you configure this **set** criteria.

Examples

```
-> ip route-map 111 sequence-number 50 set tag 23
-> no ip route-map 111 sequence-number 50 set tag 23
```

Release History

Release 6.1.3; command introduced.

Related Commands

ip route-map action	Creates a route map and sets the status of the route map to permit or deny.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

ip route-map set community

Configures the community name of the route being redistributed into BGP.

ip route-map *route-map-name* **[sequence-number** *number***] set community** *community-string*

no ip route-map *route-map-name* **[sequence-number** *number***] set community** *community-string*

Syntax Definitions

route-map-name	The name of the route map (up to 20 characters).
number	A number that links together the route maps. The range is 1–100.
community-string	Defines a community for an aggregate route. Community names range from 0 to 70 characters.

Defaults

parameter	default
number	50

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete the **set community** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route-map-name* and **sequence-number** exist before you configure this **set** criteria.

Examples

```
-> ip route-map 111 sequence-number 50 set community 29
-> no ip route-map 111 sequence-number 50 set community 29
```

Release History

Release 6.1.3; command introduced.

Related Commands

ip route-map action	Creates a route map and sets the status of the route map to permit or deny.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

ip route-map set local-preference

Configures the local preference value for a route being distributed into BGP.

ip route-map *route-map-name* **[sequence-number** *number***] set local-preference** *value*

no ip route-map *route-map-name* **[sequence-number** *number***] set local-preference** *value*

Syntax Definitions

route-map-name	The name of the route map (up to 20 characters).
number	A number that links together the route maps. The range is 1–100.
value	Configures the local-preference value for routes being redistributed in to BGP. The value is between 0 and 4294967295.

Defaults

parameter	default
number	50

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete the **set local-preference** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route-map-name* and **sequence-number** exist before you configure this **set** criteria.
- The local preference attribute is used to set preference to an exit point from the local autonomous system (AS).
- If there are multiple exit points from the AS, the local preference attribute is used to select the exit point for a specific route.

Examples

```
-> ip route-map 111 sequence-number 50 set local-preference 4
-> no ip route-map 111 sequence-number 50 set local-preference 4
```

Release History

Release 6.1.3; command introduced.

Related Commands

ip route-map action	Creates a route map and sets the status of the route map to permit or deny.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

ip route-map set level

Configures the level of the ISIS route being redistributed.

ip route-map *route-map-name* **[sequence-number** *number***] set level {level1 | level2 | level1-2}**

no ip route-map *route-map-name* **[sequence-number** *number***] set level {level1 | level2 | level1-2}**

Syntax Definitions

route-map-name	The name of the route map (up to 20 characters).
number	A number that links together the route maps. The range is 1–100.
level1	Matches IS-IS Level-1 routes only.
level2	Matches IS-IS Level-2 routes only.
level1-2	Matches IS-IS Level1-2 routes**.**

Defaults

parameter	default
number	50

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete the **set level** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route-map-name* and **sequence-number** exist before you configure this **set** criteria.

Examples

```
-> ip route-map 111 sequence-number 50 set level level1
-> no ip route-map 111 sequence-number 50 set level level1
```

Release History

Release 6.2.1; command introduced.

Related Commands

ip route-map action	Creates a route map and sets the status of the route map to permit or deny.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

ip route-map set ip-nexthop

Configures the IP address of the next hop in a route map.

ip route-map *route-map-name* **[sequence-number** *number***] set ip-nexthop** *ip_address*

no ip route-map *route-map-name* **[sequence-number** *number***] set ip-nexthop** *ip_address*

Syntax Definitions

route-map-name	The name of the route map (up to 20 characters).
number	A number that links together the route maps. The range is 1–100.
ip_address	IP address of the next hop.

Defaults

parameter	default
number	50

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete the **set ip-nexthop** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route-map-name* and **sequence-number** exist before you configure this **set** criteria.

Examples

```
-> ip route-map 222 sequence-number 50 set ip-nexthop 128.251.17.224
-> no ip route-map 222 sequence-number 50 set ip-nexthop 128.251.17.224
```

Release History

Release 6.1.5; command introduced.

Related Commands

ip route-map action	Creates a route map and sets the status of the route map to permit or deny.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaIPRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

ip route-map set ipv6-nexthop

Configures the IPv6 address of the next hop in a route map.

ip route-map *route-map-name* **[sequence-number** *number***] set ipv6-nexthop** *ipv6_address*

no ip route-map *route-map-name* **[sequence-number** *number***] set ipv6-nexthop** *ipv6_address*

Syntax Definitions

route-map-name	The name of the route map (up to 20 characters).
number	A number that links together the route maps. The range is 1–100.
ipv6_address	IPv6 address of the next hop.

Defaults

parameter	default
number	50

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete the **set ipv6-nexthop** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route-map-name* and **sequence-number** exist before you configure this **set** criteria.

Examples

```
-> ip route-map 222 sequence-number 50 set ipv6-nexthop 2001::1
-> no ip route-map 222 sequence-number 50 set ipv6-nexthop 2001::1
```

Release History

Release 6.1.5; command introduced.

Related Commands

ip route-map action	Creates a route map and sets the status of the route map to permit or deny.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaIPRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

vrf

Configures and selects a virtual routing and forwarding (VRF) instance on the switch.

vrf [*name* | **default]**

no vrf *name*

Syntax Definitions

name	The alphanumeric name (1–20 characters) assigned to the VRF instance.
default	Optional. Selects the default VRF instance.

Defaults

A default VRF instance exists in the switch configuration. All applications that are not VRF aware belong to this instance.

Parameter	Default
name | **default**	default VRF instance

Platforms Supported

OmniSwitch 9000E, 6855-U24X

Usage Guidelines

- Use the **no** form of this command to delete a VRF instance. Deleting the default instance is not allowed. In addition, any interfaces configured for a VRF instance are automatically removed when the instance is deleted.
- To return to the default VRF instance from within the context of another instance, enter the **vrf** command with or without the optional **default** parameter (for example, **vrf** or **vrf default**).
- Configuring a VRF instance name is case sensitive. In addition, if the name specified does not exist, a VRF instance is automatically created. As a result, it is possible to create instances or delete the wrong instance by accident. Use the **show ip dynamic-proxy-arp** command to verify the VRF instance configuration before adding or removing instances.
- If the name of an existing instance is specified with this command, VRF changes the command prompt to reflect the specified instance name. All CLI commands entered at this point are applied within the context of the active VRF instance.
- It is also possible to configure other instances from within the CLI context of the default VRF instance by entering the **vrf** command followed by the instance name. For example, entering **vrf IpOne ip interface intf100 address 100.1.1.1/24 vlan 100** is applied to the IpOne instance even though IpOne is not the active CLI context.

Examples

```
-> vrf IpOne
IpOne: ->

IpOne: -> vrf IpTwo
IpTwo: ->

IpTwo: -> vrf
->

IpTwo: -> vrf default
->

-> vrf IpOne ip interface intf100 address 100.1.1.1/24 vlan 100
->
```

Release History

Release 6.4.1; command introduced.

Related Commands

show vrf	Displays the VRF instance configuration for the switch.

MIB Objects

```
alaVirutalRouterNameTable
   alaVirtualRouterName
```

ip export route-map

Configures a route map to export routes from the source VRF to Global Routing Table (GRT). Only those FDB (Forwarding Routing Database) routes that match the conditions of the route map is exported to GRT.

[vrf *name***] ip export route-map** *route-map-name*

[vrf *name***] no ip export**

Syntax Definitions

name	The alphanumeric name (1–20 characters) assigned to the VRF instance. Routes are exported from the specified VRF to GRT.
route-map-name	Name of the configured route map. This route map controls export of routes from the source VRF FRD to GRT.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- If VRF is not configured, the routes are exported from the Default VRF to GRT.
- Use the **no** form of this command to disable exporting of routes from the VRF to GRT.
- Create a route-map and define protocol preference for the export policy route map by using **ip route-map** command. This route map controls export of routes from the VRF FDB to GRT. Refer to "Configuring IP" chapter in the *OmniSwitch AOS Release 6 Network Configuration Guide* for more information on how to create a route map.
- Route map configured for an export policy can contain any of the following filter and set options:
  - Filter options: ip-address, ip-next-hop, tag, protocol, ipv4-interface, metric, route-type
  - Set option: tag, metric
- Only one route map can be configured as export policy in a VRF.
- You cannot modify a route map that is tagged to an export policy.
- Route leaking between VRFs only supports IPv4 routes.

Examples

```
-> ip export route-map R1

-> vrf vrf2 ip export route-map R1

-> vrf vrf1
```

```
vrf1::-> ip export route-map R1

-> no ip export
```

Release History

Release 6.4.5; command introduced.

Related Commands

vrf	Configures and selects a virtual routing and forwarding (VRF) instance on the switch.
ip route-map action	Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
ip route-map match protocol	Matches the protocol specified in the route map with the protocol of the route.
show ip export	Displays the configured route map for exporting routes to GRT.
show ip global-route-table	Displays the Global Routing Table (GRT) for all the routes that are exported from the VRFs. This command can be executed only in default VRF.
show ip route-map	Displays the IP route maps configured on the switch.

MIB Objects

```
alaIprmConfig
   alaIprmExportRouteMap
```

ip import vrf

Configures a route map to import routes from GRT to the destination VRF from a given source VRF. The route-map is used to filter routes.

[vrf *name***] ip import vrf {***src-vrf-name* **| default} route-map** *route-map-name*

[vrf *name***] no ip import vrf {***src-vrf-name* **| default}**

Syntax Definitions

name	The alphanumeric name (1–20 characters) assigned to the VRF instance.
src-vrf-name	The export (source) VRF instance name. The routes will be imported from the specified VRF.
default	Default VRF. The routes will be imported from the default VRF.
route-map-name	Name of the configured route map. This route map controls the import of routes from GRT to the destination VRF RDB.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove importing of routes from GRT from the specified export VRF.
- Create a route-map and define the criteria that a route must match by using **ip route-map match** command. This route map controls export of routes from the VRF FDB (Forwarding Routing Database) to GRT based on the match. Refer to “Configuring IP” chapter in the *OmniSwitch AOS Release 6 Network Configuration Guide* for more information on how to create a route map.
- Route map configured for the import policy can contain any of the following filter and set options:
  - Filter options: ip-address, ip-next-hop, tag, metric
  - Set option: tag, metric
- Only one route map can be configured for an import policy for each export VRF.
- You cannot modify a route map tagged to an import policy.
- Leaked routes are only for forwarding. If a local route is leaked, that interface is not accessible in the importing VRF. Another switch will not be able to ping the interface in the import VRF.
- Leaked routes are only for forwarding plane. If a local route is leaked, that interface is not present in the importing VRF's control plane. Hence, switch will not be able to ping the interface in the import VRF as the ping is handled in the control plane.

Examples

```
-> ip import vrf V1 import route-map R2
-> no ip import VRF V1
```

Release History

Release 6.4.5; command introduced.

Related Commands

vrf	Configures and selects a virtual routing and forwarding (VRF) instance on the switch.
ip route-map action	Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
ip route-map match protocol	Matches the protocol specified in the route map with the protocol of the route.
show ip import	Displays the route map and the source VRF combination configured for importing routes.
show ip global-route-table	Displays the Global Routing Table (GRT) for all the routes that are exported from the VRFs. This command can be executed only in default VRF.
show ip route-map	Displays the IP route maps configured on the switch.

MIB Objects

```
alaIprmImportVrfTable
   alaIprmImportVrfName
   alaIprmImportVrfRouteMap
   alaIprmImportVrfRowStatus
```

show ip export

Displays the configured route map for exporting routes to GRT.

[vrf *name***] show ip export**

Syntax Definitions

name	The alphanumeric name (1–20 characters) assigned to the VRF instance.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

If a VRF is specified, configured export route map for that VRF is displayed.

Examples

```
-> show ip export
Configured Route Map = r1
```

Release History

Release 6.4.5; command introduced.

Related Commands

ip export route-map	Configures a route map to export routes from the source VRF to Global Routing Table (GRT).

MIB Objects

```
alaIprmConfig
   alaIprmExportRouteMap
```

show ip import

Displays the route map and the source VRF combination configured for importing routes.

[vrf *name***] show ip import**

Syntax Definitions

name	The alphanumeric name (1–20 characters) assigned to the VRF instance.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

If a VRF is specified, the import route map configurations for that VRF is displayed.

Examples

```
-> show ip import
Export Vrf Name      RouteMap
--------------------+-------------------
customer1            leak-in
customer2            import-filter
vrf3                 in-filter
```

output definitions

VRF Name	The name of the export/source VRF from where the routes are imported.
RouteMap	The route-map name.

Release History

Release 6.4.5; command introduced.

Related Commands

ip import vrf	Configures a route map to import routes from GRT to the destination VRF from a given source VRF.

MIB Objects

```
alaIprmImportVrfTable
   alaIprmImportVrfName
   alaIprmImportVrfRouteMap
   alaIprmImportVrfRowStatus
```

show ip global-route-table

Displays the Global Routing Table (GRT) for all the routes that are exported from the VRFs. This command can be executed only in default VRF.

show ip global-route-table [export-vrf *name***]**

Syntax Definitions

name	The alphanumeric name (1–20 characters) assigned to the VRF instance.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show ip global-route-table
Total 3 routes From All VRFs

Export VRF Name Dest Address  Subnet Mask     Gateway Addr   Metric   Tag
---------------+-------------+--------------+--------------+-------+-------
customer2        10.1.0.0     255.0.0.0       12.1.1.2        1       100
customer2        11.0.0.0     255.255.0.0     12.1.1.3        2       5
customer3        12.0.0.0     255.255.255.0   129.168.1.2     1       0
```

output definitions

VRF Name	The name of the VRF from where the routes were exported.
Destination	The address of the route.
Gateway	The next hop for the destination address.
Metric	The metric of the exported route.
Tag	The tag of the exported route.

Release History

Release 6.4.5; command introduced.

Related Commands

ip export route-map	Configures a route map to export routes from the source VRF to Global Routing Table (GRT).
show ip export	Displays the configured route map for exporting routes to GRT.

MIB Objects

```
alaGrtRouteTable
   alaGrtRouteDest
   alaGrtRouteMaskLen
   alaGrtRouteNextHop
   alaGrtRouteMetric
   alaGrtRouteTag
   alaGrtRouteVrfName
```

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.

arp *ip_address hardware_address* **[alias] [arp-name** *name***]**

no arp *ip_address* **[alias]**

Syntax Definitions

ip_address	IP address of the device you are adding to the ARP table.
hardware_address	MAC address of the device in hexadecimal format (for example,, 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.
name	The name to assign to this ARP entry.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete a permanent ARP entry.
- 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
```

Release History

Release 6.1; command 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 6400, 6850E, 6855, 9000E

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 **arp** command.
- Dynamic entries remain in the ARP table until they time out after a period of 8 minutes.

Examples

```
-> clear arp-cache
```

Release History

Release 6.1; command introduced.

Related Commands

arp	Adds a permanent entry to the ARP table.
show arp	Displays the ARP table.

MIB Objects

```
alaIpClearArpCache
```

ip dos arp-poison restricted-address

Adds or deletes an ARP Poison restricted address.

ip dos arp-poison restricted-address *ip_address*

no ip dos arp-poison restricted-address *ip_address*

Syntax Definitions

ip_address	32-bit IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the **no** form of the command to remove an already configured ARP Poison restricted address.

Examples

```
-> ip dos arp-poison restricted-address 192.168.1.1
-> no ip dos arp-poison restricted-address 192.168.1.1
```

Release History

Release 6.3.1; command introduced.

Related Commands

show ip dos arp-poison	Displays the number of attacks detected for configured ARP poison restricted-addresses.

MIB Objects

```
alaDoSArpPoisonTable
   alaDoSArpPoisonIpAddr
   alaDosArpPoisonRowStatus
```

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 IP address is examined for filtering (for example, 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this 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 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 6.1; command 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 summary	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 filter

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 6.1; command introduced.

Related Commands

arp filter	Configures an ARP filter to allow or block the processing of specified ARP Request packets.
show arp summary	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 in conjunction with the ICMP code determines the type of ICMP message being specified.
code	The ICMP code type. This in conjunction with the ICMP type 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**	disabled
gap	0

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- This command allows the user 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 messages 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**

- Enabling **Host unreachable** and **Network unreachable** messages is not recommended. Enabling these messages can cause switch instability due to high-CPU conditions, depending upon the volume of traffic required by these messages.

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 6.1; command introduced.

Related Commands

icmp messages	Enables or disables all ICMP messages.
show icmp control	Allows the viewing of the ICMP control settings.

MIB Objects

```
alaIcmpCtrlTable
   alaIcmpCtrlType
alaIcmpCtrlTable
   alaIcmpCtrlCode
   alaIcmpCtrlStatus
   alaIcmpCtrlPktGap
```

icmp unreachable

Enables or disables 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**	disabled
gap	0

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- This command enables ICMP messages relating to unreachable destinations. Unreachable networks, hosts, protocols, and ports can all be specified.
- Enabling **host-unreachable** and **net-unreachable** messages are not recommended as it can cause the switch instability due to high-CPU conditions depending upon the volume of traffic required by these messages.
- 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 6.1; command introduced.

Related Commands

show icmp control	Allows the viewing of the ICMP control settings.

MIB Objects

```
alaIcmpCtrlTable
   alaIcmpCtrlType
alaIcmpCtrlTable
   alaIcmpCtrlCode
   alaIcmpCtrlStatus
   alaIcmpCtrlPktGap
```

icmp echo

Enables or disables 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 6400, 6850E, 6855, 9000E

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 6.1; command introduced.

Related Commands

show icmp control	Allows the viewing of the ICMP control settings.

MIB Objects

```
alaIcmpCtrlTable
   alaIcmpCtrlType
alaIcmpCtrlTable
   alaIcmpCtrlCode
   alaIcmpCtrlStatus
   alaIcmpCtrlPktGap
```

icmp timestamp

Enables or disables 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 6400, 6850E, 6855, 9000E

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 6.1; command introduced.

Related Commands

show icmp control	Allows the viewing of the ICMP control settings.

MIB Objects

```
alaIcmpCtrlTable
   alaIcmpCtrlType
alaIcmpCtrlTable
   alaIcmpCtrlCode
   alaIcmpCtrlStatus
   alaIcmpCtrlPktGap
```

icmp addr-mask

Enables or disables 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 addr-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 6400, 6850E, 6855, 9000E

Usage Guidelines

- A gateway receiving an address mask request 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 6.1; command introduced.

Related Commands

show icmp control	Allows the viewing of 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 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> icmp messages enable
-> icmp messages disable
```

Release History

Release 6.1; command introduced.

Related Commands

icmp type	Enables or disables a specific type of ICMP message, and sets the minimum packet gap.
show icmp control	Allows the viewing of 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 6400, 6850E, 6855, 9000E

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 6.1; command 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 6400, 6850E, 6855, 9000E

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 6.1; command 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 6400, 6850E, 6855, 9000E

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 6.1; command 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 6400, 6850E, 6855, 9000E

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 6.1; command 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 6400, 6850E, 6855, 9000E

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 6.1; command 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 6400, 6850E, 6855, 9000E

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 6.1; command 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 6400, 6850E, 6855, 9000E

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.
- 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.

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
```

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 (for example,, 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 (for example,, 0.0.0.0) and addresses of unsupported classes (for example,, 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 (for example,, lack of buffer space). This does not include any datagrams discarded while awaiting reassembly. This value 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 (for example,, 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.
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 (for example,, lack of buffer space). This number includes datagrams counted as “Forwarded” if the packets are discarded for these reasons.
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.
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.
Fragments generated	The of IP datagram fragments generated as a result of fragmentation.

Release History

Release 6.1; command 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* | **dhcp-client]**

Syntax Definitions

name	The name associated with the IP interface.
emp	Displays the configuration and status of the Ethernet Management Port interface. This parameter is available on OmniSwitch 9000E Series switches only.
vlan_id	VLAN ID (displays a list of IP interfaces associated with a VLAN).
dhcp-client	Displays the configuration and status of the DHCP-Client interface.

Defaults

By default, all IP interfaces are displayed.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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. This parameter is available on OmniSwitch 9000E Series switches only.

Examples

```
-> show ip interface
Total 13 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
dhcp-client         172.16.105.10   255.255.255.0       UP      NO vlan 60
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
gre-1               24.24.24.1      255.255.255.0       UP     YES GRE tunnel
ipip-1              25.25.25.1      255.255.255.0       UP     YES IPIP tunnel
```

```
vlan-23             23.23.23.1      255.255.255.0       UP      YES vlan 23
```

output definitions

Name	Interface name. Generally, this is the name configured for the interface (for example,, 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 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. • **GRE tunnel**—GRE tunnel is configured for the interface. • **IPIP tunnel**—IPIP tunnel is configured for the interface. 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,
  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,

-> show ip interface dhcp-client
Interface Name = Marketing
  SNMP Interface Index          =   13600012,
  IP Address                    =   172.16.105.10,
  Subnet Mask                   =   255.255.0.0,
  Broadcast Address             =   172.16.255.255,
  Device                        =   vlan 60,
  Forwarding                    =   disabled,
  Administrative State          =   enabled,
  Operational State             =   up,
  Router MAC                    =   00:d0:95:6a:f4:55,
  Maximum Transfer Unit         =   1500,
 DHCP-CLIENT Parameter Details
  Client Status                 =   Active,
  Server IP                     =   198.206.181.55,
```

```
Lease Time Remaining          =   2 Days 10 Hours 20 Min,
Option-60                     =   Option60_example,
HostName                      =   TechPubs
```

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.
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. • **GRE tunnel**—GRE tunnel is configured for the interface. • **IPIP tunnel**—IPIP tunnel is configured for the interface. Configured through the **ip interface** command.
Forwarding	Indicates whether 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 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. • **tunnel-src-invalid—**Tunnel's source IP address is invalid. • **tunnel-dst-unreachable—**Tunnel's destination IP address is not reachable. The **tunnel-src-invalid** and **tunnel-dst-unreachable** are only applicable for the **GRE tunnel** and **IPIP tunnel** device types. **Operational State Reason** 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. Each interface assigned to the same VLAN will share the same switch MAC address.
Local Proxy ARP	Indicates whether 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.
DHCP-CLIENT Parameter Details	(Parameters below are only applicable to the 'dhcp-client' interface)
Client Status	DHCP Client Status (**In-active**, **Inactive**)
Server IP	The IP address of the DHCP server.
Lease Time Remaining	The lease time remaining for the DHCP client IP address.

output definitions (continued)

Option-60	The option-60 string that shall be included in DHCP discover/request packets.
HostName	The system name of the OmniSwitch.

The following are examples of the output display on OmniSwitch stackable and chassis-based switches:

```
-> show ip interface ipip-1
Interface Name = ipip-1
  SNMP Interface Index           =   13600001,
  IP Address                     =   25.25.25.1,
  Subnet Mask                    =   255.255.255.0,
  Device                         =   IPIP Tunnel,
  Tunnel Source Address          =   23.23.23.1
  Tunnel Destination Address     =   23.23.23.2,
  Forwarding                     =   enabled,
  Administrative State           =   enabled,
  Operational State              =   up,
  Maximum Transfer Unit          =   1480,

-> show ip interface gre-1
Interface Name = gre-1
  SNMP Interface Index           =   13600002,
  IP Address                     =   24.24.24.1,
  Subnet Mask                    =   255.255.255.0,
  Device                         =   GRE Tunnel,
  Tunnel Source Address          =   23.23.23.1
  Tunnel Destination Address     =   23.23.23.2,
  Forwarding                     =   enabled,
  Administrative State           =   enabled,
  Operational State              =   down,
  Operational State Reason       =   unbound,
  Maximum Transfer Unit          =   1476,
```

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.
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. • **GRE tunnel**—GRE tunnel is configured for the interface. • **IPIP tunnel**—IPIP tunnel is configured for the interface. Configured through the **ip interface** command.
Tunnel Source Address	The source IP address for the tunnel.
Tunnel Destination Address	The destination IP address for the tunnel.
Forwarding	Indicates whether the IP forwarding is active for the interface (**enabled** or **disabled**). Configured through the **ip interface** command.

output definitions (continued)

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 the interface is active (**up** or **down**).
Operational State Reason	Indicates why the operational state of the interface is down: • **interface-up—**The admin state of the interface is up. • **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. • **tunnel-src-invalid—**Tunnel's source IP address is invalid. • **tunnel-dst-unreachable—**Tunnel's destination IP address is not reachable. This field is only included in the display output when the operational state of the interface is **down**.
Maximum Transfer Unit	The Maximum Transmission Unit size set for the interface. Configured through the **ip interface** command.

Release History

Release 6.1; command introduced.
Release 6.3.1; **Tunnel Source Address** and **Tunnel Destination Address** fields added.
Release 6.4.3; **DHCP Client** options added.

Related Commands

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 dhcp-client	Configures a DHCP client IP interface that is to be assigned an IP address from a DHCP server.
ip interface tunnel	Configures the end points for the GRE and IPIP tunnels.
show icmp statistics	Displays ICMP statistics and errors.

MIB Objects

```
alaIpInterfaceTable
   alaIpInterfaceName
   alaIpInterfaceAddress
   alaIpInterfaceMask
   alaIpInterfaceAdminState
   alaIpInterfaceDeviceType
   alaIpInterfaceVlanID
   alaIpInterfaceIpForward
   alaIpInterfaceEncap
   alaIpInterfaceLocalProxyArp
   alaIpInterfacePrimCfg
   alaIpInterfaceOperState
   alaIpInterfaceOperReason
   alaIpInterfaceRouterMac
   alaIpInterfaceBcastAddr
```

```
alaIpInterfacePrimAct
alaIpInterfaceMtu
alaIpInterfaceTunnelSrc
alaIpInterfaceTunnelDst
```

show ip managed-interface

Displays the application name and the corresponding interface name.

show ip managed-interface

Syntax Definitions

N/A.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use this command to view the interface name used by the application.

Examples

```
-> show ip managed-interface
 Application       Interface-Name
-----------------+----------------------
 tacacs            -
 sflow             -
 ntp               Loopback0
 syslog            -
 dns               -
 dhcp-server       -
 telnet            management
 ssh               -
 tftp              -
 ldap-server       -
 radius            -
 snmp              -
 ftp               -
```

Release History

Release 6.4.3; command introduced.

Related Commands

ip managed-interface	Specifies the source IP address for the outgoing packets that are sent by the applications.

MIB Objects

```
alaIpManagedIntfTable
   AlaIpManagedIntfAppIndex
   alaIpManagedIntfEntry
   alaIpManagedIntfName
   alaIpManagedRowStatus
```

show ip route

Displays the IP Forwarding table.

[vrf *name***] show ip route [gateway** *ip_address* **| protocol** *type* **| summary | destination {***ip_address/prefixLen* | *ip_address***}]**

Syntax Definitions

name	The alphanumeric name (1–20 characters) assigned to the VRF instance.
type	Routing protocol type (local, static, OSPF, RIP, or BGP).
ip_address	Destination IP address.
ip_address/prefixLen	The destination IP address along with the prefix length of the routes processed for redistribution.
summary	Displays a summary of routing protocols that appear in the IP Forwarding table.

Defaults

By default, all routes are displayed.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The IP Forwarding table includes static routes as well as all routes learned through routing protocols (for example,, 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
 * = BFD Enabled static route
 Total 6 routes

  Dest Address      Subnet Mask       Gateway Addr      Age       Protocol
------------------+-----------------+-----------------+---------+-----------
  127.0.0.1         255.255.255.255     127.0.0.1        2d 3h    LOCAL
  10.0.0.0          255.0.0.0           10.10.1.1        2d 3h    NETMGMT
  10.0.0.0          255.255.0.0         10.10.1.1        2d 3h    NETMGMT
  10.0.0.0          255.255.255.0       10.10.1.1        2d 3h    NETMGMT
  10.1.0.0          255.255.0.0         10.10.1.1        2d 3h    NETMGMT
  10.1.1.0          255.255.255.0       10.10.1.1        2d 3h    LOCAL
```

```
-> show ip route summary

 Protocol        Route Count
---------------+--------------
 All                       7
 Local                     3
 Netmgmt                   4
 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 (for example,, a route that is 2 days and 12 hours old is displayed as 2d12h).
Protocol	Protocol by which this IP address was learned (for example,, RIP). NETMGT indicates a static route. LOCAL indicates a local interface. IMPORT indicates routes imported from other VRF(s).
Route Count	The number of routes that appear in the IP Forwarding table for each protocol type listed.

Release History

Release 6.1; command introduced.
Release 6.3.4; **BFD Enabled** field added.
Release 6.4.5; **vrf** parameter added.

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 managed-interface	Displays a list of all routes (static and dynamic) that exist in the IP router database.

MIB Objects

```
ipCidrRouteTable
   ipCidrRouteDest
   ipCidrRouteMask
   ipCidrRouteTos
   ipCidrRouteNextHop
   ipCidrRouteIfIndex
   ipCidrRouteType
   ipCidrRouteProto
   ipCidrRouteAge
   ipCidrRouteInfo
```

```
ipCidrRouteNextHopAS
ipCidrRouteMetric1
ipCidrRouteMetric2
ipCidrRouteMetric3
ipCidrRouteMetric4
ipCidrRouteMetric5
ipCidrRouteStatus
```

show ip route-pref

Displays the IPv4 routing preferences of a router.

[vrf *name***] show ip route-pref**

Syntax Definitions

name	The alphanumeric name (1–20 characters) assigned to the VRF instance.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

The command also displays the import preference.

Examples

```
-> show ip route-pref
  Protocol    Route Preference Value
------------+-----------------------
  Local                 1
  Static                2
  OSPF                110
  ISISL1              115
  ISISL2              118
  RIP                 120
  EBGP                190
  IBGP                200
  Import              210
```

Release History

Release 6.1.1; command introduced.
Release 6.4.5; **vrf** parameter added.

Related Commands

ip route-pref	Configures the route preference of a router.

MIB Objects

```
alaIprmRtPrefTable
  alaIprmRtPrefLocal
  alaIprmRtPrefStatic
  alaIprmRtPrefOspf
  alaIprmRtPrefRip
```

```
alaIprmRtPrefEbgp
alaIprmRtPrefIbgp
```

show ip redist

Displays the IPv4 route map redistribution configuration.

[vrf *name***] show ip redist [rip | ospf | isis | bgp]**

Syntax Definitions

name	The alphanumeric name (1–20 characters) assigned to the VRF instance.
rip	Displays route map redistribution configurations that use RIP as the destination (into) protocol.
ospf	Displays route map redistribution configurations that specify OSPF as the destination (into) protocol.
isis	Displays route map redistribution configurations that specify ISIS as the destination (into) protocol.
bgp	Displays the route map redistribution configurations that specify BGP as the destination (into) protocol at this time.

Defaults

By default, all route map redistribution configurations are shown.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Specify a destination protocol with this command to display only those configurations that redistribute routes into the specified protocol.

Release History

Release 6.1.3; command introduced.
Release 6.4.5; **vrf** parameter added.

Examples

```
-> show ip redist

Source       Destination
Protocol     Protocol     Status    Route Map
-------------+------------+---------+--------------------
RIP          OSPF         Enabled   ipv4rm
BGP          RIP          Enabled   ipv4rm
IMPORT       RIP          Enabled   ipv4rm
```

```
-> show ip redist rip

Source       Destination
Protocol     Protocol     Status    Route Map
-------------+------------+---------+--------------------
BGP          RIP          Enabled   ipv4rm
IMPORT       RIP          Enabled   ipv4rm
```

output definitions

Source Protocol	The protocol from which the routes are learned.
Destination Protocol	The protocol into which the source protocol routes are redistributed.
Status	The administrative status (**Enabled** or **Disabled**) of the route map redistribution configuration.
Route Map	The name of the route map that is applied with this redistribution configuration.

Related Commands

ip redist	Controls the conditions for redistributing different IPv6 routes between protocols.

MIB Objects

```
alaRouteMapRedistProtoTable
   alaRouteMapRedistSrcProtoId
   alaRouteMapRedistDestProtoId
   alaRouteMapRedistRouteMapIndex
   alaRouteMapRedistStatus
   alaRouteMapRedistAddressType
   alaRouteMapRedistRowStatus
```

show ip access-list

Displays the details of the access list.

show ip access-list [*access-list-name***]**

Syntax Definitions

access-list-name	Name of the access list.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

If the *access-list-name* is not specified in this command, all the access lists will be displayed.

Examples

```
-> show ip access-list
                    Address /                   Redistribution
Name                Prefix Length      Effect   Control
--------------------+------------------+-------+--------------
al_3                10.0.0.0/8          permit   all-subnets
al_3                11.0.0.0/8          permit   all-subnets
al_4                1.0.0.0/8           permit   no-subnets
al_4                10.0.0.0/8          permit   all-subnets

-> show ip access-list al_4

                    Address /                   Redistribution
Name                Prefix Length      Effect   Control
--------------------+------------------+-------+--------------
al_4                1.0.0.0/8           permit   no-subnets
al_4                10.0.0.0/8          permit   all-subnets
```

output definitions

Name	Name of the access list.
Address/Prefix Length	IP address that belongs to the access list.
Effect	Indicates whether the IP address is permitted or denied for redistribution.
Redistribution Control	Indicates the conditions specified for redistributing the matched routes.

Release History

Release 6.1.3; command introduced.

Related Commands

ip access-list	Creates an access list for adding multiple IPv4 addresses to route maps.
ip access-list address	Adds multiple IPv4 addresses to the access list.

MIB objects

```
alaRouteMapAccessListIndex
alaRouteMapAccessListAddressType
alaRouteMapAccessListAddress
alaRouteMapAccessListPrefixLength
alaRouteMapAccessListAction
alaRouteMapAccessListRedistControl
```

show ip route-map

Displays the IP route maps configured on the switch.

show ip route-map [*route-map-name***]**

Syntax Definitions

route-map-name	The name of the specific route map.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

If the *route-map-name* is not specified in this command, all the route maps are displayed.

Examples

```
-> show ip route-map
Route Maps: configured: 1 max: 200
Route Map: Route_map1 Sequence Number: 50 Action permit
  match ip address 10.0.0.0/8 redist-control all-subnets permit
  set metric 100 effect replace
```

Release History

Release 6.1.3; command introduced.

Related Commands

ip route-map action	Creates a route map and sets the status of the route map to permit or deny.
ip route-map match ip address	Matches the route with the specified IPv4 address or with addresses contained in an IPv4 access list specified by the access list name.
ip route-map match ipv6 address	Matches the route with the specified IPv6 address or with addresses contained in an IPv6 access list specified by the access list name
ip route-map match ip-nexthop	Matches the routes that have a next-hop router address permitted by the specified access list.
ip route-map match ipv6-nexthop	Matches the routes that have an IPv6 next-hop router address permitted by the specified access list
ip route-map match tag	Permits or denies a route based on the specified next-hop IP address.
ip route-map match tag	Matches the tag value specified in the route map with the one that the routing protocol learned the route on.
ip route-map match metric	Matches the metric value specified in the route map with the one that the routing protocol learned the route on.
ip route-map match route-type	Matches the specified route type with the one that the routing protocol learned the route on.

MIB Objects

```
alaRouteMapRedistProtoTable
   alaRouteMapRedistRouteMapIndex
alaRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

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 and where duplicate routes are compared to determine the best route for the Forwarding Routing Database. 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.

[vrf *name***] show ip router database [protocol** *type* | **gateway** *ip_address* | **dest {***ip_address/prefixLen* | *ip_address***}]**

Syntax Definitions

name	The alphanumeric name (1–20 characters) assigned to the VRF instance.
type	Routing protocol type (local, static, OSPF, RIP, or BGP).
ip_address	Destination IP address.
ip_address/prefixLen	The destination IP address along with the prefix length of the routes processed for redistribution.

Defaults

By default, all routes are displayed.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 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 forwarding table 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.

- Static routes that appear as inactive are not included in the main IP router database listing. If an inactive route becomes active, however, it is removed from the inactive list and added to the active route list.

Examples

```
-> show ip router database
Legend: + indicates routes in-use
        * indicates BFD-enabled static route
        r indicates recursive static route, with following address in brackets

Total IPRM IPv4 routes: 9
Destination         Gateway          Protocol Metric Tag   Misc-Info
------------------+----------------+--------+------+-----+-------
+ 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
+ 10.212.66.0/24      10.212.66.17     LOCAL    1      46
+r 143.209.92.0/24     172.28.6.254     STATIC   1     N/A  [192.168.10.1]
+ 172.28.6.0/24       172.28.6.2       LOCAL    1      6
+ 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 STATIC name HRDept
Legend: + indicates routes in-use
        * indicates BFD-enabled static router indicates recursive static route,
          with following address in brackets

Total IPRM IPv4 routes: 2

Destination         Gateway   Interface    Protocol Metric  Tag   Misc-Info
------------------+----------+--------+-----------+------+----+---------------
+ 10.0.3.0/24      30.0.3.1     intf        STATIC     1    123   {HRDept}

Inactive Static Routes
Destination       Gateway        Metric
-----------------+--------------+----------


-> show ip router database dest 10.212.62.0/24 protocol ospf
Destination         Gateway          Protocol Metric Tag   Misc-Info
------------------+----------------+--------+------+-----+---------
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) + indicates routes in-use * indicates BFD-enabled static route 'r' indicates a recursive static route.
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.
Tag	The VLAN on which the route was *learned*, not forwarded. **N/A** appears in this field for static routes as they are not learned on a VLAN.
Misc-Info	Used for various output such as IP address of the recursive static route or IP address of backup routes.

Release History

Release 6.1; command introduced.
Release 6.1.5; mask parameter deleted; /prefixLen parameter added.
Release 6.4.3; '**r**' added to indicate recursive static route.
Release 6.4.5; **vrf** parameter added.

Related Commands

show ip route	Displays the IP Forwarding table.

MIB Objects

```
alaIprmRouteTable
   alaIprmRouteDest
   alaIprmRouteMask
   alaIprmRouteTos
   alaIprmRouteNextHop
   alaIprmRouteProto
   alaIprmRouteMetric
   alaIprmRoutePriority
```

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 6400, 6850E, 6855, 9000E

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 emp-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 (for example,, a route that is 2 days and 12 hours old is displayed as 2d12h).
Protocol	Protocol by which this IP address was learned (for example,, RIP). NETMGT indicates a static route. LOCAL indicates a local interface.

Release History

Release 6.1; command introduced.

Related Commands

ping	Tests whether an IP destination can be reached from the local switch.
traceroute	Finds 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 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show ip config
IP directed-broadcast   =   OFF,
IP default TTL          =   64
Dual Hash Mode          =   enabled (reboot required)
```

output definitions

IP directed-broadcast	Indicates whether the IP directed-broadcast feature is on or off.
IP default TTL	IP default TTL interval.
Dual Hash Mode	The status of dual-hash mode and whether a reboot is required for it to take effect.

Release History

Release 6.1; command introduced.
Release 6.4.5; Dual Hash Mode field added.

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 6400, 6850E, 6855, 9000E

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 6.1; command 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 6400, 6850E, 6855, 9000E

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
avlan-http-proxy          262   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 6.1; command 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 ip dynamic-proxy-arp

Displays the dynamic proxy ARP table. The ARP table contains a listing of router IP addresses and their corresponding translations to physical MAC addresses.

show ip dynamic-proxy-arp

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The OmniSwitch provides the proxy ARP functionality for the addresses contained in this table.
- Dynamic proxy arp is used in conjuntion with the DHCP Snooping and Port Mapping features.

Examples

```
-> show ip dynamic-proxy-arp
Router IP Addr        Hardware Addr           VLAN       Interfaces
----------------+-----------------------+----------+--------------------
 172.18.16.1            00:d0:95:3a:e8:08     10             1/1
 172.18.16.100          00:1a:92:42:ac:63     20             3/2
```

output definitions

Router IP Addr	Router IP address.
Hardware Addr	Router MAC address.
VLAN	The VLAN the entry is learned on.
Interface	The interface the entry is learned on.

Release History

Release 6.4.3; command introduced.

Related Commands

port mapping dynamic-proxy-arp	Enables or disables the dynamic proxy arp functionality on a port mapping session.
ip helper dhcp-snooping	Enables or disables dhcp snooping.

MIB Objects

```
alaIpNetToMediaDpGroup
   alaIpNetToMediaDpaPhysAddress
   alaIpNetToMediaDpaIpType
   alaIpNetToMediaDpaIp
   alaIpNetToMediaDpaSlot
   alaIpNetToMediaDpaPort
```

show vrf

Displays the Multiple VRF instance configuration for the switch.

show vrf

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 9000E, 6855-U24X

Usage Guidelines

Information is displayed for all VRF instances configured on the switch.

Examples

```
-> show vrf
Virtual Routers   Protocols
-----------------------------
        default
          IpOne   RIP
          IpTwo   BGP
```

Release History

Release 6.4.1; command introduced.

Related Commands

vrf	Configures a Multiple VRF instance for the switch.

MIB Objects

```
alaVirutalRouterNameTable
   alaVirtualRouterNameIndex
   alaVirtualRouterName
```

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 6400, 6850E, 6855, 9000E

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  Name
-----------------+------------------+----------+-------+--------+----------+------
 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
 10.255.13.25      00:b0:d0:42:80:24   DYNAMIC               0/20  vlan 13   agg20
 10.255.13.26      00:b0:d0:42:82:59   DYNAMIC               0/20  vlan 13   agg20
 10.255.11.254     11:50:04:11:11:11   STATIC                3/20  vlan 1   demoarp
```

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
Port	The port or link aggregate on the switch attached to the device identified by the IP address.

output definitions (continued)

Interface	The interface to which the entry belongs (for example,, VLAN, EMP).
Name	User configured name of static arp entry.

Release History

Release 6.1; command 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 summary

Displays the number of each ARP entry type.

show arp summary

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show arp summary

   Type               Count
-----------------+-----------
 Total                105

 Static                 2
 Dynamic                100
 Authenticated          3
 Proxy                  0
 VRRP                   0
```

output definitions

Type	The type of ARP entry.
Count	The number of entries for that type.

Release History

Release 6.1; command introduced.

Related Commands

show arp	Displays the ARP table.

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 6400, 6850E, 6855, 9000E

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 to **block** or **allow** a switch response to an ARP packet that matches the filter.

Release History

Release 6.1; command 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

Allows the viewing of the ICMP control settings.

show icmp control

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 6.1; command introduced.

Related Commands

icmp type	Enables or disables a specific type of ICMP message, and sets the minimum packet gap.
icmp unreachable	Enables or disables ICMP messages pertaining to unreachable destinations, and sets the minimum packet gap.
icmp echo	Enables or disables ICMP echo messages, and sets the minimum packet gap.
icmp timestamp	Enables or disables ICMP timestamp messages, and sets the minimum packet gap.
icmp addr-mask	Enables or disables 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 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the ICMP Table 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 (for example,, bad ICMP checksums, bad length).
Destination unreachable	Number of “destination unreachable” messages that were sent/received by the switch.

output definitions (continued)

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 the gateway’s software.
Source quench	Number of messages sent/received that tell a host that it is sending too many packets. A host 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 6.1; command 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 6400, 6850E, 6855, 9000E

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 (for example,, 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 6.1; command 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 6400, 6850E, 6855, 9000E

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 accepts 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.

output definitions (continued)

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 6.1; command 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 6400, 6850E, 6855, 9000E

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 6.1; command 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 6400, 6850E, 6855, 9000E

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 6.1; command 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 6400, 6850E, 6855, 9000E

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 a DoS attack is in progress, and a trap is generated to inform the system administrator.

Examples

```
-> show ip dos config

   Dos type                                    Status
-------------------------------------------+-----------------
   port scan                                   ENABLED
   tcp sync flood                              ENABLED
   ping of death                               ENABLED
   smurf                                       ENABLED
   pepsi                                       ENABLED
   land                                        ENABLED
   teardrop/bonk/boink                         ENABLED
   loopback-src                                ENABLED
   invalid-ip                                  ENABLED
   invalid-multicast                           ENABLED
   unicast dest-ip/multicast-mac               ENABLED
   ping overload                               DISABLED
   arp flood                                   ENABLED
   arp poison                                  ENABLED
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,
Dos MAximum Ping Rate                          =  100
Dos Maximum ARP Request Rate                   =  500
```

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.
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 6.1; command introduced.

Related Commands

show ip dos statistics	Displays the statistics on detected DoS attacks for the switch.

MIB Objects

```
alaDosTable
   alaDoSType
```

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 6400, 6850E, 6855, 9000E

Usage Guidelines

- This command displays the number of attacks the switch has detected for several types of DoS attacks.
- If an attack is detected and reported, it does not necessarily mean that an attack occurred. The switch assumes 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                     0
tcp sync flood                0
ping of death                 0
smurf                         0
pepsi                         0
land                          0
teardrop/bonk/boink           0
loopback-src                  0
invalid-ip                    0
invalid-multicast             0
unicast dest-ip/multicast-mac 0
ping overload                 0
arp flood                     0
arp poison                    0
```

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 6.1; command introduced.

Related Commands

show ip dos config	Displays the configuration parameters of the DoS scan for the switch.

MIB Objects

```
alaDoSTable
   alaDoSType
```

show ip dos arp-poison

Displays the number of attacks detected for configured ARP poison restricted-addresses.

show ip dos arp-poison

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show ip dos arp-poison
  IP Address                          Attacks
-----------------------------------+------------
192.168.1.1                            0
192.168.1.2                            0
192.168.1.3                           0
```

output definitions

IP Address	The configured ARP Poison restricted-addresses.
Attacks detected	The number of ARP Poison attacks detected for each address.

Release History

Release 6.3.1; command introduced.

Related Commands

ip dos arp-poison restricted-address	Adds or deletes an ARP Poison restricted address.

MIB Objects

```
alaDoSArpPoisonTable
   alaDoSArpPoisonIpAddr
   alaDoSArpPoisonDetected
```

ip wccp admin-state

Enables or disables the Web Cache Communication Protocol (WCCP) globally on the switch.

ip wccp admin-state {enable | disable}

Syntax Definitions

enable	Enables the administrative status for the WCCP feature.
disable	Disables the administrative status for the WCCP feature.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

Use this command to enable or disable the WCCP globally on the switch.

Examples

```
-> ip wccp admin-state enable
-> ip wccp admin-state disable
```

Release History

Release 6.4.4; command introduced.

Related Commands

clear ip wccp	Clears the statistics for the given service group.
show ip wccp service-group	Displays the global statistics related to WCCP.
show ip wccp service-group	Displays the WCCP statistics related to the specified service group.

MIB Objects

```
wccpAdminEnabled
```

ip wccp service-group web-cache md5

Configures one or a range of service groups and sets the MD5 authentication.

ip wccp service-group {web-cache | *service-id***[-***service-id2***]} [md5 password** *string***]**

no ip wccp service-group {web-cache | *service-id***[-***service-id2***]}**

Syntax Definitions

web-cache	The well-known service (ID = 0).
service-id	A WCCP service ID number (1 to 255). Use a hyphen to specify a range of service IDs (5-10).
string	The MD5 password for the service group (0 to 8 characters).

Defaults

parameter	default
md5 authentication	**disabled**

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

Use the **no** form of the command to remove the service group.

Examples

```
-> ip wccp service-group web-cache
-> ip wccp service-group web-cache md5 password san
-> ip wccp service-group 10
-> ip wccp service-group 10 md5 password san
-> no ip wccp service-group web-cache
-> no ip wccp service-group 10
-> no ip wccp service-group 2-8
```

Release History

Release 6.4.4; command introduced.

Related Commands

clear ip wccp	Clears the statistics for the given service group.
show ip wccp services	Displays the list of service groups created on the switch and their related information.

MIB Objects

```
wccpServiceTable
   wccpServiceId
   wccpServicePassword
```

ip wccp service-group web-cache restrict

Restricts a port, VLAN or IP in a service group from processing WCCP messages.

ip wccp service-group {web-cache | *service-id***} restrict { port** *slot/port* | **vlan** *vlan_id* | **ip** *ipv4* **[mask** *mask***]}**

no ip wccp service-group {web-cache | *service-id***} restrict { port** *slot/port* | **vlan** *vlan_id* | **ip** *ipv4* **[mask** *mask***]}**

Syntax Definitions

web-cache	The well-known service (ID = 0).
service-id	A WCCP service ID number (1 to 255).
slot/port	Restricts the specified port from processing the WCCP messages.
vlan_id	Restricts the specified VLAN from processing the WCCP messages.
ipv4	Restricts the specified cache server IP from processing the WCCP messages.
mask	Specifies an optional mask when an IPv4 address is used.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

Use the **no** form of the command to remove the restriction from the service group.

Examples

```
-> ip wccp service-group web-cache restrict port 1/20
-> no ip wccp service-group web-cache restrict port 1/20
-> ip wccp service-group 10 restrict vlan 20
-> no ip wccp service-group 10 restrict vlan 20
-> ip wccp service-group 10 restrict ip 30.0.0.20
-> no ip wccp service-group 10 restrict ip 30.0.0.20
```

Release History

Release 6.4.4; command introduced.

Related Commands

show ip wccp restricts	Displays the restricted ports, VLANs and server IPs for the service groups created on the switch.

MIB Objects

```
wccpRestrictPortTable
   wccpRestrictPortServiceId
   wccpRestrictPortIndex
wccpRestrictVlanTable
   wccpRestrictVlanServiceId
   wccpRestrictVlanVlanId
wccpRestrictWebCacheTable
   wccpRestrictWebCacheServiceId
   wccpRestrictWebCacheIpAddress
   wccpRestrictWebCacheIpMask
```

clear ip wccp

Clears the statistics for the given service group.

clear ip wccp [service-group {web-cache | *service-id*}] statistics

Syntax Definitions

web-cache	The well-known service (ID = 0).
service-id	A WCCP service ID number (1 to 255).

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

If no service group is specified, then the statistics for all the service groups are cleared.

Examples

```
-> clear ip wccp service-group web-cache statistics
-> clear ip wccp statistics
```

Release History

Release 6.4.4; command introduced.

Related Commands

show ip wccp service-group	Displays the global statistics related to WCCP.

MIB Objects

```
wccpStatisticsTable
   wccpStatsServiceId
```

show ip wccp status

Displays the WCCP admin status.

show ip wccp status

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

N/A.

Examples

```
-> show ip wccp status
Admin status            : Enabled
```

Release History

Release 6.4.4; command introduced.

Related Commands

ip wccp admin-state	Enable or disable the WCCP globally on the switch.

MIB Objects

```
wccpServiceTable
   wccpAdminEnabled
```

show ip wccp services

Displays the list of service groups created on the switch and their related information.

show ip wccp services

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show ip wccp services
Service  Status   RcvId   Chgs  Caches   Type     Version   Password  Redirects
-------+--------+--------+-----+-------+--------+----------+---------+-------------
  95     Enable    42       20     1     Dynamic    2          Yes        0
```

output definitions

Service	Indicates the WCCP service ID.
Status	Indicates the admin status of the WCCP service.
RcvId	Indicates the current Receive Id from the router for the WCCP service. This is incremented every time a WCCP message is sent.
Chgs	Indicates the current change number for the service. This gets updated each time there is a WCCP topology change.
Caches	Indicates the total number of cache servers currently active on the WCCP service.
Type	Indicates the WCCP service type.
Version	Indicates the WCCP service version.
Password	Indicates if password has been specified for the WCCP service.
Redirects	Indicates the number of packets WCCP has redirected for the service.

Release History

Release 6.4.4; command introduced.

Related Commands

ip wccp admin-state	Enable or disable the WCCP globally on the switch.
ip wccp service-group web-cache md5	Allows to configure or remove a service group.

MIB Objects

```
wccpServiceTable
   wccpServiceId
   wccpServiceAdminEnabled
   wccpServiceRecieveId
   wccpServiceChangeNumber
   wccpServiceWebCacheCount
   wccpServiceType
   wccpServiceVersion
   wccpServicePassword
   wccpStatsPacketsRedir
```

show ip wccp cache-engines

Displays the various cache servers learned for the service groups created and their related information.

show ip wccp cache-engines

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show ip wccp cache-engines
Service     Status     RcvId   Chgs       IP        RcvId  Chgs   Routers   Caches
----------+----------+--------+-----+------------+-------+-----+---------+---------
      95    Enable     14781   161      40.1.1.2   14781    1      1          1
```

output definitions

Service	Indicates the WCCP service ID.
Status	Indicates the admin status of the WCCP service..
RcvId	Indicates the current Receive Id from the router for the WCCP service. This is incremented every time a WCCP message is sent.
Chgs	Indicates the current change number for the service. This gets updated each time there is a WCCP topology change.
IP	Indicates the IP address of the Cache-Engine.
Routers	Indicates how many WCCP routers the Cache-Engine is in contact with.
Caches	Indicates the total count of cache servers currently active on the WCCP service.

Release History

Release 6.4.4; command introduced.

Related Commands

ip wccp admin-state	Enable or disable the WCCP globally on the switch.

MIB Objects

```
wccpServiceTable
   wccpServiceId
   wccpServiceAdminEnabled
   wccpServiceRecieveId
   wccpServiceChangeNumber
wccpWebCacheTable
   wccpWebCacheIpAddress
   wccpWebCacheNumberOfRouters
   wccpServiceWebCacheCount
```

show ip wccp restricts

Displays the restricted ports, VLANs and cache server IPs for the created service group.

show ip wccp [service-group {web-cache | *service-id***}] restricts**

Syntax Definitions

web-cache	The well-known service (ID = 0).
service-id	A WCCP service ID number (1 to 255).

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

If no service group is specified, the restrictions for all the service groups created is displayed..

Examples

```
-> show ip wccp restricts
Service     Port
----------+---------
95           1/23

Service    VLAN
----------+--------
95          100

Service         IP              Mask
----------+----------------+--------------------
65         50.0.0.90         255.255.255.255
95         60.0.0.0          255.255.255.0
```

output definitions

Service	Indicates the WCCP service ID.
Port	Indicates the restricted port number for the respective service group.
VLAN	Indicates the restricted VLAN Id for the respective service group.
IP	Indicates the restricted IP address for the respective service group.
Mask	Indicates the IP mask of the restricted IP address.

Release History

Release 6.4.4; command introduced.

Related Commands

ip wccp service-group web-cache restrict	Allows to restrict a port, VLAN or IP in a service group from processing WCCP messages.

MIB Objects

```
wccpRestrictPortTable
   wccpRestrictPortServiceId
   wccpRestrictPortIndex
wccpRestrictVlanTable
   wccpRestrictVlanServiceId
   wccpRestrictVlanVlanId
wccpRestrictWebCacheTable
   wccpRestrictWebCacheServiceId
   wccpRestrictWebCacheIpAddress
   wccpRestrictWebCacheIpMask
```

show ip wccp service-group

Displays the WCCP statistics related to the specified service group.

show ip wccp service-group {web-cache | *service-id***}**

Syntax Definitions

web-cache	The well-known service (ID = 0).
service-id	A WCCP service ID number (1 to 255).

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

If no service group is specified the information for all the service groups created is displayed.

Examples

```
-> show ip wccp service-group web-cache
Global WCCP Information:
       Service Name/ID              :  web-cache,
       Protocol                     :  TCP,
       Ports                        :  80, 0, 0, 0, 0, 0, 0, 0,
       Port Type                    :  Source,
       Precedence                   :  240,
       Number of Cache Engines      :  1,
       Number of Routers            :  1,
       Type of Message              :  Unicast,
       Total Packets Redirected     :  50,
       Total WCCP Messages Dropped  :  0,
       Total Authentication failures :  0
```

output definitions

Service Name/ID	Indicates the WCCP service ID.
Protocol	Indicates the protocol type for the WCCP service.
Ports	Indicates the list of TCP/UDP ports identified for the service group.
Port Type	Indicates the port type.
Precedence	Indicates the priority of the service group. The lowest priority is 0, the highest is 255.
Number of Cache Engines	Indicates the total number of cache servers currently active on the WCCP service.

output definitions (continued)

Number of Routers	Indicates the total number WCCP routers the Cache-Engine is connected.
Type of Message	Indicates the mode of WCCP message exchange used (unicast/multicast).
Total Packets Redirected	Indicates the count of how many packets the WCCP has redirected for the service.
Total WCCP Messages Dropped	Indicates the count of how many WCCP packets were dropped for the service.
Total Authentication failures	Indicates the count of how many WCCP packets resulted in authentication failure because of mismatch in the password used for the service on the Router and Cache-Engine.

Release History

Release 6.4.4; command introduced.

Related Commands

ip wccp service-group web-cache md5	Allows to configure or remove a service group.

MIB Objects

```
wccpServiceTable
   wccpServiceId
   wccpServiceProtocol
   wccpServicePortPortNum
wccpWebCacheTable
   wccpServiceWebCacheCount
   wccpWebCacheNumberOfRouters
wccpStatisticsTable
   wccpServiceMessageType
   wccpStatsPacketsRedir
   wccpStatsInvalidMessages
   wccpStatsAuthFailures
```

show ip wccp service-group detail

Displays detailed statistics of the switch and the cache engine for specified service group.

show ip wccp [service-group {web-cache | *service-id***}] detail**

Syntax Definitions

web-cache	The well-known service (ID = 0).
service-id	A WCCP service ID number (1 to 255).

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

If the service group is not specified, then the statistics related to all the service groups are displayed.

Examples

```
-> show ip wccp service-group web-cache detail
WCCP Detail:
Service ID: web-cache
        Router information:
            IP Address         :  10.135.38.120,
            Protocol Version   :  2.0

        Cache-Engine Information
         IP Address           :  192.168.1.1
         Protocol Version     :  2.0,
         State                :  Usable,
         Connect Time         :  01:10:55

-> show ip wccp detail
WCCP Detail:
Service ID: web-cache
        Router information:
            IP Address         :  10.135.38.120,
            Protocol Version   :  2.0

        Cache-Engine Information
         IP Address           :  192.168.1.1,
         Protocol Version     :  2.0,
         State                :  Usable,
         Connect Time         :  01:10:55

Service ID: 95
        Router information:
            IP Address         :  10.135.38.120,
```

```
    Protocol Version   :  2.0

Cache-Engine Information
 IP Address           :  192.168.1.2,
 Protocol Version     :  2.0,
 State                :  Usable,
 Connect Time         :  00:10:17
```

output definitions

Service ID	Indicates the WCCP service ID.
Router information	Indicates the IP address of the router and the WCCP service version supported by the Router.
Cache-Engine Information	
IP Address	Indicates the IP address of the Cache-Engine.
Protocol Version	Indicates the WCCP service version supported by the Cache-Engine.
State	Indicates the state of the Cache-Engine.
Connect Time	Indicates the time at which the cache server became active for the service.

Release History

Release 6.4.4; command introduced.

Related Commands

ip wccp admin-state	Enable or disable the WCCP globally on the switch.

MIB Objects

```
wccpServiceTable
   wccpServiceId
   wccpServiceVersion
wccpWebCacheTable
   wccpWebCacheIpAddress
   wccpServiceVersion
   wccpWebCacheState
   wccpWebCacheConnectTime
```

show ip wccp service-group view

Displays the WCCP view for the specified service group.

show ip wccp [service-group {web-cache | *service-id*}] view

Syntax Definitions

web-cache	The well-known service (ID = 0).
service-id	A WCCP service ID number (1 to 255).

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

If the service group is not specified, then the information related to all the service groups are displayed.

Examples

```
-> show ip wccp service-group 95 view
WCCP View:
Service ID : 95
      Routers Participating:
        10.135.38.120,
        10.135.38.140
      Cache Engines Usable:
        192.168.1.1, Connect Since: 01:10:55,
        192.168.1.2, Connect Since: 01:10:30
      Cache Engines Un-Usable:
        -none-

-> show ip wccp view
WCCP View:
Service ID: web-cache
     Routers Participating:
       10.135.38.120,
       10.135.38.140
     Cache Engines Usable:
       192.168.1.1, Connected Since: 01:10:55,
       192.168.1.2, Connected Since: 01:10:30
     Cache Engines Un-Usable:
       -none-

Service ID : 95
     Routers Participating:
       10.135.38.120
     Cache Engines Usable:
       192.168.1.2, Connected Since: 02:50:06,
```

```
    192.168.1.4, Connected Since: 00:30:10
  Cache Engines Un-Usable:
    192.168.1.5, Disconnected Since: 00:35:10
```

output definitions

Service ID	Indicates the WCCP service ID.
Routers Participating	Indicates the IP addresses of the routers participating in the service group.
Cache Engines Usable	Indicates the IP addresses of the Usable Cache-Engines participating in the service group, and the time when the cache server became active.
Cache Engines Un-Usable	Indicates the IP addresses of the Un-Usable Cache-Engines participating in the service group, and the time when the cache server became inactive.

Release History

Release 6.4.4; command introduced.

Related Commands

ip wccp admin-state	Enable or disable the WCCP globally on the switch.
show ip wccp service-group	Displays the global statistics related to the WCCP.

MIB Objects

```
wccpServiceTable
   wccpServiceId
wccpWebCacheTable
   wccpWebCacheServiceId
   wccpWebCacheIpAddress
   wccpWebCacheConnectTime
wccpRouterTable
   wccpRouterServiceId
   wccpRouterIpAddressType
   wccpRouterIpAddress
```

show ip wccp service-group statistics

Displays the total number of WCCP messages transmitted, received, and dropped for the specified service group.

show ip wccp [service-group {web-cache | *service-id*}] statistics

Syntax Definitions

web-cache	The well-known service (ID = 0).
service-id	A WCCP service ID number (1 to 255).

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

If the service group is not specified, then the statistics related to all the service groups is displayed including the total of all such statistics, along with the total number of invalid WCCP messages received.

Examples

```
-> show ip wccp service-group 95 statistics
Service ID: 95
        Total WCCP messages Received         : 338,
        Total WCCP messages Transmitted      : 339,
        Total WCCP messages Dropped          : 0


-> show ip wccp statistics
Service ID: web-cache
        Total WCCP messages Received         : 0,
        Total WCCP messages Transmitted      : 0,
        Total WCCP messages Dropped          : 0

Service ID: 95
        Total WCCP messages Received         : 358,
        Total WCCP messages Transmitted      : 359,
        Total WCCP messages Dropped          : 0

Total:
        Total WCCP messages Received         : 358,
        Total WCCP messages Transmitted      : 359,
        Total WCCP messages Dropped          : 0,
        Total WCCP messages Invalid          : 12
```

output definitions

Service ID	Indicates the WCCP service ID.
Total WCCP messages Received	Indicates the total number of WCCP messages received by the router for the service group (if specified), else it displays the total for all the service groups created.
Total WCCP messages Transmitted	Indicates the total number of WCCP messages transmitted by the router for the service group (if specified), else it displays the total for all the service groups created.
Total WCCP messages Dropped	Indicates the total number of WCCP Messages dropped due to WCCP restrictions applied to Port/Vlan/Ip for a service group (if specified), else it displays the total for all the service groups created.

Release History

Release 6.4.4; command introduced.

Related Commands

ip wccp admin-state	Enable or disable the WCCP globally on the switch.
clear ip wccp	Clears the statistics for the given service group.

MIB Objects

```
wccpStatisticsTable
   wccpServiceId
   wccpStatsMessagesReceived
   wccpStatsMessagesTransmitted
   wccpStatsMessagesDropped
```

ip dos anti-spoofing

Enable or disable IP anti-spoofing globally on the switch.

ip dos anti-spoofing {enable | disable}

Syntax Definitions

enable	Enable IP anti-spoofing.
disable	Disable IP anti-spoofing.

Defaults

By default, IP anti-spoofing is enabled globally on the switch.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- By default, anti-spoofing is enabled on all the IP or VRRP interface. Anti-spoof is enabled for VRRP interface only if the interface is in active state and is a VRRP master.
- If IP anti-spoofing is enabled, any IP packet ingressing on the switch with VLAN and the IP-address of that VLAN as source information is dropped.

Examples

```
-> ip dos anti-spoofing enable
-> ip dos anti-spoofing disable
```

Release History

Release 6.4.5; command introduced.

Related Commands

ip dos anti-spoofing address	Enable or disable IP anti-spoofing on a specific interface (IP interface or VRRP interface).
show ip dos anti-spoofing	Displays attack information and the last attempted source (VLAN, MAC address, port) of all the IP and VRRP interfaces configured on the switch.
ip dos anti-spoofing clear stats	Clears the IP anti-spoofing attack information globally.

MIB Objects

```
alaDoSIpAntiSpoof
```

ip dos anti-spoofing arp-only

Enable or disable ARP-only anti-spoofing globally on the switch.

ip dos anti-spoofing arp-only {enable | disable}

Syntax Definitions

enable	Enable ARP anti-spoofing.
disable	Disable ARP anti-spoofing.

Defaults

By default, ARP-only anti-spoofing is disabled globally on the switch.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

IP spoofing must be enabled globally to enable ARP-only spoofing. ARP-only anti-spoofing is enabled for VRRP interface only if interface is in an active state and is a VRRP master.

Examples

```
-> ip dos anti-spoofing arp-only enable
-> ip dos anti-spoofing arp-only disable
```

Release History

Release 6.4.5; command introduced.

Related Commands

ip dos anti-spoofing	Enable or disable IP anti-spoofing globally on the switch.
ip dos anti-spoofing address arp-only	Enable or disable ARP-only anti-spoofing on an interface (IP interface or VRRP interface).
show ip dos anti-spoofing	Displays attack information and the last attempted source (VLAN, MAC address, port) of all the IP and VRRP interfaces configured on the switch.
ip dos anti-spoofing clear stats	Clears the IP anti-spoofing attack information globally.

MIB Objects

```
alaDoSIpAntiSpoof
```

ip dos anti-spoofing address

Enable or disable IP anti-spoofing on a specific interface (IP interface or VRRP interface).

ip dos anti-spoofing address *ip-address* **{enable | disable}**

Syntax Definitions

ip-address	IP address of the interface.
enable	Enable IP anti-spoofing.
disable	Disable IP anti-spoofing.

Defaults

By default, IP anti-spoof is enabled globally on the switch.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- IP spoofing must be enabled globally to enable IP spoofing at an interface level. IP anti-spoofing is enabled for VRRP interface only if the interface is in an active state and is a VRRP master.
- If you want to enable IP anti-spoofing on a specific interface, ARP-only anti spoofing must be disabled on that interface.

Examples

```
-> ip dos anti-spoofing address 192.168.10.1 enable
-> ip dos anti-spoofing address 192.168.10.1 disable
```

Release History

Release 6.4.5; command introduced.

Related Commands

ip dos anti-spoofing	Enable or disable IP anti-spoofing globally on the switch.
show ip dos anti-spoofing	Displays attack information and the last attempted source (VLAN, MAC address, port) of all the IP and VRRP interfaces configured on the switch.
ip dos anti-spoofing address clear stats	Clears the IP anti-spoofing attack information at an interface level.

MIB Objects

`alaDoSIpAntiSpoof`

ip dos anti-spoofing address arp-only

Enable or disable ARP-only anti-spoofing for a specific interface (IP interface or VRRP interface).

ip dos anti-spoofing address *ip-address* **arp-only {enable | disable}**

Syntax Definitions

ip-address	IP address of the interface.
enable	Enable ARP-only anti-spoofing.
disable	Disable ARP-only anti-spoofing.

Defaults

By default, IP anti-spoof is enabled globally on the switch.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- ARP-only anti-spoofing must be enabled globally to enable ARP-only anti-spoofing at an interface level.
- The ARP-only anti-spoofing is enabled for VRRP interface only if the interface is active and is a VRRP master.

Examples

```
-> ip dos anti-spoofing address 172.18.16.1 arp-only enable
-> ip dos anti-spoofing address 172.18.16.1 arp-only disable
```

Release History

Release 6.4.5; command introduced.

Related Commands

ip dos anti-spoofing address arp-only	Enable or disable ARP-only anti-spoofing on an interface (IP interface or VRRP interface).
show ip dos anti-spoofing	Displays attack information and the last attempted source (VLAN, MAC address, port) of all the IP and VRRP interfaces configured on the switch.
ip dos anti-spoofing clear stats	Clears the IP anti-spoofing attack information globally.

MIB Objects

`alaDoSIpAntiSpoof`

ip dos anti-spoofing clear stats

Clears the IP anti-spoofing attack information globally.

ip dos anti-spoofing clear stats

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use of this command clears all the attack information and resets the counters.

Examples

```
-> ip dos anti-spoofing clear stats
```

Release History

Release 6.4.5; command introduced.

Related Commands

show ip dos anti-spoofing	Displays attack information and the last attempted source (VLAN, MAC address, port) of all the IP and VRRP interfaces configured on the switch.
ip dos anti-spoofing address clear stats	Clears the IP anti-spoofing attack information at an interface level.

MIB Objects

```
alaDoSIpAntiSpoof
```

ip dos anti-spoofing address clear stats

Clears the IP anti-spoofing attack information at an interface level.

ip dos anti-spoofing address *ip-address* **clear stats**

Syntax Definitions

ip-address	IP address of the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use of this command clears all the attack information and resets the counters for a specific interface or VRRP interface IP.

Examples

```
-> ip dos anti-spoofing address 172.18.16.95 clear stats
```

Release History

Release 6.4.5; command introduced.

Related Commands

show ip dos anti-spoofing	Displays attack information and the last attempted source (VLAN, MAC address, port) of all the IP and VRRP interfaces configured on the switch.
ip dos anti-spoofing clear stats	Clears the IP anti-spoofing attack information globally.

MIB Objects

```
alaDoSIpAntiSpoof
```

show ip dos anti-spoofing

Displays the attack information and the last attempted source (VLAN, MAC address, port) of all the IP and VRRP interfaces configured on the switch. Specify the IP address to view the attack information for a specific interface.

show ip dos anti-spoofing [*ip-address***]**

Syntax Definitions

ip-address	IP address of the interface or VRRP interface.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show ip dos anti-spoofing
Global Status:
IP Spoof Status- Enabled
ARP-only Spoof status -Disabled

*- VRRP IP Address

                                        Last Attempted Source
 IP Address       Anti-Spoofing     Attacks   VLAN      MAC               PORT
---------------+----------------+-----------+------+-------------------+---------
127.0.0.1            IN              0         0    00:00:00:00:00:00     0/0
15.15.15.1           IP              131       15   e8:e7:32:14:11:6e     2/15
172.18.16.36         IP              0         0    00:00:00:00:00:00     0/0
*15.15.15.15         IP              0         0    00:00:00:00:00:00     0/0

IP - Anti-spoofing for IP Pkts
ARP -  Anti-spoofing for ONLY ARP Pkts
IN - Inactive
```

```
-> show ip dos anti-spoofing 15.15.15.2
Global Status:
IP Spoof Status- Enable
ARP-only Spoof status -Disable

*- VRRP IP Address
                                    Last Attempted Source

 IP Address       Anti-Spoofing     Attacks   VLAN      MAC               PORT
---------------+----------------+-----------+------+-------------------+---------
15.15.15.2           IP              587       15    00:00:5e:00:01:01     2/15

IP - Anti-spoofing for IP Pkts
ARP -  Anti-spoofing for ONLY ARP Pkts
IN - Inactive
```

output definitions

Global Status	Indicates the IP spoofing or ARP-only spoofing status. Enabled or disabled.
IP Address	Interface or VRRP address for which spoof detection is enabled.
Anti-Spoofing	Anti-spoofing detected for IP or ARP packets.
Attacks	Number of attacks or packets dropped.
Last Attempted Source	Signifies the attack received from which VLAN or MAC address or port.

Release History

Release 6.4.5; command introduced.

Related Commands

ip dos anti-spoofing	Enable or disable IP anti-spoofing globally on the switch.
ip dos anti-spoofing address	Enable or disable IP anti-spoofing on a specific interface (IP interface or VRRP interface).
ip dos anti-spoofing clear stats	Clears the IP anti-spoofing attack information globally.
ip dos anti-spoofing address clear stats	Clears the IP anti-spoofing attack information at an interface level.

MIB Objects

```
alaDoSIpAntiSpoof
```

20 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 IPv4. 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 on 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.

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: AlcatelIND1Iprmv6.mib
Module: alcatelIND1IprmV6MIB

Filename: AlcatelIND1Ripng.mib
Module: alcatelIND1RipngMIB

A summary of the IPv6 commands is listed here:

IPv6	**ipv6 interface** **ipv6 address** **ipv6 address global-id** **ipv6 address local-unicast** **ipv6 dad-check** **ipv6 hop-limit** **ipv6 pmtu-lifetime** **ipv6 host** **ipv6 neighbor stale-lifetime** **ipv6 neighbor** **ipv6 prefix** **ipv6 static-route** **ipv6 route-pref** **ping6** **traceroute6** **show ipv6 hosts** **show ipv6 interface** **show ipv6 pmtu table** **clear ipv6 pmtu table** **show ipv6 neighbors** **clear ipv6 neighbors** **show ipv6 prefixes** **show ipv6 routes** **show ipv6 route-pref** **show ipv6 router database** **show ipv6 tcp ports** **show ipv6 traffic** **clear ipv6 traffic** **show ipv6 tunnel** **show ipv6 udp ports** **show ipv6 information**
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** **ipv6 rip interface metric** **ipv6 rip interface recv-status** **ipv6 rip interface send-status** **ipv6 rip interface horizon** **show ipv6 rip** **show ipv6 rip interface** **show ipv6 rip peer** **show ipv6 rip routes**

ipv6 interface

Configures an IPv6 interface on a VLAN or IPv6 tunnel.

ipv6 interface *if_name* **[vlan** *vid* **| tunnel {***tid* **| 6to4}] [enable | disable]**
[base-reachable-time *time***]**
[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.
base-reachable-time *time*	Base value used to compute the reachable time for neighbors reached via this 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 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to delete an interface.
- When you create an IPv6 interface, it is enabled by default.
- 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 4, “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 address global-id** command.

Examples

```
-> ipv6 interface Test vlan 1
-> ipv6 interface Test_Tunnel tunnel 2
-> ipv6 interface Test_6to4 tunnel 6to4
```

Release History

Release 6.1; command introduced.
Release 6.1.1; **base-reachable-time** parameter added.

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
   alaIPv6InterfaceBaseReachableTime
   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* **[anycast] {***if_name* **| loopback}**

ipv6 address *ipv6_prefix* **eui-64 {***if_name* | **loopback}**

no ipv6 address *ipv6_prefix* **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). (3..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

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to delete an address.
- You can assign multiple IPv6 addresses to an IPv6 interface.
- No default value for prefix length.
- 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 4, “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 address global-id** command.

Examples

```
-> ipv6 address 4132:86::19A/64 Test_Lab
-> ipv6 address 2002:d423:2323::35/64 Test_6to4
```

Release History

Release 6.1; command 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 address global-id

Automatically generates or allows a new global ID to be entered.

ipv6 address global-id {generate | *globalID*}

Syntax Definitions

generate	Automatically generates the global ID.
globalID	A 5-byte global ID value specified in the form hh:hhhh:hhhh

Defaults

By default, the IPv6 global ID is set to all zeros.

Platforms Supported

OmniSwitch 6855, 6850E, 9000E

Usage Guidelines

- Global ID needs to be automatically generated or configured explicitly.
- A 40-bit global identifier is used to make the local IPv6 address prefixes globally unique.
- The global ID will be generated the first time a local unicast address is added via the **ipv6 address local-unicast** command or when the **ipv6 address global-id** command is executed.

Examples

```
-> ipv6 address global-id generate
-> ipv6 address global-id 32:57a3:8fed
```

Release History

Release 6.3.4; command introduced.

Related Commands

ipv6 address local-unicast	Creates a IPv6 local unicast address using the configured global ID.
ipv6 bgp unicast	Enables or disables unicast IPv6 updates for the BGP routing process.
show ip bgp	Displays the current global settings for the local BGP speaker.

MIB Objects

```
alaIPv6GlobalID
```

ipv6 address local-unicast

Creates a IPv6 local unicast address using the configured global ID.

ipv6 address local-unicast [global-id *globalID***] [subnet-id** *subnetID***] {interface-id** *interfaceID* **| eui-64} [prefix-length** *prefixLength***]** *{if-name* **| loopback}**

[no] ipv6 address local-unicast [global-id *globalID***] [subnet-id** *subnetID***] {interface-id** *interfaceID* **| eui-64} [prefix-length** *prefixLength***]** *{if-name* **| loopback}**

Syntax Definitions

globalID	A 5-byte global ID value specified in the form hh:hhhh:hhhh.
subnetID	A 2-byte Subnet ID specified in the form 0xhhhh. The valid range is 0x0000-0xffff or 0-65535.
interfaceID	An interface identifier specified in the form hhhh:hhhh:hhhh:hhhh.
eui-64	Automatically-generated EUI-64 value to be used for interface identfier.
prefixLength	The number of bits that are significant in the IPv6 address (mask). The valid range is 0-128; however, the default value should rarely be over-ridden.
if-name	The name assigned to the interface.
loopback	The loopback for the loopback interface.

Defaults

parameter	default
prefixLength	64

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to delete the local unicast address. However, addresses are normally deleted using the **ipv6 address** command.
- If the global ID value is not explicitly specified, the default global ID set by the **ipv6 address global-id** command is used.
- If the global ID value is explicitly configured using the **ipv6 address local-unicast** command, the address' global ID will not be changed if the **ipv6 address global-id** command is executed.
- The use of a double-colon abbreviation for the interface identifier similar to that used for full IPv6 addresses is allowed.

Examples

```
-> ipv6 address local-unicast global-id 0073:110:255 subnet-id 23 interface-id
215:60ff:fe7a:adc0 prefix-length 64 loopback
```

Release History

Release 6.3.4; command introduced.

Related Commands

ipv6 address global-id	Automatically generates or allows a new global ID to be entered. .
show ipv6 information	Displays IPv6 information.

MIB Objects

```
alaIPv6LocalUnicastGlobalID
alaIPv6LocalUnicastSubnetID
alaIPv6LocalUnicastInterfaceID
alaIPv6LocalUnicastEUI64
alaIPv6LocalUnicastPrefixLength
```

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 6400, 6855, 6850E, 9000E

Usage Guidelines

Use the **ipv6 interface** command to create an IPv6 tunnel interface.

Examples

```
-> ipv6 interface Test tunnel 2 source 10.255.11.242 destination 10.255.11.12
```

Release History

Release 6.1; command 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 6400, 6855, 6850E, 9000E

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.

Examples

```
-> ipv6 dad-check fe80::2d0:95ff:fe6a:f458/64 Test_Lab
```

Release History

Release 6.1; command 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 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to return the hop limit to its default value.
- Inputting the value 0 (zero) will result in the default (64) hop-limit.

Examples

```
-> ipv6 hop-limit 64
```

Release History

Release 6.1; command introduced.

Related Commands

show ipv6 information	Displays IPv6 information.

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 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> ipv6 pmtu-lifetime 30
```

Release History

Release 6.1; command introduced.

Related Commands

show ipv6 pmtu table	Displays the IPv6 path MTU Table.
show ipv6 information	Displays IPv6 information.
clear ipv6 pmtu table	Removes all the 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 6400, 6855, 6850E, 9000E

Usage Guidelines

Use the **no** form of this command to remove the mapping from the host table.

Examples

```
-> ipv6 host Lab 4235::1200:0010
```

Release History

Release 6.1; command introduced.

Related Commands

show ipv6 hosts	Displays IPv6 Local Hosts Table.

MIB Objects

```
alaIPv6HostTable
   alaIPv6HostName
   alaIPv6HostAddress
   alaIPv6HostRowStatus
```

ipv6 neighbor stale-lifetime

Configures the minimum lifetime for all neighbor entries.

ipv6 neighbor stale-lifetime *stale-lifetime*

Syntax Definitions

stale-lifetime	Minimum lifetime for neighbor entries in the stale state (5–2800).

Defaults

parameter	default
stale-lifetime	1440

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> ipv6 neighbor stale-lifetime 1400
```

Release History

Release 6.1.1; command introduced.

Related Commands

show ipv6 neighbors	Displays IPv6 Neighbor Table.
show ipv6 information	Displays IPv6 information.

MIB Objects

```
IPv6IfIndex
   alaIPv6NeighborTable
   alaIPv6NeighborStaleLifetime
```

ipv6 neighbor

Configures a static entry in 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 (for example, 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 6400, 6855, 6850E, 9000E

Usage Guidelines

Use the **no** form of this command to remove an entry from IPv6 Neighbor Table.

Examples

```
-> ipv6 neighbor 4132:86::203 00:d0:c0:86:12:07 Test 1/1
```

Release History

Release 6.1; command introduced.

Related Commands

show ipv6 neighbors	Displays IPv6 Neighbor Table.
show ipv6 information	Displays IPv6 information.

MIB Objects

```
IPv6IfIndex
alaIPv6NeighborTable
   alaIPv6NeighborNetAddress
   alaIPv6NeighborPhysAddress
   alaIPv6NeighborSlot
   alaIPv6NeighborPort
   alaIPv6NeighborRowStatus
   alaIPv6NeighborStaleLifetime
```

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). (1...127).
valid-lifetime *time*	Length of time, in seconds, that this prefix will remain valid (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 (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 (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 6400, 6855, 6850E, 9000E

Usage Guidelines

Use the **no** form of this command to delete a prefix.

Examples

```
-> ipv6 prefix 4132:86::/64 Test
```

Release History

Release 6.1; command 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 static-route

Creates/deletes an IPv6 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.

ipv6 static-route *ipv6_prefix/prefix_length* **gateway** *ipv6_address* **[***if_name***][metric** *metric***][tag** *tag-num***][name** *tag-name***]**

no ipv6 static-route *ipv6_prefix/prefix_length* **gateway** *ipv6_address* **[***if_name***][metric** *metric***][tag** *tag-num***][name** *tag-name***]**

Syntax Definitions

ipv6_prefix	IPv6 network that is the destination of this static route.
/prefix_length	The number of bits (0...128) that are significant in the iPv6 address (mask).
gateway *ipv6_address*	IPv6 address of the next hop used to reach the destination IPv6 address.
if_name	If the next hop is a link-local address, the name of the interface used to reach it.
metric	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.
tag-num	The tag number.
tag-name	The name of the tag.

Defaults

parameter	default
metric	1

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a static route.
- A name can be assigned to the static route to identify it quickly at a later time.
- If you want to classify certain static routes and filter them, then a tag value may be allocated to those routes and route-map match statement to filter those routes. If the tag or name value is not specified, then the previously configured values for the tag and name will remain unchanged.
- In order to remove the previously configured tag value, configure the same route with tag value as 0. This will be equivalent to un-tagging the route.
- To remove the previously configured name value, configure the static route with the name field as “”. Un-configuring the static route will as intended delete both the tag and name values.

- To view the tag and name of the configured static routes, use the **show ipv6 router database** command.

Examples

```
-> ipv6 static-route 10.1.5.1/64 gateway fe80::2d0:95ff:fe6a:f458 v6if-137 metric 3
-> Ipv6 static-route 10.1.1.1/128 gateway 30.00.1.1 name HRDept
-> Ipv6 static-route 10.4.7.1/128 gateway 30.5.4.1 name Finance
-> ipv6 static-route 10.2.1/128 gateway 30.2.1.1 tag 234
```

Release History

Release 6.1.3; command was introduced.
Release 6.4.5; **tag** and **name** parameter was added.

Related Commands

show ipv6 routes	Displays IPv6 Forwarding Table.
show ipv6 router database	Displays a list of all routes (static and dynamic) that exist in the IPv6 router database.

MIB Objects

```
alaIprmv6StaticRouteTable
   alaIprmV6StaticRouteDest,
   alaIprmV6StaticRoutePfxLength,
   alaIprmV6StaticRouteNexthop,
   alaIprmV6StaticRouteMetric,
   alaIprmV6StaticRouteTag,
   alaIprmV6StaticRouteName,
```

ipv6 route-pref

Configures the route preference of a router.

ipv6 route-pref {static | ospf | rip | ebgp | ibgp} *value*

Syntax Definitions

static	Configures the route preference of static routes.
ospf	Configures the route preference of OSPF3 routes.
rip	Configures the route preference of RIPng routes.
ebgp	Configures the route preference of external BGP routes.
ibgp	Configures the route preference of internal BGP routes.
value	Route preference value.

Defaults

parameter	default
static *value*	2
ospf *value*	110
rip *value*	120
ebgp *value*	190
ibgp *value*	200

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Route preference of local routes cannot be changed.
- The valid route preference range is 1–255.
- The IPv6 version of BGP is not supported currently.

Examples

```
-> ipv6 route-pref ospf 20
-> ipv6 route-pref rip 60
```

Release History

Release 6.1.3; command introduced.

Related Commands

show ipv6 route-pref	Displays the configured route preference of a router.

MIB Objects

```
alaIprmRtPrefTable
   alaIprmRtPrefLocal
   alaIprmRtPrefStatic
   alaIprmRtPrefOspf
   alaIprmRtPrefRip
   alaIprmRtPrefEbgp
   alaIprmRtPrefIbgp
```

ping6

Tests 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 6400, 6855, 6850E, 9000E

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.

Examples

```
-> ping6 fe80::2d0:95ff:fe6a:f458/64
```

Release History

Release 6.1; command introduced.

Related Commands

traceroute6	Finds the path taken by an IPv6 packet from the local switch to a specified destination.

traceroute6

Finds 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 6400, 6855, 6850E, 9000E

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.

Examples

```
-> traceroute6 41EA:103::65C3
```

Release History

Release 6.1; command introduced.

Related Commands

ping6	Tests whether an IPv6 destination can be reached from the local switch.

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 6400, 6855, 6850E, 9000E

Usage Guidelines

If you do not specify a substring, all IPv6 hosts are displayed.

Examples

```
-> show ipv6 hosts

Name                                      IPv6 Address
------------------------------------------+-------------------------------------
ipv6-test1.alcatel-lucent.com                    4235::1200:0010
ipv6-test2.alcatel-lucent.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 6.1; command introduced.

Related Commands

ipv6 host	Configures a static host name to the 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 6400, 6855, 6850E, 9000E

Usage Guidelines

Use the ICMP table to monitor and troubleshoot the switch.

Examples

```
-> 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, and so on).

output definitions (continued)

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 6.1; command 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 6400, 6855, 6850E, 9000E

Usage Guidelines

- If you do not specify an interface name, all IPv6 interfaces are displayed.
- Specify an interface name (for example, VLAN 12) to obtain a more detailed information about a specific interface.

Examples

```
-> 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.

output definitions

Status	Interface status (for example, Active/Inactive).
Device	The device on which the interface is configured (for example, 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 6.1; command 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 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show ipv6 pmtu table

1-PMTU Entry
PMTU entry minimum lifetime = 10m
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 6.1; command introduced.

Related Commands

ipv6 pmtu-lifetime	Configures the minimum lifetime for entries in the path MTU Table.
clear ipv6 pmtu table	Removes all the entries from the IPv6 path MTU Table.

MIB Objects

```
alaIPv6ConfigTable
   alaIPv6PMTUDest
   alaIPv6PMTUexpire
```

clear ipv6 pmtu table

Removes all the entries from the IPv6 path MTU Table.

clear ipv6 pmtu table

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> clear ipv6 pmtu table
```

Release History

Release 6.1; command 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 6400, 6855, 6850E, 9000E

Usage Guidelines

If you do not specify an option (for example, if_name), all IPv6 neighbors are displayed.

Examples

```
-> 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 (for example, vlan_1)

Release History

Release 6.1; command 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 IPv6 Neighbor Table.

clear ipv6 neighbors

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

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.

Examples

```
-> clear ipv6 neighbors
```

Release History

Release 6.1; command introduced.

Related Commands

ipv6 neighbor	Configures a static entry in 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 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> 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 (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 (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 (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 6.1; command 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 6400, 6855, 6850E, 9000E

Usage Guidelines

If you do not specify an option (for example, “static”), all IPv6 interfaces are displayed.

Examples

```
-> 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   Gateway Address           Interface         Age          Protocol  Flags
Prefix
-------------+-----------------------+---------------+------------+---------+-----
::/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 (for example, 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 6.1; command introduced.

Related Commands

ipv6 static-route	Configures a static entry in the IPv6 route.

MIB Objects

```
IPv6RouteTable
   IPv6Routes
   IPv6RoutesPrefix
   IPV6RoutesStatic
alaIPv6StaticRouteTable
   alaIPv6StaticRouteEntry
```

show ipv6 route-pref

Displays the IPv6 routing preference of the router.

show ipv6 route-pref

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

The IPv6 version of BGP is not supported currently.

Examples

```
-> show ipv6 route-pref
  Protocol    Route Preference Value
------------+-----------------------
  Local                   1
  Static                  2
  OSPF                  110
  RIP                   120
  EBGP                  190
  IBGP                  200
```

Release History

Release 6.1.1; command introduced.

Related Commands

ipv6 route-pref	Configures the IPv6 route preference of a router.

show ipv6 router database

Displays a list of all routes (static and dynamic) that exist in the IPv6 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 IPv6 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 iv6p router database [protocol *type* | **gateway** *ipv6_address* | **dest** *ipv6_prefix/prefix_length***]**

Syntax Definitions

type	Routing protocol type (local, static, OSPF, RIP, or BGP).
gateway *ipv6_address*	IPv6 address of the next hop used to reach the destination IPv6 address.
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).

Defaults

By default, all routes are displayed.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- The IPv6 forwarding table is derived from IPv6 router database processing performed by the switch and contains only unique routes that the switch currently uses. Use the **show ipv6 routes** command to view the forwarding table.
- If an expected route does not appear in the IPv6 forwarding table, use the **show ipv6 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 forwarding table if a duplicate route with a higher protocol precedence exists.
- A list of inactive static routes is also included in the **show ipv6 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 as inactive are not included in the main IP router database listing. If an inactive route becomes active, however, it is removed from the inactive list and added to the active route list.

Examples

```
-> show ipv6 router database
Legend: + indicates routes in use

Total IPRM IPv6 routes: 5

Destination/Prefix  Gateway Address           Interface         Protocol  Metric
------------------+------------------------+-----------------+---------+-------
::/0                2002:d468:8a89::137       v6if-6to4-137      Static    1
137:35:35::/64      fe80::2d0:95ff:fe12:f470  v6if-tunnel-137    OSPF      2
195:35::/64         fe80::2d0:95ff:fe12:f470  v6if-to-eagle      OSPF      2
212:95:5::/64       fe80::2d0:95ff:fe12:f470  smbif-5            Local     1
2002::/16           2002:d423:2323::35        v6if-6to4-137      Local     1

Inactive Static Routes:

VLAN  Destination/Prefix   Gateway Address          Metric
-----+------------------+------------------------+-------
1510  212:95:5::/64       fe80::2d0:95ff:fe6a:f458   1
```

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 (for example, VLAN 6to4tunnel); or loopback.
Protocol	Protocol by which this IPv6 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 6.1.3; command introduced.

Related Commands

show ipv6 routes	Displays the IPv6 Forwarding Table.

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 6400, 6855, 6850E, 9000E

Usage Guidelines

Only connections between IPv6 addresses are contained in this table.

Examples

```
-> 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 6.1; command 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 6400, 6855, 6850E, 9000E

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.

Examples

```
-> show ipv6 traffic

Global 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 (for example, version number mismatch, other format errors, hop count exceeded, and 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 (for example, ::0) and unsupported addresses (for example, 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, but which were discarded (for example, 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, and so on).
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 (for example, 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.

output definitions

Fragments generated	Number of output packet fragments generated as a result of fragmentation.
Multicast packets	Number of multicast packets transmitted.

Release History

Release 6.1; command 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 6400, 6855, 6850E, 9000E

Usage Guidelines

Use the **show ipv6 traffic** command to view current IPv6 traffic statistics.

Examples

```
-> clear ipv6 traffic
```

Release History

Release 6.1; command 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 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> 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 6.1; command introduced.

Related Commands

ipv6 address global-id	Configures the source and destination IPv4 addresses for a configured tunnel.

MIB Objects

```
alaIPv6ConfigTunnelTable
   alaIPv6Tunnel6to4
   alaIPv6ConfigTunnelv4Source
   alaIPv6ConfigTunnelv4Dest
```

show ipv6 udp ports

Displays 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 6400, 6855, 6850E, 9000E

Usage Guidelines

Only endpoints utilizing IPv6 addresses are displayed in this table.

Examples

```
-> show ipv6 udp ports

Local Address                                Port  Interface
---------------------------------------------+-----+--------------------
::                                            521
```

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 6.1; command introduced.

Related Commands

show ipv6 tcp ports	Displays TCP Over IPv6 Connection Table.

MIB Objects

```
IPv6UdpTable
   IPv6UdpEntry
   IPv6UdpLocalAddress
   IPv6UdpLocalPort
   IPv6UdpIfIndex
```

show ipv6 information

Displays the global IPv6 configuration values.

show ipv6 information

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show ipv6 information

Default hop limit                     = 64
Path MTU entry minimum lifetime (min) = 60
Neighbor stale lifetime (min)         = 1440
Local Unicast Global ID               = 32:57a3:8fed
```

output definitions

Default hop limit	The value placed in the hop limit field in router advertisements
Path MTU entry minimum lifetime	Minimum lifetime for entries in the path MTU.
Neighbor stale lifetime	Minimum lifetime for neighbor entries in the stale state.
Local Unicast Global ID	40-bit global identifier which makes the local IPv6 address prefixes globally unique.

Release History

Release 6.1.1; command introduced.
Release 6.3.4; **Local Unicast Global ID** field added.

Related Commands

ipv6 neighbor	Configures a static entry in the IPv6 Neighbor Table.
ipv6 pmtu-lifetime	Configures the minimum lifetime for entries in the path MTU Table.
ipv6 hop-limit	Configures the value placed in the hop limit field in the header of all IPv6 packet.

MIB Objects

```
ipv6MibObjects
   Ipv6DefaultHopLimit
alaIPv6ConfigTable
   alaIPv6PMTUMinLifetime
alaIPv6NeighborTable
   alaIPv6NeighborStaleLifetime
   alaIPv6GlobalID
```

ipv6 redist

Controls the conditions for redistributing IPv6 routes between different protocols.

ipv6 redist {local | static | rip | ospf | isis | bgp} into {rip | ospf | isis | bgp} route-map *route-map-name* **[status {enable | disable}]**

no ipv6 redist {local | static | ospf | isis | bgp} into {rip | ospf | isis | bgp} [route-map *route-map-name***]**

Syntax Definitions

local	Redistributes local IPv6 routes.
static	Redistributes static IPv6 routes.
rip	Specifies RIP as the source or destination (into) protocol.
ospf	Specifies OSPF as the source or destination (into) protocol.
bgp	This parameter is currently not supported.
isis	This parameter is currently not supported.
route-map-name	Name of an existing route map that will control the redistribution of routes between the source and destination protocol.
enable	Enables the administrative status of the redistribution configuration.
disable	Disables the administrative status of the redistribution configuration.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a route map redistribution configuration. Note that if a route map name is not specified, all route maps associated with the redistribution configuration are removed.
- The source and destination protocols must be loaded and enabled before redistribution occurs.
- The IPv6 version of BGP is not supported currently.
- Use the **ip route-map** commands described in the “IP Commands” chapter of this guide to create a route map. Refer to the “Configuring IP” chapter in the *OmniSwitch AOS Release 6 Network Configuration Guide* for more information about how to create a route map.

Examples

```
-> ipv6 redist rip into ospf route-map rip-to-ospf1
-> ipv6 redist rip into ospf route-map rip-to-ospf2
-> no ipv6 redist rip into ospf route-map rip-to-ospf2
-> ipv6 redist local into rip route-map local-to-rip
-> ipv6 redist local into rip route-map local-to-rip disable
```

Release History

Release 6.1.3; command introduced.

Related Commands

show ipv6 redist	Displays the route map redistribution configuration.

MIB Objects

```
alaRouteMapRedistProtoTable
   alaRouteMapRedistSrcProtoId
   alaRouteMapRedistDestProtoId
   alaRouteMapRedistRouteMapIndex
   alaRouteMapRedistStatus
   alaRouteMapRedistAddressType
   alaRouteMapRedistRowStatus
```

ipv6 access-list

Creates an IPv6 access list that is used to specify multiple IPv6 addresses for a route map configuration.

ipv6 access-list *access-list-name*

no ipv6 access-list *access-list-name*

Syntax Definitions

access-list-name	Name of the IPv6 access list (up to 20 characters).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

Use the **no** form of this command to delete the access list.

Examples

```
-> ipv6 access-list access1
-> no ipv6 access-list access1
```

Release History

Release 6.1.3; command introduced.

Related Commands

ipv6 access-list address	Adds IPv6 addresses to an existing IPv6 access list.
show ipv6 access-list	Displays the contents of an IPv6 access list.

MIB Objects

```
alaRouteMapAccessListNameTable
   alaRouteMapAccessListName
   alaRouteMapAccessListNameIndex
   alaRouteMapAccessListNameAddressType
   alaRouteMapAccessListNameRowStatus
```

ipv6 access-list address

Adds IPv6 addresses to the specified IPv6 access list.

ipv6 access-list *access-list-name* **address** *address/prefixLen* **[action {permit | deny}] [redist-control {all-subnets | no-subnets | aggregate}]**

no ipv6 access-list *access-list-name* **address** *address/prefixLen*

Syntax Definitions

access-list-name	Name of the IPv6 access list (up to 20 characters).
address/prefixLen	IPv6 address along with the prefix length to be added to the access list.
permit	Permits the IPv6 address for redistribution.
deny	Denies the IPv6 address for redistribution.
all-subnets	Redistributes or denies all the subnet routes that match the network portion of the IP address as specified by the mask length.
no-subnets	Redistributes or denies only those routes that exactly match the IP address and the mask length.
aggregate	Redistributes an aggregate route if there are one or more routes that match or are subnets of this address.

Defaults

parameter	default
permit | deny	**permit**
all-subnets | no-subnets | aggregate	**all-subnets**

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to delete the address from the access list.
- The *access-list-name* should exist before you add multiple IPv6 addresses to the IPv6 access list.
- The **action** parameters (**permit** and **deny**) determine if a route that matches the **redist-control** configuration for the IP address is allowed or denied redistribution.
- The **redist-control** parameters (**all-subnets, no-subnets**, and **aggregate**) defines the criteria used to determine if a route matches an address in the access list.
- Note that configuring the combination of **redist-control aggregate** with **action deny** is not allowed.

- Use this command multiple times with the same access list name to add multiple addresses to the existing IPv6 access list.

Examples

```
-> ipv6 access-list access1 address 2001::1/64 action permit
-> ipv6 access-list access1 address 2001::1/64 redist-control aggregate
-> no ipv6 access-list access1 address 2001::1/64
```

Release History

Release 6.1.3; command introduced.

Related Commands

ipv6 access-list	Creates an IPv6 access list that is used to specify multiple IPv6 addresses for a route map configuration.
show ipv6 access-list	Displays the contents of an IPv6 access list.

MIB Objects

```
alaRouteMapAccessListTable
   alaRouteMapAccessListIndex
   alaRouteMapAccessListAddress
   alaRouteMapAccessListAddressType
   alaRouteMapAccessListPrefixLength
   alaRouteMapAccessListAction
   alaRouteMapAccessListRedistControl
   alaRouteMapAccessListRowStatus
```

show ipv6 redist

Displays the IPv6 route map redistribution configuration.

show ipv6 redist [rip | ospf | bgp]

Syntax Definitions

rip	Displays the route map redistribution configurations that specify RIP as the destination (into) protocol.
ospf	Displays the route map redistribution configurations that specify OSPF as the destination (into) protocol.
bgp	This parameter is not supported.

Defaults

By default all route map redistribution configurations are shown.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Specify a destination protocol with this command to display only those configurations that redistribute routes into the specified protocol.
- The IPv6 version of BGP is not supported currently.

Release History

Release 6.1.3; command introduced.

Examples

```
-> show ipv6 redist

Source       Destination
Protocol     Protocol     Status    Route Map
------------+------------+---------+--------------------
localIPv6    RIPng        Enabled   ipv6rm
RIPng        OSPFv3       Enabled   ipv6rm

-> show ipv6 redist ospf

Source       Destination
Protocol     Protocol     Status    Route Map
------------+------------+---------+--------------------
RIPng        OSPFv3       Enabled   ipv6rm
```

output definitions

Source Protocol	The protocol from which the routes are learned.
Destination Protocol	The protocol into which the source protocol routes are redistributed..
Status	The administrative status (**Enabled** or **Disabled**) of the route map redistribution configuration.
Route Map	The name of the route map that is applied with this redistribution configuration.

Related Commands

ipv6 redist	Controls the conditions for redistributing IPv6 routes between different protocols.

MIB Objects

```
alaRouteMapRedistProtoTable
   alaRouteMapRedistSrcProtoId
   alaRouteMapRedistDestProtoId
   alaRouteMapRedistRouteMapIndex
   alaRouteMapRedistStatus
   alaRouteMapRedistAddressType
   alaRouteMapRedistRowStatus
```

show ipv6 access-list

Displays the contents of the specified IPv6 access list.

show ip access-list [*access-list-name***]**

Syntax Definitions

access-list-name	Name of the IPv6 access list.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

If the *access-list-name* is not specified in this command, all the access lists will be displayed.

Examples

```
-> show ipv6 access-list
                    Address /                   Redistribution
Name                Prefix Length      Effect   Control
--------------------+------------------+-------+--------------
al_3                128::/64           permit   all-subnets
al_4                124::/64           permit   no-subnets

-> show ipv6 access-list 4

                    Address /                   Redistribution
Name                Prefix Length      Effect   Control
--------------------+------------------+-------+--------------
al_4                124::/64           permit   no-subnets
```

output definitions

Name	Name of the IPv6 access list.
Address/Prefix Length	IPv6 address that belongs to the access list.
Effect	Indicates whether the IPv6 address is permitted or denied for redistribution.
Redistribution Control	Indicates the conditions specified for redistributing the matched routes.

Release History

Release 6.1.3; command introduced

Related Commands

ipv6 access-list	Creates an IPv6 access list for adding multiple IPv6 addresses to route maps.
ipv6 access-list address	Adds multiple IPv6 addresses to the IPv6 access list.

MIB objects

```
alaRouteMapAccessListIndex
   alaRouteMapAccessListAddressType
   alaRouteMapAccessListAddress
   alaRouteMapAccessListPrefixLength
   alaRouteMapAccessListAction
   alaRouteMapAccessListRedistControl
```

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 6400, 6855, 6850E, 9000E

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.

Examples

```
-> ipv6 load rip
```

Release History

Release 6.1; command 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 or disables RIPng on the switch.

ipv6 rip status {enable | disable}

Syntax Definitions

N/A

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

RIPng must be loaded on the switch (**ipv6 load rip**) to enable RIP on the switch.

Examples

```
-> ipv6 rip status enable
```

Release History

Release 6.1; command 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 6400, 6855, 6850E, 9000E

Usage Guidelines

This timer is reset each time a routing update is received.

Examples

```
-> ipv6 rip invalid-timer 300
```

Release History

Release 6.1; command 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 6400, 6855, 6850E, 9000E

Usage Guidelines

Use the **ipv6 rip invalid-timer** command to set the Invalid Timer Value.

Examples

```
-> ipv6 rip garbage-timer 180
```

Release History

Release 6.1; command 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 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 6400, 6855, 6850E, 9000E

Usage Guidelines

While in holddown, the route continues being announced as usual and used in RIB. This interval is used to control route flap dampening.

Examples

```
-> ipv6 rip holddown-timer 60
```

Release History

Release 6.1; command 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 (for example, if the updated interval is 30, the range would be 0 - 300).

Defaults

parameter	default
value	5

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

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.

Examples

```
-> ipv6 rip jitter 10
```

Release History

Release 6.1; command 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 6400, 6855, 6850E, 9000E

Usage Guidelines

This value does not apply to routes learned from other routers. For these routes, the route tag propagates with the route.

Examples

```
-> ipv6 rip route-tag 30
```

Release History

Release 6.1; command 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 6400, 6855, 6850E, 9000E

Usage Guidelines

Use this command, along with the **ipv6 rip jitter** command to configure RIPng updates.

Examples

```
-> ipv6 rip update-interval 30
```

Release History

Release 6.1; command 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 6400, 6855, 6850E, 9000E

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.

Examples

```
-> ipv6 rip triggered-sends none
```

Release History

Release 6.1; command introduced.

Related Commands

show ipv6 rip	Displays RIPng status and general configuration information.

MIB Objects

```
alaProtocolripng
   alaRipngTriggeredSends
```

ipv6 rip interface

Creates or 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 6400, 6855, 6850E, 9000E

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 4, "VLAN Management Commands".
- RIPng will support a maximum of 20 interfaces.

Examples

```
-> ipv6 rip interface Test_Lab
```

Release History

Release 6.1; command introduced.

Related Commands

ipv6 redist	Loads RIPng into memory.
ipv6 rip status	Enables or 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.

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 6400, 6855, 6850E, 9000E

Usage Guidelines

- When you configure a metric for a RIPng interface, this metric cost is added to the metric of the incoming route.
- 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.

Examples

```
-> ipv6 rip Test_Lab metric 1
```

Release History

Release 6.1; command introduced.

Related Commands

ipv6 rip interface	Creates or 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 6400, 6855, 6850E, 9000E

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.

Examples

```
-> ipv6 rip interface Test_Lab recv-status disable
```

Release History

Release 6.1; command introduced.

Related Commands

ipv6 redist	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 6400, 6855, 6850E, 9000E

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.

Examples

```
-> ipv6 rip interface Test_Lab send-status enable
```

Release History

Release 6.1; command introduced.

Related Commands

ipv6 redist	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 6400, 6855, 6850E, 9000E

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.

Examples

```
-> ipv6 rip interface Test_Lab none
```

Release History

Release 6.1; command 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
```

show ipv6 rip

Displays the RIPng status and general configuration parameters.

show ipv6 rip

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

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, and None).

Release History

Release 6.1; command introduced.

Related Commands

ipv6 rip status	Enables or 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, so 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 6400, 6855, 6850E, 9000E

Usage Guidelines

If you do not specify an interface, all IPv6 RIP interfaces are displayed.

Examples

```
-> 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 (continued)

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 6.1; command introduced.

Related Commands

ipv6 rip interface	IPv6 interface name.
ipv6 rip status	Enables or 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 (for example, 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 6400, 6855, 6850E, 9000E

Usage Guidelines

If you do not specify a peer, all IPv6 RIP peers are displayed.

Examples

```
-> 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 update 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 6.1; command 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 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 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 6400, 6855, 6850E, 9000E

Usage Guidelines

If you do not enter one of the optional parameters, all IPv6 RIP routes are displayed.

Examples

```
-> 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 6.1; command 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
```

21 IPsec Commands

IPsec is a suite of protocols for securing IPv6 communications by authenticating and/or encrypting each IPv6 packet in a data stream. IPsec provides security services such as encrypting traffic, integrity validation, authenticating the peers, and anti-replay.

IPsec protocols operate at network layer using appropriate security protocols, cryptographic algorithms, and cryptographic keys. The security services are provided through use of two security protocols, the Authentication Header (AH) and the Encapsulating Security Payload (ESP), and through the use of cryptographic key management procedures and protocols.

This implementation of IPsec supports the transport mode of operation. In this mode, only the data you transfer (payload) in the IPv6 packet is encrypted and/or authenticated and only the payloads that are originated and destined between two endpoints are processed with IPsec.

The pre-configured Security Policy determines the traffic that is to be rendered with IPsec protection. A Security Association (SA) specifies the actual IPsec actions to be performed (e.g encryption using 3DES, authentication with HMAC-SHA1). A security association is a bundle of algorithms and parameters (such as keys) that is being used to encrypt and authenticate a particular flow in one direction. Security Associations are manually configured.

A summary of the available commands is listed here:.

ipsec key
ipsec security-key
ipsec policy
ipsec policy rule
ipsec sa
show ipsec policy
show ipsec sa
show ipsec key
show ipsec ipv6 statistics

ipsec key

Configures the authentication and encryption keys for a manually configured IPsec SA.

ipsec key *key_name* **{sa-authentication | sa-encryption}** *key*

no ipsec key *key_name* **{sa-authentication | sa-encryption}**

Syntax Definitions

key_name	The name of this key (maximum 20 characters).
sa-authentication	Indicates that the key value is used by an authentication algorithm.
sa-encryption	Indicates that the key value is used by an encryption algorithm.
key	Specifies the key value. The key value can be either in the hexadecimal format or as a string.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove the authentication key or the encryption key from a manually configured IPsec SA.
- The *name* parameter should be the same as the name of the manually configured SA that will use this SA authentication or encryption key.
- The length of the key value must match the value that is required by the encryption or authentication algorithm that will use the key. The required key length for the supported algorithm are as follows:

algorithm	key length
des-cbc	64 bits
3des-cbc	192 bits
aes-cbc	128, 192, or 256 bits
aes-ctr	160, 224, or 288 bits
hmac-md5	128 bits
hmac-sha1	160 bits
aes-xcbc-mac	128 bits

- The combination of the key's name and type must be unique.
- The **encrypted** option will be used when the key commands are written to the **boot.cfg** or other snapshot file. This option should not be specified when entering this command through the switch CLI.

Examples

```
-> ipsec key sa1_ah sa-authentication 0x1122334455667788990011223344556 6
-> ipsec key sa1_esp sa-encryption "Quoth, Nevermore"
```

Release History

Release 6.3.4; command was introduced.

Related Commands

ipsec sa	Configures an IPsec Security Association (SA).
show ipsec key	Displays the keys for the manually configured IPsec SA.

MIB Objects

```
AlaIPsecKeyTable
   alaIPsecKeyName
   alaIPsecKeyType
   alaIPsecKeyEncrypted
   alaIPsecKey
```

ipsec security-key

Sets the master security key for the switch. The master security key is used to encrypt and decrypt the configured SA keys that are saved to permanent storage (e.g., **boot.cfg** file).

ipsec security-key [*old_key***]** *new_key*

Syntax Definitions

old_key	The current master security key. The key can be specified either in the hexadecimal format (16 bytes in length) or as a string (16 characters in length).
new_key	The new key value. The key can be specified either in the hexadecimal format (16 bytes in length) or as a string (16 characters in length).

Defaults

By default, no master security key is set for the switch.

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- The *old_key* parameter should always be specified when you modify an existing key. Setting the key for first time does not require the *old_key*.
- If the value of the *old_key* is incorrect, the attempt to set a new key will fail.
- When there is no master security key configured for the switch, the SA key values are written unencrypted to permanent storage (**boot.cfg** or other configuration file). A warning message is logged when this occurs.
- If the master security key is reset using **debug clear ipsec security-key** command, the currently configured SA keys will be deleted.
- When the master security key is set or changed, its value is immediately propagated to the secondary CMM. In a stacked configuration, the master security key is saved to all modules in case a stack split occurs or there is a simultaneous failure of both CMM modules. When the master security key is changed, save and synchronize the current configuration to ensure the proper operation of IPsec in the event of a switch reboot or takeover.

Examples

```
-> ipsec security-key alcatel_corp_001 alcatel_lucent01
```

Release History

Release 6.3.4; command was introduced.

Related Commands

ipsec key	Adds, modifies or deletes the authentication and encryption keys for a manually configured IPsec SA.

MIB Objects

```
AlaIPsecSecurityKeyTable
   alaIPsecSecurityKeyCurrent
   alaIPsecSecurityKeyNew
```

ipsec policy

Configures a security policy.

ipsec policy *policy_name* **[priority** *priority***] [source {***ipv6_address* **[***/prefix_length***]} [port** *port***]] [destination {***ipv6_address* **[***/prefix_length***]}[port** *port]***] [protocol** *protocol***}] [in | out] [discard | ipsec | none] [description** *description***] [no shutdown | shutdown]**

no ipsec policy *policy_name*

Syntax Definitions

policy_name	The name for the policy
priority	The priority for the policy. Values range from 1 to 1000. The higher the value, the higher the priority.
ipv6_address	The IPv6 address to which the policy applies.
prefix_length	An IPv6 address prefix used to identify a range of addresses to which the policy applies.
port	The upper-layer protocol port number to which the policy applies.
protocol	Specifies the upper-layer protocol to which the policy applies (refer to the table in the “Usage Guidelines“section below for various protocol options).
in	Specifies that the policy is applied to the inbound IPv6 traffic.
out	Specifies that the policy is applied to the outbound IPv6 traffic.
discard	Specifies that traffic to which this policy applies is discarded.
ipsec	Specifies that IPsec processing is required on traffic to which this policy applies.
none	Specifies that no IPsec processing is done on traffic to which this policy applies**.**
description	The detailed description of the policy.
no shutdown	Administratively enables the policy.
shutdown	Administratively disables the policy.

Defaults

parameter	default
priority	100
port	any port
any | **icmp6** | **tcp** | **udp** | **ospf** | **vrrp** | **number**	**any**
discard | **ipsec** | **none**	**ipsec**
no shutdown | **shutdown**	**no shutdown**

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove an IPsec policy rule from the switch configuration.
- If traffic matches more than one policy, the policy with the highest priority is applied. If two policies have the same priority, the one configured first has precedence.
- The following table lists the various **protocol** options for this command:

protocol
any
icmp6[type *type***]**
tcp
udp
ospf
vrrp
number *protocol*

  The **any** option should be used to apply the policy to all protocol traffic. Otherwise, an upper-layer protocol (or protocol number) may be specified to restrict the policy to the specified protocol traffic. The optional *type* parameter of **icmp6** can also be specified to restrict the policy for certain type of ICMPv6 packets.
- If the **ipsec** option is specified, then the IPv6 packets that matches the criteria will be processed by the the IPsec as defined with the **ipsec policy rule** command and this policy may not be enabled until at least one rule has been defined.

Examples

```
-> ipsec policy tcp_in source ::/0 destination 3ffe:200:200:4001::99 protocol tcp
in ipsec description "IPsec on all inbound TCP" no shutdown
-> no ipsec policy tcp_in
```

Release History

Release 6.3.4; command was introduced.

Related Commands

ipsec policy rule	Adds, modifies, or removes an IPsec rule for a security policy.
show ipsec policy	Displays information about the security policies.

MIB Objects

```
AlaIPsecSecurityPolicyTable
   alaIPsecSecurityPolicyName
   alaIPsecSecurityPolicyPriority
   alaIPsecSecurityPolicySource
   alaIPsecSecurityPolicySourceType
   alaIPsecSecurityPolicySourcePrefixLength
   alaIPsecSecurityPolicySourcePort
   alaIPsecSecurityPolicyDestination
   alaIPsecSecurityPolicyDestinationType
   alaIPsecSecurityPolicyDestinationPrefixLength
   alaIPsecSecurityPolicyDestinationPort
   alaIPsecSecurityPolicyULProtocol
   alaIPsecSecurityPolicyICMPv6Type
   alaIPsecSecurityPolicyDirection
   alaIPsecSecurityPolicyAction
   alaIPsecSecurityPolicyDescription
   alaIPsecSecurityPolicyAdminState
```

ipsec policy rule

Configures an IPsec rule for an IPsec security policy.

ipsec policy *policy_name* **rule** *index* **[ah | esp]**

no ipsec policy *policy_name* **rule** *index*

Syntax Definitions

policy_name	The name of an existing IPsec security policy.
index	The index of this rule. Values range from 1 to 10.
ah	Specifies that the rule requires the presence of an Authentication Header (AH).
esp	Specifies that the rule requires the presence of an Encrypted Security Payload (ESP).

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- The IPsec security policy name specified with this command must already exist in the switch configuration. Use the **ipsec policy** command to create a new security policy.
- The index value configured for the IPsec policy rule determines the order in which a rule is applied to the original payload. For example, to first enclose the original contents of an IPv6 packet in an ESP and then authenticate the encrypted payload with an AH, configure the ESP rule with and index of one and the AH rule with an index of two.

Examples

```
-> ipsec policy tcp_in rule 1 esp
-> ipsec policy tcp_in rule 2 ah
-> no ipsec policy tcp_in rule 2
```

Release History

Release 6.3.4; command was introduced.

Related Commands

ipsec policy	Configures an IPsec security policy.
show ipsec policy	Displays the IPsec security policy configuration for the switch.

MIB Objects

```
AlaIPsecSecurityPolicyRuleTable
   alaIPsecSecurityPolicyName
   alaIPsecSecurityPolicyRuleIndex
   alaIPsecSecurityPolicyRuleProtocol
```

ipsec sa

Configures an IPsec Security Association (SA).

ipsec sa *sa_name* **{esp | ah} [source** *ipv6_address***] [destination** *ipv6_address***] [spi** *spi***] [encryption {null | des-cbc | 3des-cbc | aes-cbc [key-size** *key_length***] | aes-ctr [key-size** *key_length***]}] [authentication {none | hmac-md5 | hmac-sha1 | aes-xcbc-mac}] [description** *description***] [no shutdown | shutdown]**

no ipsec sa *name*

Syntax Definitions

sa_name	The name assigned to this IPsec SA.
esp	Specifies the type of security association as ESP.
ah	Specifies the type of security association as AH.
source *ipv6_address*	Specifies the source address of the IPv6 traffic that will be covered by the SA.
destination *ipv6_address*	Specifies the destination address of the IPv6 traffic that will be covered by the SA.
spi	The Security Parameters Index (SPI) for the SA.
encryption	Specifies the encryption algorithm to be used for traffic covered by the SA. This parameter is used only when the SA type is ESP.
key_length	Key length for the specified encryption algorithm.
authentication	Specifies the authentication algorithm to be used for traffic covered by the SA.
description	The detailed description of the SA.
no shutdown	Administratively enables the SA.
shutdown	Administratively disables the SA.

Defaults

parameter	Defaults
authentication {none | hmac-md5 | hmac-sha1 | aes-xcbc-mac}	**none (**ESP SAs only; no default value for AH SAs**)**
no shutdown | shutdown	**no shutdown**

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- When using **ESP** to verify integrity only, use the **null** option with the **encryption** parameter.
- If the **null** option is used with the **encryption** parameter, specify an integrity algorithm using the **authentication** parameter.
- To override the default key length for the **aes-cbc** or **aes-ctr** encryption algorithm, specify the key length value after the protocol name. The following key length values are supported:

encryption algorithm	key length (in bits)
aes-cbc	128(default), 192, and 256
aes-ctr	160(default), 224, and 288

- There are two ways to configure an ESP confidentiality-only SA: use the **none** option with the **authentication** parameter, or simply omit the **authentication** parameter from the command.
- For an integrity-only SA or an encryption and integrity SA, specify one of the authentication algorithms (**aes-xcbc-mac**, **hmac-md5** or **hmac-sha1).**
- For AH SAs, specify one of the authentication algorithms (**aes-xcbc-mac**, **hmac-md5** or **hmac-sha1).**
- Note that enabling an SA is not allowed if the required encryption and/or authentication keys have not been configured.

Examples

```
-> ipsec sa ah_in ah source 3ffe:200:200:4001::99 destination 3ffe:200:200:4001::1
spi 9901 authentication hmac-sha1 description "HMAC SHA1 on traffic from 99 to 1"
-> ipsec sa esp_out esp source 3ffe:200:200:4001::1 destination
3ffe:200:200:4001::1ae7 spi 12901 encryption aes-cbc authentication aes-xcbc-mac
description "ESP confidentiality and integrity on traffic from 1 to 1ae7"
-> no ipsec sa ah_in
```

Release History

Release 6.3.4; command was introduced.

Related Commands

ipsec key	Configures the authentication and encryption keys for a manually configured IPsec SA.
show ipsec sa	Displays information about manually configured IPsec Security Associations.

MIB Objects

AlaIPsecSAConfigTable

- alaIPsecSAConfigName
- alaIPsecSAConfigType
- alaIPsecSAConfigSource
- alaIPsecSAConfigSourceType
- alaIPsecSAConfigDestination
- alaIPsecSAConfigDestinationType
- alaIPsecSAConfigSPI
- alaIPsecSAConfigEncryptionAlgorithm
- alaIPsecSAConfigEncryptionKeyLength
- alaIPsecSAConfigAuthenticationAlgorithm
- alaIPsecSAConfigDescription
- alaIPsecSAConfigAdminState

show ipsec policy

Displays the IPsec security policy configuration for the switch.

show ipsec policy [*policy_name***]**

Syntax Definitions

policy_name	The name of an existing IPsec policy.

Defaults

By default, information is displayed for all security policies configured for the switch.

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

Use the *policy_name* parameter to display information about a specific security policy.

Examples

```
-> show ipsec policy
Name         Priority  Source-> Destination      Protocol Direction Action   State
-------------+--------+-------------------------+--------+---------+--------+------
ftp-in-drop  100     ::/0->fe80::1:1::1            TCP     in       discard  active
telnet-in-1  100     2000::/48->3ffe::200(23)      TCP     in       ipsec    active
telnet-out-1 100     3ffe::200(23)->2000::/48      TCP     out      ipsec    active
```

output definitions

Name	The name of the security policy.
Priority	The priority value assigned to the policy. If the same traffic is covered by multiple policies, the policy with the highest priority is applied.
Source -> Destination	Indicates the source and destination of traffic covered by this policy.
Protocol	Indicates the protocol traffic covered by this policy. The protocol name (TCP) or protocol number (80) will be displayed in this field.
Direction	Indicates whether the policy has been applied to the incoming or outgoing traffic.
Action	Indicates the action to be taken on the traffic covered by this policy.
State	Indicates the operational state of this policy.

```
-> show ipsec policy telnet-out-1
Name        = telnet-out-1
Priority    = 100
Source      = 3ffe::200(23)
Destination = 2000::/48
Protocol    = TCP
Direction   = out
Action      = ipsec
State       = active
Rules:
  1) esp
  2) ah
Description:
  Require AH and ESP headers on outgoing telnet traffic.
```

output definitions

Name	The name of the security policy.
Priority	The priority value assigned to the policy. If the same traffic is covered by multiple policies, the policy with the highest priority is applied.
Source	Indicates the source of the traffic covered by this policy.
Destination	Indicates the destination of the traffic covered by this policy.
Protocol	Indicates the protocol traffic covered by this policy. The protocol name (TCP) or protocol number (80) will be displayed in this field.
Direction	Indicates whether the policy has been applied to the incoming or outgoing traffic.
Action	Indicates the action to be taken on the traffic covered by this policy.
State	Indicates the operational state of this policy.
Rules	Indicates the rules specified for this policy.
Description	The description for this policy.

Release History

Release 6.3.4; command was introduced.

Related Commands

ipsec policy	Configures an IPsec security policy.

MIB Objects

```
AlaIPsecSecurityPolicyTable
   alaIPsecSecurityPolicyName
   alaIPsecSecurityPolicySource
   alaIPsecSecurityPolicySourceType
   alaIPsecSecurityPolicySourcePrefixLength
   alaIPsecSecurityPolicySourcePort
   alaIPsecSecurityPolicyDestination
   alaIPsecSecurityPolicyDestinationType
   alaIPsecSecurityPolicyDestinationPrefixLength
   alaIPsecSecurityPolicyDestinationPort
   alaIPsecSecurityPolicyProtocol
```

```
alaIPsecSecurityPolicyDirection
alaIPsecSecurityPolicyAction
alaIPsecSecurityPolicyOperationalState
alaIPsecSecurityPolicyRuleIndex
alaIPsecSecurityPolicyRuleProtocol
alaIPsecSecurityPolicyDescription
```

show ipsec sa

Displays information about manually configured IPsec Security Associations.

show ipsec sa [*sa_name* **| esp | ah]**

Syntax Definitions

sa_name	The name of the Security Association (SA).
esp	Restricts the display to ESP SAs.
ah	Restricts the display to AH SAs.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Use the *sa_name* parameter to display information about a specific SA.
- Use the **esp** or **ah** options to display information about a specific SA type.

Examples

```
-> show ipsec sa
Name           Type  Source-> Destination[SPI]      Encryption   Authentication State
---------------+----+--------------------------------+------------+------------+-----
telnet-in-esp  ESP  2000::/49->3ffe::200[8920]       aes-cbc(128) hmac-sha1 active
telnet-out-esp ESP  3ffe::200->2000::/48[100120]     aes-cbc(128) hmac-sha1 active
```

output definitions

Name	The SA name.
Type	The SA type (**AH** or **ESP**).
Source -> Destination [SPI]	The traffic source, destination, and SPI for this SA.
Encryption	The encryption algorithm used for this SA.
Authentication	The authentication algorithm used for this SA.
State	The operational state of this SA.

```
-> show ipsec sa telnet-in-esp

Name           = telnet-in-esp
Type           = ESP
Source         = 2000::/49
Destination    = 3ffe::200
SPI            = 8920
Encryption     = aes-cbc(128)
Authentication = hmac-sha1
State          = active
Description:
  Security association for traffic from 2000::/49 to
  3ffe::200.
```

output definitions

Name	The SA name.
Type	The SA type (**AH** or **ESP**).
Source	The traffic source for this SA.
Destination	The traffic destination for this SA.
SPI	The SPI for this SA.
Encryption	The encryption algorithm used for this SA.
Authentication	The authentication algorithm used for this SA.
State	The operational state of this SA.
Description	The description for this SA.

Release History

Release 6.3.4; command was introduced.

Related Commands

ipsec sa	Configures an IPsec Security Association (SA).

MIB Objects

```
AlaIPsecSAConfigTable
   alaIPsecSAConfigName
   alaIPsecSAConfigType
   alaIPsecSAConfigSource
   alaIPsecSAConfigSourceType
   alaIPsecSAConfigDestination
   alaIPsecSAConfigDestinationType
   alaIPsecSAConfigSPI
   alaIPsecSAConfigOperationalState
   alaIPsecSAConfigEncryptionAlgorithm
   alaIPsecSAConfigEncryptionKeyLength
   alaIPsecSAConfigAuthenticationAlgorithm
   alaIPsecSAConfigAuthenticationKeyLength
   alaIPsecSAConfigDescription
```

show ipsec key

Displays the encryption and authentication key values for the manually configured IPsec security association (SA).

show ipsec key {sa-encryption | sa-authentication}

Syntax Definitions

sa-encryption	Displays encryption SA key information.
sa-authentication	Displays authentication SA key information.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

The key values will not be displayed due to security reasons.

Examples

```
-> show ipsec key sa-encryption
Encryption Keys
Name                  Length (bits)
--------------------+-------------
sa_1                             192
sa_2                             160
sa_3                              64

-> show ipsec key sa-authentication

Authentication Keys
Name                  Length (bits)
--------------------+-------------
sa_1                             128
sa_5                             160
```

output definitions

Name	The name of the manually configured SA for which the key will be used. The keys may be created for SAs that do not exist.
Length	The length of the key, in bits.

Release History

Release 6.3.4; command was introduced.

Related Commands

ipsec key	Configures the authentication and encryption keys for a manually configured IPsec SA.

MIB Objects

```
AlaIPsecKeyTable
   alaIPsecKeyName
   alaIPsecKey
```

show ipsec ipv6 statistics

Displays IPsec statistics.

show ipsec ipv6 statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855 9000E

Usage Guidelines

N/A

Examples

```
Inbound:
  Successful                = 2787
  Discarded                 = 18
  Policy violation          = 0
  No SA found               = 0
  Unknown SPI               = 0
  AH replay check failed    = 0
  ESP replay check failed   = 0
  AH authentication success  = 93
  AH authentication failure  = 0
  ESP authentication success = 25
  ESP authentication failure = 0
  Packet not valid          = 0
  No memory available       = 0
Outbound:
  Successful                = 5135
  Discarded                 = 0
  Policy violation          = 0
  No SA found               = 19
  Packet not valid          = 0
  No memory available       = 0
```

output definitions

Successful (inbound)	The number of incoming packets requiring IPsec processing that were successfully handled.
Discarded (inbound)	The number of incoming packets discarded because they matched a discard policy.
Policy violation (inbound)	The number of incoming packets dropped due to policy violations.

output definitions

No SA found (inbound)	The number of incoming packets dropped because no matching SA was found.
Unknown SPI (inbound)	The number of incoming packets dropped because the SPI was unknown.
AH replay check failed (inbound)	The number of incoming packets that failed the AH replay check.
ESP replay check failed (inbound)	The number of incoming packets that failed the ESP replay check.
AH authentication success (inbound)	The number of incoming packets that successfully passed AH authentication.
AH authentication failure (inbound)	The number of incoming packets that failed AH authentication.
ESP authentication success (inbound)	The number of incoming packets that successfully passed ESP authentication.
ESP authentication failure (inbound)	The number of incoming packets that failed ESP authentication.
Packet not valid (inbound)	The number of incoming packets requiring IPsec processing that were not valid.
No memory available (inbound)	The number of incoming packets requiring IPsec processing that were dropped because memory was not available.
Successful (outbound)	The number of outgoing packets requiring IPsec processing that were successfully handled.
Discarded (outbound)	The number of outbound packets discarded because they matched a discard policy.
Policy violation (outbound)	The number of outgoing packets dropped due to policy violation.
No SA found (outbound)	The number of outgoing packets dropped because no matching SA was found.
Packet not valid (outbound)	The number of outgoing packets requiring IPsec processing that were not valid.
No memory available (outbound)	The number of outgoing IPsec packets dropped because memory was not available.

Release History

Release 6.3.4; command was introduced.

Related Commands

show ipsec policy	Displays the IPsec security policy configuration for the switch.
show ipsec sa	Displays information about manually configured IPsec Security Associations.
show ipsec key	Displays the encryption and authentication key values for the manually configured IPsec security association (SA).

MIB Objects

AlaIPsecStatisticsTable

- alaIPsecStatisticsInSuccessful
- alaIPsecStatisticsInPolicyViolation
- alaIPsecStatisticsInNoSA
- alaIPsecStatisticsInUnknownSPI
- alaIPsecStatisticsInAHReplay
- alaIPsecStatisticsInESPReplay
- alaIPsecStatisticsInAHAuthenticationSuccess
- alaIPsecStatisticsInAHAuthenticationFail
- alaIPsecStatisticsInESPAuthenticationSuccess
- alaIPsecStatisticsInESPAuthenticationFail
- alaIPsecStatisticsInBadPacket
- alaIPsecStatisticsInNoMemory
- alaIPsecStatisticsOutSuccessful
- alaIPsecStatisticsOutPolicyViolation
- alaIPsecStatisticsOutNoSA
- alaIPsecStatisticsOutBadPacket
- alaIPsecStatisticsOutNoMemory

22 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, and 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 interface auth-type
ip rip interface auth-key
ip rip update-interval
ip rip invalid-timer
ip rip garbage-timer
ip rip holddown-timer
show ip rip
show ip rip routes
show ip rip interface
show ip rip peer

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 6400, 6855, 6850E, 9000E

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 6.1; command was introduced.

Related Commands

ip rip status	Enables/disables RIP routing on the switch.
show ip rip	Displays the RIP status and general configuration parameters (e.g., forced hold-down timer).

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 6400, 6855, 6850E, 9000E

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 6.1; command was introduced.

Related Commands

ip load rip	Loads RIP into the switch memory.
show ip rip	Displays the RIP status and general configuration parameters (e.g., forced hold-down timer).

MIB Objects

```
alaProtocolRip
   alaRipProtoStatus
```

ip rip interface

Creates/deletes a RIP interface. Routing is enabled on a VLAN when you create a router interface. However, to enable RIP routing, you must also configure and enable a RIP routing interface on the VLAN's IP router interface.

ip rip interface *interface_name*

no ip rip interface *interface_name*

Syntax Definitions

interface_name	The name of the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

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 by using the **ip rip interface status** command.
- You can create a RIP interface even if an IP router interface has not been configured. However, RIP will not function unless an IP router interface is configured with the RIP interface.
- For more information on VLANs and router ports, see Chapter 4, "VLAN Management Commands".

Examples

```
-> ip rip interface rip-1
```

Release History

Release 6.1; command was introduced.

Related Commands

ip interface	Creates a VLAN router interface.
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 *interface_name* **status {enable | disable}**

Syntax Definitions

interface_name	The name of the interface.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- You must first create a RIP interface by using the **ip rip interface** command before enabling the interface.
- You can create a RIP interface even if an IP router interface has not been configured. However, RIP will not function unless an IP router interface is configured with the RIP interface.
- For more information on VLANs and router ports, see Chapter 4, “VLAN Management Commands”.

Examples

```
-> ip rip interface rip-1 status enable
```

Release History

Release 6.1; command was introduced.

Related Commands

ip interface	Creates a VLAN router interface.
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 *interface_name* **metric** *value*

Syntax Definitions

interface_name	The name of the interface.
value	Metric value. Valid range is 1–15.

Defaults

parameter	default
value	1

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

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 rip-1 metric 2
```

Release History

Release 6.1; 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 *interface_name* **send-version {none | v1 | v1compatible | v2}**

Syntax Definitions

interface_name	The name of the interface.
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 6400, 6855, 6850E, 9000E

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 rip-1 send-version v1
```

Release History

Release 6.1; 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 *interface_name* **recv-version {v1 | v2 | both | none}**

Syntax Definitions

interface_name	The name of the interface.
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 6400, 6855, 6850E, 9000E

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 rip-1 recv-version both
```

Release History

Release 6.1; 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 hold-down 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 than 120 seconds, the route enters a hold-down 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	The forced hold-down time interval, in seconds. The valid range is 0–120.

Defaults

parameter	default
seconds	0

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- The forced hold-down timer is not the same as the RIP hold-down timer. The forced hold-down timer defines a separate interval that overlaps the hold-down state. During the forced hold-down timer interval, the switch will not accept *better* routes from other gateways.
- The forced hold-down time interval can become a subset of the hold-down 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 hold-down timer set to the default value of 0.

Examples

```
-> ip rip force-holddowntimer 10
```

Release History

Release 6.1; command was introduced.

Related Commands

show ip rip	Displays the RIP status and general configuration parameters (e.g., forced hold-down 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 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this 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 bit 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 6.1; 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 6400, 6855, 6850E, 9000E

Usage Guidelines

Only RIPv2 supports route tags.

Examples

```
-> ip rip route-tag 0
```

Release History

Release 6.1; command was introduced.

Related Commands

show ip rip	Displays the RIP status and general configuration parameters (e.g., forced hold-down timer).

MIB Objects

```
alaRipRedistRouteTag
```

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 *interface_name* **auth-type {none | simple | md5}**

Syntax Definitions

interface_name	The name of the interface.
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 6400, 6855, 6850E, 9000E

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 rip-1 auth-type none
```

Release History

Release 6.1; 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 *interface_name* **auth-key** *string*

Syntax Definitions

interface_name	The name of the interface.
string	16-byte text string.

Defaults

The default authentication string is a null string.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

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 rip-1 auth-key nms
```

Release History

Release 6.1; 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 update-interval

Configures the time interval during which RIP routing updates are sent out.

ip rip update-interval *seconds*

Syntax Definitions

seconds	The RIP routing update interval, in seconds. The valid range is 1–120.

Defaults

parameter	default
seconds	30

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

The update interval value must be less than or equal to one-third the invalid interval value.

Examples

```
-> ip rip update-interval 45
```

Release History

Release 6.1.5; command was introduced.

Related Commands

show ip rip	Displays the RIP status and general configuration parameters (e.g., forced hold-down timer).

MIB Objects

```
alaProtocolRip
   alaRipUpdateInterval
```

ip rip invalid-timer

Configures the RIP invalid timer value that defines the time interval during which a route will remain active in Routing Information Base (RIB) before moving to the invalid state.

ip rip invalid-timer *seconds*

Syntax Definition

seconds	The RIP invalid timer value, in seconds. The valid range is 3–360.

Defaults

parameter	default
seconds	180

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

The invalid time interval value must be three times the update interval value.

Examples

```
-> ip rip invalid-timer 270
```

Release History

Release 6.1.5; command was introduced.

Related Commands

show ip rip	Displays the RIP status and general configuration parameters (e.g., forced hold-down timer).

MIB Objects

```
alaProtocolRip
   alaRipInvalidTimer
```

ip rip garbage-timer

Configures the RIP garbage timer value that defines the time interval, which must elapse before an expired route is removed from the RIB.

ip rip garbage-timer *seconds*

Syntax Definition

seconds	The RIP garbage timer value, in seconds. The valid range is 0–180.

Defaults

parameter	default
seconds	120

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

During the RIP garbage interval, the router advertises the route with a metric of INFINITY (i.e., 16 hops).

Examples

```
-> ip rip garbage-timer 180
```

Release History

Release 6.1.5; command was introduced.

Related Commands

show ip rip	Displays the RIP status and general configuration parameters (e.g., forced hold-down timer).

MIB Objects

```
alaProtocolRip
   alaRipGarbageTimer
```

ip rip holddown-timer

Configures the RIP hold-down timer value that defines the time interval during which a route remains in the hold-down state.

ip rip holddown-timer *seconds*

Syntax Definition

seconds	The hold-down time interval, in seconds. The valid range is 0–120.

Defaults

parameter	default
seconds	0

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

When RIP detects a route with higher metric than the route in the RIB, the route with the higher metric goes into the hold-down state. The route updates with a metric of INFINITY are rejected.

Examples

```
-> ip rip holddown-timer 10
```

Release History

Release 6.1.5; command was introduced.

Related Commands

show ip rip	Displays the RIP status and general configuration parameters (e.g., forced hold-down timer).

MIB Objects

```
alaProtocolRip
   alaRipHolddownTimer
```

show ip rip

Displays the RIP status and general configuration parameters (e.g., forced hold-down timer).

show ip rip

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show ip rip

Status                    = Enabled
Number of routes          = 9
Host Route Support        = Enabled
Route Tag                 = 42
Update interval           = 30
Invalid interval          = 180
Garbage interval          = 120
Holddown interval         = 0
Forced Hold-Down Timer    = 0
```

output definitions

Status	RIP status (**Enabled** or **Disabled**).
Number of routes	Number of network routes in the RIP routing table.
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.
Route Tag	Route tag value for RIP routes generated by the switch. Valid values are 0–2147483647.
Update interval	The RIP routing update interval, in seconds. Valid range is 1–120. Default is 30.
Invalid interval	The RIP invalid timer value, in seconds. Valid range is 3–360. Default is 180.
Garbage interval	The RIP garbage timer value, in seconds. Valid range is 0–180. Default is 120.

output definitions

Holddown interval	The hold-down time interval, in seconds. Valid range is 0–120. Default is 0.
Forced Hold-Down Timer	The forced hold-down time interval, in seconds. The valid range is 0–120. Default is 0.

Release History

Release 6.1; command was introduced.
Release 6.1.5; new fields added.

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 the forced hold-down state.
ip rip update-interval	Configures the time interval during which RIP routing updates are sent out.
ip rip invalid-timer	Configures the RIP invalid timer value that defines the time interval during which a route will remain active in Routing Information Base (RIB) before moving to the invalid state.
ip rip garbage-timer	Configures the RIP garbage timer value that defines the time interval, which must elapse before an expired route is removed from the RIB.
ip rip holddown-timer	Configures the RIP hold-down timer value that defines the time interval during which a route remains in the hold down state.

MIB Objects

```
alaProtocolRip
   alaRipProtoStatus
   alaRipRouteNumber
   alaRipHostRouteSupport
   alaRipRedistRouteTag
   alaRipUpdateInterval
   alaRipInvalidTimer
   alaRipGarbageTimer
   alaRipHolddownTimer
   alaRipForceHolddownTimer
```

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 6400, 6855, 6850E, 9000E

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

Legends: State: A = Active, H = Holddown, G = Garbage
Destination        Gateway          State Metric Proto
-----------------+----------------+----+------+------
2.0.0.0/8          +5.0.0.14          A    2      Rip
                    4.0.0.7           A    3      Rip
4.0.0.0/8          +5.0.0.14          A    3      Rip
                    2.0.0.14          A    3      Rip
5.0.0.0/8          +2.0.0.14          A    2      Rip
                    4.0.0.7           A    3      Rip
10.0.0.0/8         +4.0.0.7           A    2      Rip
                    5.0.0.14          A    2      Rip
                    2.0.0.14          A    2      Rip
22.0.0.0/8         +5.0.0.14          A    2      Rip
                    2.0.0.14          A    2      Rip
                    4.0.0.7           A    3      Rip
128.251.40.0/24    +4.0.0.7           A    2      Rip
                    5.0.0.14          A    3      Rip
                    2.0.0.14          A    3      Rip
150.0.0.0/24       +4.0.0.7           A    2      Rip
                    5.0.0.14          A    2      Rip
                    2.0.0.14          A    2      Rip
152.0.0.0/24       +4.0.0.7           A    2      Rip
                    5.0.0.14          A    3      Rip
```

output definitions

Destination	Destination network IP address.
Gateway	The Gateway IP address (switch from which the destination address was learned).
State	The associated state of the route, which can be **A** (**Active**), **H** (**Holddown**), or **G** (**Garbage**).
Metric	Metric associated with this network. Generally, this is the RIP hop count (the number of hops from this switch to the destination switch).
Proto	The type of route (**Local**, **Rip**, or **Redist**).

```
-> show ip rip routes 2.0.0.0 255.0.0.0

Destination             = 2.0.0.0,
Mask length             = 8,
Gateway(1)              = 5.0.0.14,
  Protocol              = Rip,
  Out Interface         = intf5,
  Metric                = 2,
  Status                = Installed,
  State                 = Active,
  Age                   = 19s,
  Tag                   = 0,
Gateway(2)              = 4.0.0.7,
  Protocol              = Rip,
  Out Interface         = intf4,
  Metric                = 3,
  Status                = Not Installed,
  State                 = Active,
  Age                   = 12s,
  Tag                   = 0,
```

output definitions

Destination	Destination network IP address.
Mask length	Length of the destination network IP subnet mask.
Gateway	The Gateway IP address (switch from which the destination address was learned).
Protocol	The type of the route (**Local**, **Rip**, or **Redist**).
Out Interface	The RIP interface through which the next hop is reached.
Metric	Metric associated with this network. Generally, this is the RIP hop count (the number of hops from this switch to the destination switch).
Status	The RIP interface status (Installed or Not Installed).
State	The associated state of the route (**Active**, **Holddown**, or **Garbage**).
Age	The age of the route in seconds (the number of seconds since this route was last updated or otherwise determined to be correct).
Tag	The associated route tag.

Release History

Release 6.1; command was introduced.
Release 6.1.5; new fields added.

Related Commands

ip rip host-route	Enables/disables a host route to an individual host on a network.

MIB Objects

```
alaRipEcmpRouteTable
   alaRipEcmpRouteDest
   alaRipEcmpRouteMask
   alaRipEcmpRouteNextHop
   alaRipEcmpRouteType
   alaRipEcmpMetric
   alaRipEcmpStatus
   alaRipEcmpAge
   alaRipEcmpTag
   alaRipEcmpRouteState
   alaRipEcmpRouteStatus
```

show ip rip interface

Displays RIP interface status and configuration.

show ip rip interface [*interface_name***]**

Syntax Definitions

interface_name	The interface name.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

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 rip-1

Interface IP Name                       = rip-1,
Interface IP Address                    = 11.11.11.1
IP Interface Number (VLANId)            = 4,
Interface Admin status                  = enabled,
IP Interface Status                     = enabled,
Interface Config AuthType               = None,
Interface Config AuthKey Length         = 0,
Interface Config Send-Version           = v2,
Interface Config Receive-Version        = both,
Interface Config Default Metric         = 1,
Received Packets                        = 154,
Received Bad Packets                    = 0,
Received Bad Routes                     = 0,
Sent Updates                            = 8
```

output definitions

Interface IP Name	The IP Interface name.
Interface IP Address	Interface IP address.
IP Interface Number	Interface VLAN ID number.
Interface Admin Status	The RIP administrative status (enabled/disabled).
IP Interface Status	Interface status (enabled /disabled).
Interface Config AuthType	The type of authentication that will be used for the RIP interface (None or Simple).

output definitions (continued)

Interface Config AuthKey Length	The authentication key length used for the RIP interface.
Interface Config Send-Version	Interface send option (none, v1, v2, and v1 compatible). Default is v2.
Interface Config Receive-Version	Interface receive option (none, v1, v2, and both). Default is both.
Interface Config Default Metric	Default redistribution metric. Default is 1.
Received Packets	Number of packets received on the interface.
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 6.1; command was introduced.

Related Commands

ip rip interface	Enables/disables RIP for a specific interface.

MIB Objects

```
alaProtocolRip
   alaRipProtoStatus
alaRip2IfConfAugTable
   alaRip2IfConfName
   alaRip2IfRecvPkts
   alaRip2IfIpConfStatus
rip2IfConfTable
   rip2IfConfAddress
   rip2IfConfAuthType
   rip2IfConfAuthKey
   rip2IfConfSend
   rip2IfConfReceive
   rip2IfConfDefaultMetric
rip2IfStatTable
   rip2IfStatRcvBadPackets
   rip2IfStatRcvBadRoutes
   rip2IfStatSentUpdates
```

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 6400, 6855, 6850E, 9000E

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 6.1; command was introduced.

Related Commands

show ip rip interface	Displays the RIP interface status and configuration.

MIB Objects

```
rip2PeerTable
   rip2PeerAddress
   rip2PeerDomain
   rip2PeerLastUpdate
   rip2PeerVersion
   rip2PeerRcvBadPackets
   rip2PeerRcvBadRoutes
```

23 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 6400, 6855, 6850E, 9000E

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.

Examples

```
-> ip router-discovery enable
-> ip router-discovery disable
```

Release History

Release 6.1; 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* **[enable | disable]**

no router-discovery interface *name*

Syntax Definitions

name	The IP interface name that was defined at the time the IP interface was configured.
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 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to remove the RDP interface from the switch configuration.
- 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.
- The RDP interface is not active unless RDP is also enabled for the switch.

Examples

```
-> 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 6.1; command was introduced.

Related Commands

ip router-discovery	Enables or disables RDP for the switch.
ip interface	Configures an IP router interface.

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* **advertisement-address {all-systems-multicast | broadcast}**

Syntax Definitions

name	The IP interface name that was defined at the time the IP interface was configured.
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 6400, 6855, 6850E, 9000E

Usage Guidelines

- The RDP interface advertisement address is not active unless RDP is enabled on 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

```
-> ip router-discovery interface Marketing advertisement-address all-systems-multi-
cast
-> ip router-discovery interface Accounting advertisement-address broadcast
```

Release History

Release 6.1; command was introduced.

Related Commands

ip router-discovery	Enables or disables RDP on 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* **max-advertisement-interval** *seconds*

Syntax Definitions

name	The IP interface name that was defined at the time the IP interface was configured.
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 6400, 6855, 6850E, 9000E

Usage Guidelines

- The RDP interface maximum advertisement time is not active unless RDP is enabled on 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

```
-> ip router-discovery interface Marketing max-advertisement-interval 350
-> ip router-discovery interface Accounting max-advertisement-interval 20
```

Release History

Release 6.1; command was introduced.

Related Commands

ip router-discovery	Enables or disables RDP on 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* **min-advertisement-interval** *seconds*

Syntax Definitions

name	The IP interface name that was defined at the time the IP interface was configured.
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 6400, 6855, 6850E, 9000E

Usage Guidelines

- The RDP interface minimum advertisement time is not active unless RDP is enabled on 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

```
-> ip router-discovery interface Marketing min-advertisement-interval 20
-> ip router-discovery interface Accounting min-advertisement-interval 3
```

Release History

Release 6.1; command was introduced.

Related Commands

ip router-discovery	Enables or disables RDP on 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* **advertisement-lifetime** *seconds*

Syntax Definitions

name	The IP interface name that was defined at the time the IP interface was configured.
seconds	The length of time, in seconds, that advertised IP addresses are considered valid by the receiving host.

Defaults

parameter	default
seconds	3 * maximum advertisement interval

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- The RDP interface advertisement lifetime value is not active unless RDP is enabled on 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

```
-> ip router-discovery interface Marketing advertisement-lifetime 2000
-> ip router-discovery interface Accounting advertisement-lifetime 750
```

Release History

Release 6.1; command was introduced.

Related Commands

ip router-discovery	Enables or disables RDP on 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* **preference-level** *level*

Syntax Definitions

name	The IP interface name that was defined at the time the IP interface was configured.
level	Any positive, integer value.The higher the value, the higher the precedence.

Defaults

parameter	default
level	0

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- The RDP interface preference level value is not active unless RDP is enabled on 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

```
-> ip router-discovery interface Marketing preference-level 10
-> ip router-discovery interface Accounting preference-level 50
```

Release History

Release 6.1; command was introduced.

Related Commands

ip router-discovery	Enables or disables RDP on 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 6400, 6855, 6850E, 9000E

Usage Guidelines

- Each time RDP is enabled on 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 6.1; 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***]**

Syntax Definitions

name	The IP interface name that was defined at the time the IP interface was configured.

Defaults

By default, the information for all RDP interfaces is displayed with this command.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- When an optional IP interface name 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

```
-> 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**).
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 26, "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.
#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 6.1; command was introduced.

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
```

24 BFD Commands

Bidirectional Forwarding Detection (BFD) is a hello protocol, which can be configured to interact with routing protocols for the detection of path failures and can reduce the convergence time in a network. BFD is supported with the BGP, OSPF, VRRP, and Static Routes.

When BFD is configured and enabled, BFD sessions are created and timers are negotiated between BFD neighbors. If a system does not receive a BFD control packet within the negotiated time interval, the neighbor system is considered down. Rapid failure detection notices are then sent to the routing protocol, which initiates a routing protocol recalculation. This process can reduce the time of convergence in a network.

BFD can be operated in three different modes: Asynchronous mode, Demand mode or Echo mode.

In Asynchronous mode, the systems continuously send BFD control packets between each other as part of a BFD session. If there are no packets received for a minimum time interval negotiated between the systems, then the neighbor system is considered down.

In Demand mode, a poll sequence is initiated for which there is an exchange of BFD control packets. If the demand mode is active and no control packets are received in response to the poll sequence, the session is declared down.

In Echo mode, a stream of BFD echo packets are transmitted in a forwarding path for which the neighboring system would loop the packets and send them back. If the number of packets transmitted is not echoed back, then the system is declared down. Echo mode can be operated along with Asynchronous mode and Demand mode.

MIB information for the BFD commands is as follows:

Filename: ALCATEL-IND1-BFD-MIB
Module: ALCATEL-IND-BFD-MIB

A summary of the available commands is listed here:

Global BFD commands	**ip bfd-std status** **ip bfd-std transmit** **ip bfd-std receive** **ip bfd-std mode** **ip bfd-std echo interval** **ip bfd-std l2-hold-timer** **show ip bfd-std** **show ip bfd-std sessions** **show ip bfd-std session**
BFD Interface commands	**ip bfd-std interface** **ip bfd-std interface status** **ip bfd-std interface transmit** **ip bfd-std interface receive** **ip bfd-std interface multiplier** **ip bfd-std interface mode** **ip bfd-std interface echo-interval** **ip bfd-std interface l2-hold-timer** **show ip bfd-std interfaces**
Commands to configure BFD supported protocols	**ip ospf bfd-std status** **ip ospf bfd-std all-interfaces** **ip ospf interface bfd-std** **ip ospf interface bfd-std drs-only** **ip ospf interface bfd-std all-nbrs** **ip bgp bfd-std status** **ip bgp bfd-std all-neighbors** **ip bgp neighbors bfd-std** **vrrp bfd-std** **vrrp track address bfd-std** **ip static-route all bfd-std** **ip static-routes bfd-std status**

ip bfd-std status

Enables or disables the global BFD protocol status for the switch.

ip bfd-std status {enable | disable}

Syntax Definitions

enable	Enables BFD.
disable	Disables BFD.

Defaults

By default, BFD is disabled for the switch.

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Disabling BFD does not remove the existing BFD configuration from the switch.
- When BFD is disabled, all BFD functionality is disabled for the switch, but configuring BFD is still allowed.
- Configuring BFD global parameters is not allowed when BFD is enabled for the switch.

Examples

```
-> ip bfd-std status enable
-> ip bfd-std status disable
```

Release History

Release 6.3.4; command was introduced.

Related Commands

show ip bfd-std	Displays the BFD global status and general configuration parameters.

MIB Objects

```
alaBfdGlobalAdminStatus
```

ip bfd-std transmit

Configures the global transmit time interval for BFD control packets. This command specifies the minimum amount of time BFD waits between each transmission of control packets.

ip bfd-std transmit *transmit-interval*

Syntax Definitions

transmit-interval	The transmit time interval, in milliseconds. The valid range is 100–999.

Defaults

parameter	default
transmit-interval	100 milliseconds

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- The transmit time interval is also configurable at the BFD interface level. Note that configuring the global value with the **ip bfd-std transmit** command does not override the value set for the interface using the **ip bfd-std interface transmit** command.
- The global transmit time interval serves as the default interval value for a BFD interface. The default interval value is overridden when a specific value is configured for the interface.

Examples

```
-> ip bfd-std transmit 500
```

Release History

Release 6.3.4; command was introduced.

Related Commands

ip bfd-std interface transmit	Configures the transmit time interval for a specific BFD interface.
show ip bfd-std	Displays the BFD global status and general configuration parameters.

MIB Objects

```
alaBfdGlobalTxInterval
```

ip bfd-std receive

Configures the global receive time interval for BFD control packets. This command specifies the minimum amount of time BFD waits to receive control packets before determining there is a problem.

ip bfd-std receive *receive-interval*

Syntax Definitions

receive-interval	The receive time interval, in milliseconds. The valid range is 100–999.

Defaults

parameter	default
receive-interval	100 milliseconds

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- The minimum receive time interval is also configurable at the BFD interface level. Note that configuring the global value with the **ip bfd-std receive** command does not override the value set for the interface using the **ip bfd-std interface receive** command.
- The global receive time interval serves as the default interval value for a BFD interface. The default interval value is overridden when a specific value is configured for the interface.

Examples

```
-> ip bfd-std receive 500
```

Release History

Release 6.3.4; command was introduced.

Related Commands

ip bfd-std interface receive	Configures the receive time interval for a specific BFD interface.
show ip bfd-std	Displays the BFD global status and general configuration parameters.

MIB Objects

```
alaBfdGlobalRxInterval
```

ip bfd-std mode

Configures the global operational mode and echo status for the BFD protocol.

ip bfd-std mode {echo-only | demand echo {enable | disable} | asynchronous echo {enable|disable}}

Syntax Definitions

echo-only	Specifies echo only mode.
demand echo enable	Specifies demand mode with the echo function enabled.
demand echo disable	Specifies demand mode with the echo function disabled.
asynchronous echo enable	Specifies asynchronous mode with the echo function enabled.
asynchronous echo disable	Specifies asynchronous mode with the echo function disabled.

Defaults

By default, BFD is set to globally operate in demand mode with the echo function enabled.

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- The global operational mode and echo status is also configurable at the BFD interface level. Note that configuring the global value with the **ip bfd-std mode** command does not override the value set for the interface using the **ip bfd-std interface mode** command.
- The global operational mode and echo status serves as the default mode and status for a BFD interface. The default mode and status is overridden when a specific value is configured for the interface.

Examples

```
-> ip bfd-std mode echo-only
-> ip bfd-std mode demand echo enable
```

Release History

Release 6.3.4; command was introduced.

Related Commands

ip bfd-std interface mode	Configures the operational mode and echo status for a BFD interface.
show ip bfd-std	Displays the BFD global status and general configuration parameters.

MIB Objects

```
alaBfdGlobalOperMode
alaBfdGlobalEchoStatus
```

ip bfd-std echo interval

Configures the global BFD echo packet time interval. The echo function is available with the asynchronous or demand mode. Echo packets are transmitted to BFD peers to see if they loop back to the peer from which they originated.

ip bfd-std echo interval *echo-interval*

Syntax Definitions

echo-interval	The echo time interval, in milliseconds. The valid range is 100–999.

Defaults

parameter	default
echo-interval	100 milliseconds

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- The echo packet time interval is also configurable at the BFD interface level. Note that configuring the global value with the **ip bfd-std echo interval** command does not override the value set for the interface using the **ip bfd-std interface echo interval** command.
- The global echo packet time interval serves as the default interval value for a BFD interface. The default interval value is overridden when a specific value is configured for the interface.

Examples

```
-> ip bfd-std echo interval 500
```

Release History

Release 6.3.4; command was introduced.

Related Commands

ip bfd-std interface echo-interval	Configures the echo packet time interval for a BFD interface.
show ip bfd-std	Displays the BFD global status and general configuration parameters.

MIB Objects

```
alaBfdGlobalEchoRxInterval
```

ip bfd-std l2-hold-timer

Configures the global Layer 2 hold-down (convergence) timer value for the BFD protocol. This command specifies the amount of time BFD remains in a hold-down state after a Layer 2 topology change occurs.

ip bfd-std 12-hold-timer *l2-holdtimer-interval*

Syntax Definitions

l2-holdtimer-interval	The Layer 2 hold-down time interval, in milliseconds. The valid range is 100–999.

Defaults

parameter	default
l2-holdtimer-interval	100 milliseconds

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- The global Layer 2 hold-down timer is also configurable at the BFD interface level. Note that configuring the global value with the **ip bfd-std l2-hold-timer** command does not override the value set for the interface using the **ip bfd-std interface l2-hold-timer** command.
- The global Layer 2 hold-down timer serves as the default value for a BFD interface. The default timer value is overridden when a specific value is configured for the interface.

Examples

```
-> ip bfd-std l2-holdtimer 500
```

Release History

Release 6.3.4; command was introduced.

Related Commands

ip bfd-std interface l2-hold-timer	Configures the Layer 2 hold-down timer value for a BFD interface.
show ip bfd-std	Displays the BFD global status and general configuration parameters.

MIB Objects

```
alaBfdGlobalL2HoldTimer
```

ip bfd-std interface

Configures a BFD interface.

ip bfd-std interface *interface_name*

no ip bfd-std interface *interface_name*

Syntax Definitions

interface_name	The name of an existing IP interface.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete a BFD interface.
- The interface name must be an existing IP interface name that is configured with an IP address.

Examples

```
-> ip bfd-std interface bfd-vlan-101
-> no ip bfd-std interface bfd-vlan-101
```

Release History

Release 6.3.4; command was introduced.

Related Commands

ip bfd-std interface status	Configures the administrative status of a BFD interface.
show ip bfd-std interfaces	Displays the status and statistics of a BFD interface.
show ip bfd-std sessions	Displays the status and statistics of the BFD sessions.

MIB Objects

```
alaBfdIntfTable
   alaBfdIntfAddrType
   alaBfdIntfAddr
   alaBfdIntfIndex
```

ip bfd-std interface status

Enables or disables the administrative status of a BFD interface.

ip bfd-std interface *interface_name* **status {enable | disable}**

Syntax Definitions

interface_name	The name of an existing BFD interface.
enable	Enables the BFD interface.
disable	Disables the BFD interface.

Defaults

By default, a BFD interface is disabled when it is created.

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

The BFD interface must be enabled to participate in the BFD protocol.

Examples

```
-> ip bfd-std interface bfd-vlan-101 status enable
-> ip bfd-std interface bfd-vlan-101 status disable
```

Release History

Release 6.3.4; command was introduced.

Related Commands

ip bfd-std interface	Creates a BFD interface.
show ip bfd-std interfaces	Displays the status and statistics of a BFD interface.
show ip bfd-std sessions	Displays the status and statistics of BFD sessions.

MIB Objects

```
alaBfdIntfTable
   alaBfdIntfAdminStatus
```

ip bfd-std interface transmit

Configures the transmit time interval for the BFD interface. This command specifies the minimum amount of time BFD waits between each transmission of control packets from the interface.

ip bfd-std interface *interface_name* **transmit** *transmit-interval*

Syntax Definitions

interface_name	The name of an existing BFD interface.
transmit-interval	The transmit time interval, in milliseconds. The valid range is 100–999.

Defaults

The global transmit time interval value is used by default.

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- The global transmit time interval serves as the default interval value for a BFD interface. The default interval value is overridden when a specific value is configured for the interface.
- Note that configuring the interface transmit time interval using the **ip bfd-std interface transmit** command does not change the global value configured with the **ip bfd-std transmit** command.

Examples

```
-> ip bfd-std interface bfd-vlan-101 transmit 500
```

Release History

Release 6.3.4; command was introduced.

Related Commands

ip bfd-std interface	Creates a BFD interface.
ip bfd-std transmit	Configures a global BFD transmit time interval.
show ip bfd-std interfaces	Displays the status and statistics of a BFD interface.
show ip bfd-std sessions	Displays the status and statistics of the BFD sessions.

MIB Objects

```
alaBfdIntfTable
   alaBfdIntfDesiredMinTxInterval
```

ip bfd-std interface receive

Configures the receive time interval for the BFD interface. This command specifies the minimum amount of time BFD waits to receive control packets on the interface before determining there is a problem.

ip bfd-std interface *interface_name* **receive** *receive-interval*

Syntax Definitions

interface_name	The name of an existing BFD interface.
receive-interval	The receive time interval, in milliseconds. The valid range is 100–999.

Defaults

The global receive time interval value is used by default.

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- The global receive time interval serves as the default interval value for a BFD interface. The default interval value is overridden when a specific value is configured for the interface.
- Note that configuring the interface transmit time interval using the **ip bfd-std interface receive** command does not change the global value configured with the **ip bfd-std receive** command.

Examples

```
-> ip bfd-std interface bfd-vlan-101 receive 500
```

Release History

Release 6.3.4; command was introduced.

Related Commands

ip bfd-std interface	Creates a BFD interface.
ip bfd-std receive	Configures a global BFD receive time interval.
show ip bfd-std interfaces	Displays the BFD interface configuration table.
show ip bfd-std sessions	Displays the BFD interface configuration table.

MIB Objects

```
alaBfdIntfTable
   alaBfdIntfMinRxInterval
```

ip bfd-std interface multiplier

Configures the BFD interface dead interval multiplier. This command specifies a number that is used to calculate the BFD detection time used in the asynchronous mode. When an interface stops receiving packets from a neighbor, the interface uses the detection time value to determine how long to wait before declaring that the BFD session is down.

ip bfd-std interface *interface_name* **multiplier** *multiplier_value*

Syntax Definitions

interface_name	The name of an existing BFD interface.
multiplier_value	The dead interval multiplier number. The valid range is 1–10.

Defaults

By default, the multiplier value is set to 3.

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

The detection time between neighbors is calculated by multiplying the negotiated transmit time interval by the dead interval multiplier.

Examples

```
-> ip bfd-std interface bfd-vlan-101 multiplier 5
```

Release History

Release 6.3.4; command was introduced.

Related Commands

ip bfd-std interface	Creates a BFD interface.
show ip bfd-std interfaces	Displays the BFD interface configuration table.
show ip bfd-std sessions	Displays the BFD interface configuration table.

MIB Objects

```
alaBfdIntfTable
   alaBfdIntfDetectMult
```

ip bfd-std interface echo-interval

Configures the echo time interval for the BFD interface. The echo function is available with the asynchronous or demand mode. Echo packets are transmitted to BFD peers to see if they loop back to the peer from which they originated.

ip bfd-std interface *interface_name* **echo-interval** *echo-interval*

Syntax Definitions

interface_name	The name of an existing IP interface.
echo-interval	The echo time interval, in milliseconds. The valid range is 100–999.

Defaults

The global echo interval value is used by default.

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- The global echo time interval serves as the default interval value for a BFD interface. The default interval value is overridden when a specific value is configured for the interface.
- Note that configuring the interface echo time interval using the **ip bfd-std interface echo-interval** command does not change the global value configured with the **ip bfd-std echo-interval** command.

Examples

```
-> ip bfd-std interface bfd-vlan-101 echo-interval 500
```

Release History

Release 6.3.4; command was introduced.

Related Commands

ip bfd-std interface	Creates a BFD interface.
ip bfd-std echo interval	Configures a global BFD echo time interval.
show ip bfd-std interfaces	Displays the BFD interface configuration table.
show ip bfd-std sessions	Displays the BFD interface configuration table.

MIB Objects

```
alaBfdIntfTable
   alaBfdIntfReqMinEchoRxInterval
```

ip bfd-std interface mode

Configures the operational mode and echo status for the BFD interface.

ip bfd-std interface *interface_name* **mode {echo-only | demand [echo {enable | disable}] | asynchronous [echo {enable|disable}}**

Syntax Definitions

interface_name	The name of an existing IP interface.
echo-only	Specifies echo only mode.
demand echo enable	Specifies demand mode with the echo function enabled.
demand echo disable	Specifies demand mode with the echo function disabled.
asynchronous echo enable	Specifies asynchronous mode with the echo function enabled.
asynchronous echo disable	Specifies asynchronous mode with the echo function disabled.

Defaults

By default, the BFD interface is set to operate in demand mode with the echo function enabled.

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- The global operational mode and echo status serves as the default mode and status for a BFD interface. The default mode and status is overridden when a specific value is configured for the interface.
- Note that configuring the interface mode and echo status using the **ip bfd-std interface mode** command does not change the global value configured with the **ip bfd-std mode** command.

Examples

```
-> ip bfd-std mode echo-only
-> ip bfd-std mode demand echo enable
```

Release History

Release 6.3.4; command was introduced.

Related Commands

ip bfd-std interface	Creates a BFD interface.
ip bfd-std mode	Configures the global BFD operational mode and echo status.
show ip bfd-std interfaces	Displays the BFD interface configuration table.
show ip bfd-std sessions	Displays the BFD interface configuration table.

MIB Objects

```
alaBfdIntfTable
   alaBfdIntfOperMode
   alaBfdIntfEchoMode
```

ip bfd-std interface l2-hold-timer

Configures the Layer 2 hold-down (convergence) timer value for the BFD interface. This command specifies the amount of time the interface remains in a hold-down state after a Layer 2 topology change occurs.

ip bfd-std interface *interface_name* **12-hold-timer** *l2-holdtimer-interval*

Syntax Definitions

interface_name	The name of an existing BFD interface.
l2-holdtimer-interval	The Layer 2 hold-down time interval, in milliseconds. The valid range is 100–999.

Defaults

The global Layer 2 hold-down time interval is used by default.

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- The global Layer 2 hold-down time interval serves as the default interval for a BFD interface. The default interval value is overridden when a specific value is configured for the interface.
- Note that configuring the Layer 2 hold-down time interval using the **ip bfd-std interface l2-hold-timer** command does not change the global value configured with the **ip bfd-std l2-hold-timer** command.

Examples

```
-> ip bfd-std interface bfd-vlan-101 l2-hold-timer 500
```

Release History

Release 6.3.4; command was introduced.

Related Commands

ip bfd-std interface	Creates a BFD interface.
ip bfd-std l2-hold-timer	Configures the global BFD Layer 2 hold-down time interval.
show ip bfd-std interfaces	Displays the BFD interface configuration table.
show ip bfd-std sessions	Displays the BFD interface configuration table.

MIB Objects

```
alaBfdIntfTable
   alaBfdIntfL2HoldTimer
```

ip ospf bfd-std status

Enables or disables the BFD status for the OSPF protocol.

ip ospf bfd-std status {enable | disable}

Syntax Definitions

enable	Enables BFD Status.
disable	Disables BFD Status.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- All the status changes on the neighbors are received from the BFD level and the OSPF protocol acts based upon the BFD message.
- Whenever a neighbor goes down, OSPF informs BFD to remove that neighbor from the BFD active list.

Examples

```
-> ip ospf bfd-std status enable
-> ip ospf bfd-std status disable
```

Release History

Release 6.3.4; command was introduced.

Related Commands

ip ospf bfd-std all-interfaces	Enables or disables BFD for all OSPF interfaces configured.
ip ospf interface bfd-std	Enables or disables BFD for a specific OSPF interface.
ip ospf interface bfd-std drs-only	Establishes BFD sessions only on neighbors in full state.
ip ospf interface bfd-std all-nbrs	Establishes BFD sessions with all neighbors of the corresponding interface which are greater than or equal to “2-way” state.

MIB Objects

```
alaProtocolospf
   alaOspfBfdStatus
```

ip ospf bfd-std all-interfaces

Enables or disables BFD for all OSPF interfaces in the switch configuration.

ip ospf bfd-std all-interfaces

no ip ospf bfd-std all-interfaces

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to disable the BFD status for all OSPF interfaces.
- The BFD status for OSPF must be enabled before OSPF can interact with BFD.

Examples

```
-> ip ospf bfd-std all-interfaces
-> no ip ospf bfd-std all-interfaces
```

Release History

Release 6.3.4; command was introduced.

Related Commands

ip ospf bfd-std status	Enables or disables the BFD status for the OSPF protocol.
ip ospf interface bfd-std	Enables or disables BFD for a specific OSPF interface.
ip ospf interface bfd-std drs-only	Establishes BFD sessions only on neighbors in full state.
ip ospf interface bfd-std all-nbrs	Establishes BFD sessions with all neighbors of the corresponding interface which are greater than or equal to “2-way” state.

MIB Objects

```
alaProtocolospf
   alaOspfBfdAllInterfaces
```

ip ospf interface bfd-std

Enables or disables BFD for a specific OSPF interface.

ip ospf interface *interface-name* **bfd-std {enable | disable}**

Syntax Definitions

interface-name	The name of an existing OSPF interface.
enable	Enables the OSPF interface.
disable	Disables the OSPF interface.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

The BFD status for OSPF must be enabled before OSPF can interact with BFD.

Examples

```
-> ip ospf interface int1 bfd-std enable
-> ip ospf interface int2 bfd-std disable
```

Release History

Release 6.3.4; command was introduced.

Related Commands

ip ospf bfd-std status	Enables or disables the BFD status for the OSPF protocol.
ip ospf bfd-std all-interfaces	Enables or disables BFD for all OSPF interfaces configured.
ip ospf interface bfd-std drs-only	Establishes BFD sessions only on neighbors in full state.
ip ospf interface bfd-std all-nbrs	Establishes BFD sessions with all neighbors of the corresponding interface which are greater than or equal to “2-way” state.

MIB Objects

```
alaOspfIfAugEntry
   ospfIfIpAddress
   alaOspfIfBfdStatus
```

ip ospf interface bfd-std drs-only

Establishes BFD sessions only with neighbors that are in the full state.

ip ospf interface *interface-name* **bfd-std drs-only**

Syntax Definitions

interface-name	The name of an existing OSPF interface.

Defaults

By default, BFD is enabled for DR neighbors only.

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- The specified OSPF interface must be enabled to interact with BFD.
- The BFD status for OSPF must be enabled before OSPF can interact with BFD.

Examples

```
-> ip ospf interface int1 bfd-std drs-only
```

Release History

Release 6.3.4; command was introduced.

Related Commands

ip bfd-std interface status	Enables or disables the BFD status for OSPF protocol.
ip ospf bfd-std all-interfaces	Enables or disables BFD for all OSPF interfaces configured.
ip ospf interface bfd-std	Enables or disables BFD for a specific OSPF interface.
ip ospf interface bfd-std all-nbrs	Establishes BFD sessions with all neighbors of the corresponding interface which are greater than or equal to “2-way” state.

MIB Objects

```
alaOspfIfAugEntry
   ospfIfIpAddress
   alaOspfIfBfdDrsOnly
```

ip ospf interface bfd-std all-nbrs

Establishes BFD sessions with all neighbors of the corresponding interface which are greater than or equal to “2-way” state.

ip ospf interface *interface-name* **bfd-std all-nbrs**

Syntax Definitions

interface-name	The name of an existing OSPF interface.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- The specified OSPF interface must be enabled to interact with BFD.
- The BFD status for OSPF must be enabled before OSPF can interact with BFD.

Examples

```
-> ip ospf interface int1 bfd-std all-nbrs
```

Release History

Release 6.3.4; command was introduced.

Related Commands

ip bfd-std interface status	Enables or disables the BFD status for OSPF protocol.
ip ospf bfd-std all-interfaces	Enables or disables BFD for all OSPF interfaces configured.
ip ospf interface bfd-std	Enables or disables BFD for a specific OSPF interface.
ip ospf interface bfd-std drs-only	Establishes BFD sessions only on neighbors in full state.

MIB Objects

```
alaOspfIfAugEntry
   ospfIfIpAddress
   alaOspfIfBfdDrsOnly
```

ip bgp bfd-std status

Enables or disables BFD for the BGP protocol.

ip bgp bfd-std status {enable | disable}

Syntax Definitions

enable	Enables BGP.
disable	Disables BGP.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- All the status changes on the neighbors are received from the BFD level and the BGP protocol acts based upon the BFD message.
- Whenever a neighbor goes down, BGP informs BFD to remove that neighbor from the BFD active list.

Examples

```
-> ip bgp bfd-std status enable
-> ip bgp bfd-std status disable
```

Release History

Release 6.3.4; command was introduced.

Related Commands

ip bgp bfd-std all-neighbors	Enables or disables BFD for all BGP neighbors.
ip bgp neighbors bfd-std	Enables or disables BFD for a specific neighbor.

MIB Objects

```
alaBgpGlobal
   alaBgpBfdStatus
```

ip bgp bfd-std all-neighbors

Enables or disables BFD for all BGP neighbors.

ip bgp bfd-std all-neighbors

no ip bgp bfd-std all-neighbors

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to disable BFD for all BGP neighbors.
- The BFD status for BGP must be enabled before BGP can interact with BFD.

Examples

```
-> ip bgp bfd-std all-neighbors
-> no ip bgp bfd-std all-neighbors
```

Release History

Release 6.3.4; command was introduced.

Related Commands

ip bgp bfd-std status	Enables or disables BGP with BFD protocol.
ip bgp neighbors bfd-std	Enables or disables the BFD for a specific BGP neighbor.

MIB Objects

```
alaBgpGlobal
   alaBgpBfdAllNeighbors
```

ip bgp neighbors bfd-std

Enables or disables BFD for a specific BGP neighbor.

ip bgp neighbor *name* **bfd-std {enable | disable}**

Syntax Definitions

name	The peer name of the BGP neighbor.
enable	Enables BGP neighbor.
disable	Disables BGP neighbor.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

The BFD status for BGP must be enabled before BGP can interact with BFD.

Examples

```
-> ip bgp neighbor neigh1 bfd-std enable
-> ip bgp neighbor neigh2 bfd-std disable
```

Release History

Release 6.3.4; command was introduced.

Related Commands

ip bgp bfd-std status	Enables or disables BGP with BFD protocol.
ip bgp bfd-std all-neighbors	Enables or disables BFD for all BGP neighbors.

MIB Objects

```
alaBgpPeerEntry
   alaBgpPeerName
   alaBgpPeerBfdStatus
alaBgpGlobal
   alaBgpBfdAllNeighbors
```

vrrp bfd-std

Enables or disables VRRP with the BFD protocol.

vrrp bfd-std {enable | disable}

Syntax Definitions

enable	Enables BFD for VRRP.
disable	Disables BFD for VRRP.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- BFD support for VRRP is done only for tracking policy configuration for a remote address.
- The BFD status for VRRP must be enabled before VRRP can interact with BFD.

Examples

```
-> ip vrrp bfd-std enable
-> ip vrrp bfd-std disable
```

Release History

Release 6.3.4; command was introduced.

Related Commands

vrrp track address bfd-std	Enables or disable BFD for a specific tracking policy.

MIB Objects

```
alaVrrpConfig
   alaVrrpBfdStatus
```

vrrp track address bfd-std

Enables or disable BFD for a specific track policy.

vrrp track *num* **address** *address* **bfd-std {enable| disable}**

Syntax Definitions

num	The VRRP track number.
address	The remote IP address.
enable	Enables BFD.
disable	Disables BFD.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- BFD support for VRRP is done only for tracking policy configuration for a remote address.
- The BFD status for VRRP must be enabled before VRRP can interact with BFD.

Examples

```
-> vrrp track 2 address 10.1.1.1 bfd-std enable
-> vrrp track 3 address 10.1.1.2 bfd-std disable
```

Release History

Release 6.3.4; command was introduced.

Related Commands

vrrp bfd-std	Enables or disables VRRP with BFD protocol.

MIB Objects

```
alaVRRPConfig
   alaVrrpTrackBfdStatus
```

ip static-route all bfd-std

Enables BFD for all static routes.

ip static-route all bfd-std {enable| disable}

Syntax Definitions

enable	Enables BFD.
disable	Disables BFD.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- When there are static route configured in the switch, BFD is enabled to track the gateway.
- If the route is not reachable, it is moved to the inactive database.

Examples

```
-> ip static-route all bfd-std enabled
-> ip static-route all bfd-std disabled
```

Release History

Release 6.3.4; command was introduced.

Related Commands

ip static-routes bfd-std status	Enables or disables BFD for a specific static route.

MIB Objects

```
alaIprmConfig
   alaIprmStaticallbfd
```

ip static-routes bfd-std status

Enables or disables BFD for a specific static route.

ip static-routes *ip-address/prefixLen* **gateway** *ip-address* **bfd-std status {enable| disable}**

Syntax Definitions

ip_address	The destination IP address.
prefixLen	The prefix length for the destination IP address.
gateway *ip_address*	The gateway IP address.
enable	Enables BFD.
disable	Disables BFD.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

BFD is enabled to track the gateway of static routes.

Examples

```
-> ip static-route 10.1.1.1 255.0.0.0 gateway 10.1.1.25 bfd-std status enable
-> ip static-route 10.1.1.2 255.0.0.0 gateway 10.1.1.25 bfd-std status disabled
```

Release History

Release 6.3.4; command was introduced.

Related Commands

ip bfd-std l2-hold-timer	Configures BFD at Global Level.
ip static-route all bfd-std	Enables BFD for all static routes.

MIB Objects

```
alaIprmStaticRouteEntry
   alaIprmStaticRouteDest
   alaIprmStaticRouteMask
   alaIprmStaticRouteNextHop
   alaIprmStaticRouteBfdStatus
```

show ip bfd-std

Displays the global BFD configuration table.

show ip bfd-std

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

N/A

Examples

```
-> show ip bfd-std
BFD Version Number              = 1,
Admin Status                    = Disabled,
Transit Interval                = 300,
Receive Interval                = 300,
Multiplier                      = 3,
Echo Status                     = Enabled,
Echo Interval                   = 300,
Mode                            = ASYNCHRONOUS,
L2 Hold Down Interval           = 500,
Protocols Registered            = PIM
```

output definitions

BFD Version Number	Refers to BFD Version.
Admin Status	Refers to BFD global admin status.
Transmit interval	Refers to BFD global Tx interval.
Receive interval	Refers to BFD global Rx interval.
Multiplier	Refers to BFD interface Multiplier.
Echo status	Refers to Echo functionality status.
Echo interval	Refers to BFD echo Rx interval.
Mode	Refers to BFD echo operational mode.
L2 Hold Down Interval	Refers to BFD Layer 2 hold down interval.
Protocols Registered	Refers to Protocols registered to BFD.

Release History

Release 6.3.4; command was introduced.
Release 6.4.5; **L2 Hold Down Interval** added in output.

Related Commands

ip bfd-std status	Configures BFD at global level.
ip bfd-std interface	Configures BFD at interface level.

MIB Objects

```
alaBfdIntfTable
   alaBfdGlobalVersionNumber
   alaBfdGlobalAdminStatus
   alaBfdGlobalTxInterval
   alaBfdGlobalRxInterval
   alaBfdGlobalEcho
   alaBfdGlobalEchoRxInterval
   alaBfdGlobalOperMode
   alaBfdGlobalProtocols
```

show ip bfd-std interfaces

Displays the BFD interface configuration table.

show ip bfd-std interfaces [*interface-name***]**

Syntax Definitions

interface-name	The name of the BFD interface.

Defaults

By default, the configuration for all BFD interfaces is displayed.

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

Enter an interface name to display information for a specific BFD interface.

Examples

```
->show ip bfd-std interfaces
Interface               Admin     Tx        Min Rx                Oper
Name        Mode        Status    Interval  Interval  Multiplier  Status
----------+------------+---------+---------+---------+-----------+----------
vlan-10     ASYNCHRONOUS enabled     100      100        3          UP
vlan-20     ASYNCHRONOUS disabled    0        0          5          DOWN

-> show ip bfd-std interfaces vlan-10
Interface IP Address:           = 215.20.10.1,
Admin Status:                   = Enabled,
Mode:                           = ASYNCHRONOUS,
Echo Status:                    = Disabled,
Transmit Interval:              = 100,
Receive Interval:               = 100,
Multiplier:                     = 3,
Echo Interval:                  = 100,
L2 Hold Down Interval           = 100
```

output definitions

Interface address	Refers to BFD Interface address.
Admin status	Refers to BFD interface admin status.
Mode	Refers to BFD interface operational mode.
Echo status	Refers to Interface Echo functionality status.
Transmit Interval	Refers to BFD interface Tx interval.
Receive Interval	Refers to BFD interface Rx interval.
Multiplier	Refers to BFD interface Multiplier.

output definitions (continued)

Echo interval	Refers to BFD interface echo Rx interval.
Layer2 Hold down Interval	Refers to BFD Layer 2 hold down interval.

Release History

Release 6.3.4; command was introduced.

Related Commands

ip bfd-std status	Configures BFD at global level.
ip bfd-std interface	Configures BFD at interface level.

MIB Objects

```
alaBfdIntfTable
   alaBfdIntfAddr
   alabfdIntfAdminStatus
   alaBfdIntfOperMode
   alaBfdIntfDesiredMinTxInterval
   alaBfdIntfReqMinRxInterval
   alaBfdIntfDetectMult
   alaBfdIntfEchoMode
   alaBfdIntfReqMinEchoRxInterval
   alaBfdIntfL2HoldTimer
```

show ip bfd-std sessions

Displays all the BFD sessions for the switch.

show ip bfd-std sessions

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show ip bfd-std sessions
Neighbor    Interface            Local  Remote  Negotiated  Negotiated Echo Rx
IP Address  Address       State  Disc   Disc     Tx          Rx
-----------+------------+-------+------+------+------------+----------+----------
25.25.25.1   25.25.25.25  UP     45      53     100          100        200
26.26.26.63  26.26.26.36  INIT   43      21     200          200        200
```

output definitions

Interface address	The IP address associated with the BFD interface.
State	The state of the BFD session.
Neighbor address	The IP address of the BFD neighbor.
Local discriminator	The local discriminator.
Remote discriminator	The remote discriminator.
Protocol	The protocols registered with the BFD session.
Negotiated Tx interval	The negotiated transmit interval.
Negotiated Rx interval	The negotiated receive interval.
Echo Rx interval	The Echo packet receive interval.
Multiplier	The BFD multiplier number.
Tx packet counter	The transmit packet counter.
Rx packet counter	The receive packet counter.
Protocols enabled	The protocols enabled for BFD.

Release History

Release 6.3.4; command was introduced.

Related Commands

ip bfd-std status	Configures BFD at global level.
ip bfd-std interface	Configures BFD at interface level.
show ip bfd-std session	Displays information for a specific session.

MIB Objects

```
alaBfdIntfTable
   alaBfdSessNeighborAddr
   alaBfdIntfAddr
   alaBfdSessState
   alaBfdSessDiscriminator
   alaBfdSessRemoteDiscr
   alaBfdIntfProtocols
   alaBfdSessNegotiatedTxInterval
   alaBfdSessNegotiatedRxInterval
   alaBfdIntfReqMinEchoRxInterval
   alaBfdIntfL2HoldTimer
   alaBfdSessPerfPktOut
   alaBfdSessPerfPktIn
   alaBfdSessProtocols
```

show ip bfd-std session

Displays information for an individual BFD session.

show ip bfd-std session *neighbor_address*

Syntax Definitions

neighbor_address	The local BFD descriminator address for the neighbor.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show ip bfd-std session 1
Interface IP Address             = 101.101.101.2,
Neighbor IP Address              = 101.101.101.8,
State                            = Up,
Local discriminator              = 1,
Remote discriminator             = 0,
Negotiated Tx interval           = 240,
Negotiated Rx interval           = 300,
Echo Rx interval                 = 300,
Multiplier                       = 3,
Tx packet counter                = 42523,
Rx packet counter                = 0,
Protocols Registered             = PIM
```

output definitions

Interface address	The IP address associated with the BFD interface.
State	The state of the BFD session.
Neighbor address	The IP address of the BFD neighbor.
Local discriminator	The local discriminator.
Remote discriminator	The remote discriminator.
Protocol	The protocols registered with the BFD session.
Negotiated Tx interval	The negotiated transmit interval.
Negotiated Rx interval	The negotiated receive interval.
Echo Rx interval	The Echo packet receive interval.
Multiplier	The BFD multiplier number.

output definitions (continued)

Tx packet counter	The transmit packet counter.
Rx packet counter	The receive packet counter.
Protocols Registered	The protocols registered for BFD.

Release History

Release 6.3.4; command was introduced.
Release 6.4.5; **Protocol Enabled** in output is modified to **Protocol Registered**.

Related Commands

ip bfd-std status	Configures BFD at global level.
ip bfd-std interface	Configures BFD at interface level.
show ip bfd-std sessions	Displays all BFD sessions.

MIB Objects

```
alaBfdIntfTable
   alaBfdSessNeighborAddr
   alaBfdIntfAddr
   alaBfdSessState
   alaBfdSessDiscriminator
   alaBfdSessRemoteDiscr
   alaBfdIntfProtocols
   alaBfdSessNegotiatedTxInterval
   alaBfdSessNegotiatedRxInterval
   alaBfdIntfReqMinEchoRxInterval
   alaBfdIntfL2HoldTimer
   alaBfdSessPerfPktOut
   alaBfdSessPerfPktIn
   alaBfdSessProtocols
```

25 DHCP and DHCPv6 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 (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 and DHCPv6 Relay commands is as follows:

Filename: AlcatelIND1UDPRelay.MIB
Module: ALCATEL-IND1-UDP-RELAY-MIB

A summary of the available DHCP Relay commands are listed here.

DCHP Relay Commands	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 pxe-support ip helper dhcp-snooping ip helper dhcp-snooping mac-address verification ip helper dhcp-snooping option-82 data-insertion ip helper dhcp-snooping option-82 format ip helper dhcp-snooping option-82 format ascii circuit-id ip helper dhcp-snooping option-82 format ascii remote-id ip helper dhcp-snooping bypass option-82-check ip helper dhcp-snooping vlan ip helper dhcp-snooping port ip helper dhcp-snooping linkagg ip helper dhcp-snooping port traffic-suppression ip helper dhcp-snooping port ip-source-filtering ip helper dhcp-snooping binding ip helper dhcp-snooping ip-source-filter ip helper dhcp-snooping binding timeout ip helper dhcp-snooping binding action ip helper dhcp-snooping binding persistency ip helper boot-up 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 dhcp-server clear dhcp-server statistics clear dhcp-server statistics show dhcp-server leases show dhcp-server statistics ip helper dhcp-snooping ip-source-filter show ip helper dhcp-snooping ip-source-filter

A summary of the available DHCPv6 Relay commands are listed here.:

DHCPv6 Relay commands	**ipv6 helper address** **ipv6 helper address vlan** **ipv6 helper standard** **ipv6 helper per-vlan only** **ipv6 helper maximum hops** **ipv6 helper dhcp-snooping** **ipv6 helper dhcp-snooping vlan** **ipv6 helper dhcp-snooping port** **ipv6 helper dhcp-snooping linkagg** **ipv6 helper dhcp-snooping binding** **ipv6 helper dhcp-snooping binding timeout** **ipv6 helper dhcp-snooping binding action** **ipv6 helper dhcp-snooping binding persistency** **ipv6 helper interface-id prefix** **ipv6 helper remote-id format** **show ipv6 helper** **show ipv6 helper stats** **show ipv6 helper dhcp-snooping vlan** **show ipv6 helper dhcp-snooping port** **show ipv6 helper dhcp-snooping binding**

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 (for example, 21.0.0.10).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 can 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.
- UDP 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 6.1; command 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 (for example, 21.0.0.10) of the DHCP server VLAN.
vlan_id	VLAN identification number (for example, 3) of the DHCP server VLAN.

Defaults

If no VLAN identification number is entered, VLAN ID 0 is used by default.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete the DHCP server VLAN from the DHCP Relay.
- Specifying multiple VLAN IDs and/or a range of VLAN IDs on the same command line is allowed. Use a hyphen to indicate a contiguous range and a space to separate multiple VLAN ID entries (for example, 10-15 500-510 850).
- 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
-> ip helper address 198.206.15.2 250-255
-> ip helper address 10.11.4.1 550-555 1500 1601-1620
-> ip helper no address 198.206.15.2 1601-1620
```

Release History

Release 6.1; command introduced.
Release 6.1.2; support added for entering a range and/or multiple entries of VLAN IDs.

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 6400, 6850E, 6855, 9000E

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 6.1; command 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 6400, 6850E, 6855, 9000E

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 6.1; command 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 6400, 6850E, 6855, 9000E

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 6.1; command 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 6400, 6850E, 6855, 9000E

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 6.1; command 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 6400, 6850E, 6855, 9000E

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 6.1; command 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 6400, 6850E, 6855, 9000E

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 6.1.2; command 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 6400, 6850E, 6855, 9000E

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 6.1.2; command 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 pxe-support

Enables or disables relay agent support for Preboot Execution Environment (PXE) devices.

ip helper pxe-support {enable | disable}

Syntax Definitions

enable	Enables PXE support.
disable	Disables PXE support.

Defaults

By default, PXE support is disabled for the switch.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- PXE support was enabled by default in previous releases. Note that PXE is currently disabled by default and is now a user-configurable option using the **ip helper pxe-support** command.
- Enable PXE support to insert 'relay agent IP address' (client IP address space) as the source IP address. With PXE support disabled, relayed DHCP packets toward the DHCP server take the outgoing interface IP as the source IP address.
- Configure PXE support only on switches where packets are routed between IP networks. Also, validate the reachability of relay agent IP address, in case configuration is deemed necessary.
- **ip helper pxe-support disable** is the no form of this command. This is the default configuration of PXE support.

Examples

```
-> ip helper pxe-support enable
-> ip helper pxe-support disable
```

Release History

Release 6.3.1; command introduced.

Related Commands

show ip helper	Displays current DHCP Relay configuration information.

MIB Objects

```
iphelperPXESupport
```

ip helper traffic-suppression

Globally enables or disables the suppression of DHCP broadcast traffic on the switch. When this feature is enabled, all DHCP broadcast packets are forwarded to the relay agent for processing even if the client and server reside in the same VLAN.

This command is currently not supported. Traffic suppression is automatically enabled when DHCP Snooping is enabled for the switch or for specific VLANs.

ip helper traffic-suppression {enable | disable}

Syntax Definitions

enable	Enables traffic suppression for the switch.
disable	Disables traffic suppression for the switch.

Defaults

By default, traffic suppression is disabled for the switch.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- When traffic suppression is enabled, any active relay agent features (for example, Option-82 data insertion, DHCP Snooping) are also effected on all DHCP broadcast traffic, regardless of the VLAN in which the traffic originated.
- Enabling traffic suppression requires the configuration of IP helper addresses for all DHCP servers, even if the server resides in the same VLAN as the DHCP clients.
- Note that enabling DHCP traffic suppression for the switch overrides any traffic suppression status configured for an individual DHCP Snooping port.
- If the per-VLAN UDP Relay mode is active for the switch, DHCP broadcast traffic originating in a VLAN that does not have an IP helper address configured is still broadcast whether or not traffic suppression is enabled for the switch.
- When traffic suppression is disabled, DHCP packets are flooded on the default VLAN for the port. Any DHCP server in the same VLAN domain as the client will receive and respond to such packets without the involvement of the relay agent.

Examples

```
-> ip helper traffic-suppression enable
-> ip helper traffic-suppression disable
```

Release History

Release 6.1.3; command introduced.
Release 6.1.5; command was deprecated.

Related Commands

ip helper dhcp-snooping	Enables or disables DHCP Snooping for the switch.
ip helper dhcp-snooping vlan	Enables or disables DHCP Snooping on a per VLAN basis.
show ip helper	Displays the current DHCP configuration for the switch.

MIB Objects

```
iphelperTrafficSuppressionStatus
```

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 6400, 6850E, 6855, 9000E

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 prevents 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 6.1.2; command introduced.

Related Commands

ip helper dhcp-snooping vlan	.Enables or disables DHCP Snooping on a per VLAN basis.
show ip helper	Displays the current DHCP configuration for the switch.

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 6400, 6850E, 6855, 9000E

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 6.1.2; command 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 6400, 6850E, 6855, 9000E

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.

Examples

```
-> ip helper dhcp-snooping option-82 data-insertion enable
-> ip helper dhcp-snooping option-82 data-insertion disable
```

Release History

Release 6.1.2; command introduced.

Related Commands

ip helper dhcp-snooping option-82 format	Configures the type of information that is inserted in both the Circuit ID and Remote ID suboption of the Option-82 field.
ip helper dhcp-snooping	.Globally enables or disables DHCP Snooping for the switch.
ip helper dhcp-snooping ip-source-filter	Enables or disables the DHCP Snooping binding table functionality
show ip helper	Displays the current DHCP configuration for the switch.

MIB Objects

iphelperDhcpSnoopingOpt82DataInsertionStatus

ip helper dhcp-snooping option-82 format

Configures the type of information that is inserted into both the Circuit ID and Remote ID suboption fields of the Option-82 field.

ip helper dhcp-snooping option-82 format {base-mac | system-name | user-string *string* | **interface-alias | auto-interface-alias}**

Syntax Definitions

base-mac	The base MAC address of the switch.
system-name	The system name of the switch.
string	A user-defined text string up to 64 characters.
interface-alias	The alias configured for the interface.
auto-interface-alias	The switch automatically generates the interface-alias in the following format: *SystemName_slot_port*.

Defaults

parameter	value
base-mac | system-name | user-string *string*	**base-mac**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The *string* parameter specifies user-defined information to insert into the Circuit ID and Remote ID fields.
- When entering a *string* for user-defined Option-82 information, quotes are required around ambiguous characters, such as hex characters, spaces, etc, so they are interpreted as text. For example, the *string* “Building B Server” requires quotes because of the spaces between the words.
- The interface-alias parameter will use the alias configured with the **interfaces alias** command. If no alias is configured a NULL string will be inserted.
- A maximum of 63 characters can be inserted when using the **interface-alias** and **auto-interface-alias** commands, remaining characters will be truncated.
- The Option-82 format option is a global setting, the format specified will be applied to all ports on the switch.
- The data specified with this command is added to the Circuit ID and Remote ID fields only when DHCP Option-82 data insertion is enabled for the switch.
- When DHCP Snooping is enabled at the switch level, Option-82 data insertion is enabled by default.

Examples

```
-> ip helper dhcp-snooping option-82 format user-string “Building B Server”
-> ip helper dhcp-snooping option-82 format system-name
-> ip helper dhcp-snooping option-82 format base-mac
-> ip helper dhcp-snooping option-82 format interface-alias
-> ip helper dhcp-snooping option-82 format auto-interface-alias
```

Release History

Release 6.3.1; command introduced.
Release 6.4.2; **interface-alias** and **auto-interface-alias** parameters introduced.

Related Commands

ip helper dhcp-snooping option-82 data-insertion	Globally enables or disables DHCP Option-82 data insertion for DHCP packets.
ip helper dhcp-snooping	Globally enables or disables DHCP Snooping for the switch.
show ip helper	Displays the current DHCP configuration for the switch.
interfaces alias	Configures an alias for a port.

MIB Objects

```
iphelperDhcpSnoopingOption82FormatType
iphelperDhcpOption82FormatInterfaceAliasAutoGen
iphelperDhcpSnoopingOption82StringValue
```

ip helper dhcp-snooping option-82 format ascii circuit-id

Configures the type of information that is inserted into the Option-82 Circuit ID suboption. The information is inserted into the Circuit ID field in ASCII text string format.

ip helper dhcp-snooping option-82 format ascii circuit-id {base-mac | system-name | vlan | user-string *string* | **interface-alias | cvlan} {delimiter** *character***}**

no ip helper dhcp-snooping option-82 format ascii circuit-id

Syntax Definitions

base-mac	The base MAC address of the switch.
system-name	The system name of the switch.
vlan	The VLAN ID of which the client is a member.
string	A user-defined text string up to 64 characters.
interface-alias	The alias configured for the interface.
cvlan	The Customer VLAN ID.
character	The delimiter character that separates fields within the Circuit ID ASCII string value. Valid characters are **|** (pipe), \ (backward slash), / (forward slash), **-** (dash), **_** (underscore), and " " (space).

Defaults

By default, the base MAC address of the switch is used in ASCII format.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guideline

- This command is used to specify the type of information that is configured in ASCII text string format and then inserted into the Option-82 Circuit ID suboption. Each parameter provided with this command represents a different type of information.
- Configuring the Circuit ID suboption in ASCII format allows up to five fields (types) of information within the ASCII string. However, if the contents of all the fields combined exceeds 127 characters, then the ASCII string is truncated.
- Specifying at least one parameter with this command is required. If multiple parameters are selected, then specifying one of the valid delimiter characters is also required.
- The *string* parameter specifies user-defined information to insert into the Circuit ID ASCII field.
- When entering a *string* for user-defined Option-82 information, quotes are required around ambiguous characters, such as hex characters, spaces, etc, so they are interpreted as text. For example, the *string* "Building B Server" requires quotes because of the spaces between the words.

- The **interface-alias** parameter will use the alias configured with the **interfaces alias** command. If no alias is configured, a NULL string will be inserted.
- A maximum of 63 characters can be inserted when using the **interface-alias** keyword, remaining characters will be truncated.
- The Option-82 format option is a global setting, the format specified will be applied to all ports on the switch.
- The data specified with this command is inserted into the Circuit ID suboption only when DHCP Option-82 data insertion is enabled for the switch.
- When DHCP Snooping is enabled at the switch level, Option-82 data insertion is enabled by default.

Examples

```
-> ip helper dhcp-snooping option-82 format ascii circuit-id user-string “Bldg A
Server”
-> ip helper dhcp-snooping option-82 format ascii circuit-id vlan system-name
delimiter /
-> ip helper dhcp-snooping option-82 format ascii circuit-id user-string “Bldg. B
Server” base-mac system name vlan interface-alias delimiter |
```

Release History

Release 6.4.4; command introduced.

Related Commands

ip helper dhcp-snooping option-82 data-insertion	Globally enables or disables DHCP Option-82 data insertion for DHCP packets.
ip helper dhcp-snooping	Globally enables or disables DHCP Snooping for the switch.
show ip helper	Displays the current DHCP configuration for the switch.
interfaces alias	Configures an alias for a port.

MIB Objects

```
iphelperDhcpSnoopingOption82FormatASCIIConfigurableEntry
iphelperDhcpSnoopingOption82FormatASCIIConfigurableIndex
iphelperDhcpSnoopingOption82FormatASCIIConfigurableField1
iphelperDhcpSnoopingOption82FormatASCIIConfigurableField1StringValue
iphelperDhcpSnoopingOption82FormatASCIIConfigurableConfigurableField2
iphelperDhcpSnoopingOption82FormatASCIIConfigurableField2StringValue
iphelperDhcpSnoopingOption82FormatASCIIConfigurableField3
iphelperDhcpSnoopingOption82FormatASCIIConfigurableField3StringValue
iphelperDhcpSnoopingOption82FormatASCIIConfigurableField4
iphelperDhcpSnoopingOption82FormatASCIIConfigurableField4StringValue
iphelperDhcpSnoopingOption82FormatASCIIConfigurableField5
iphelperDhcpSnoopingOption82FormatASCIIConfigurableField5StringValue
iphelperDhcpSnoopingOption82FormatASCIIConfigurableDelimiter
```

ip helper dhcp-snooping option-82 format ascii remote-id

Configures the type of information that is inserted into the Option-82 Remote ID suboption. The information is inserted into the Remote ID field in ASCII text string format.

ip helper dhcp-snooping option-82 format ascii remote-id {base-mac | system-name | vlan | user-string *string* | **interface-alias | cvlan} {delimiter** *character***}**

no ip helper dhcp-snooping option-82 format ascii remote-id

Syntax Definitions

base-mac	The base MAC address of the switch.
system-name	The system name of the switch.
vlan	The VLAN ID of which the client is a member.
string	A user-defined text string up to 64 characters.
interface-alias	The alias configured for the interface.
cvlan	The Customer VLAN ID.
character	The delimiter character that separates fields within the Circuit ID ASCII string value. Valid characters are **|** (pipe), \ (backward slash), / (forward slash), **-** (dash), **_** (underscore), and " " (space).

Defaults

By default, the base MAC address of the switch is used in ASCII format.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guideline

- This command is used to specify the type of information that is configured in ASCII text string format and then inserted into the Option-82 Remote ID suboption. Each parameter provided with this command represents a different type of information.
- Configuring the Remote ID suboption in ASCII format allows up to five fields (types) of information within the ASCII string. However, if the contents of all the fields combined exceeds 127 characters, then the ASCII string is truncated.
- Specifying at least one parameter with this command is required. If multiple parameters are selected, then specifying one of the valid delimiter characters is also required.
- The *string* parameter specifies user-defined information to insert into the Remote ID ASCII field.
- When entering a *string* for user-defined Option-82 information, quotes are required around ambiguous characters, such as hex characters, spaces, etc, so they are interpreted as text. For example, the *string* "Building B Server" requires quotes because of the spaces between the words.

- The **interface-alias** parameter will use the alias configured with the **interfaces alias** command. If no alias is configured, a NULL string will be inserted.
- A maximum of 63 characters can be inserted when using the **interface-alias** commands, remaining characters will be truncated.
- The Option-82 format option is a global setting, the format specified will be applied to all ports on the switch.
- The data specified with this command is inserted into the Remote ID suboption only when DHCP Option-82 data insertion is enabled for the switch.
- When DHCP Snooping is enabled at the switch level, Option-82 data insertion is enabled by default.

Examples

```
-> ip helper dhcp-snooping option-82 format ascii remote-id user-string “Bldg A
Server”
-> ip helper dhcp-snooping option-82 format ascii remote-id vlan system-name delim-
iter /
-> ip helper dhcp-snooping option-82 format ascii remote-id user-string “Bldg. B
Server” base-mac system name vlan interface-alias delimiter |
```

Release History

Release 6.4.4; command introduced.

Related Commands

ip helper dhcp-snooping option-82 data-insertion	Globally enables or disables DHCP Option-82 data insertion for DHCP packets.
ip helper dhcp-snooping	Globally enables or disables DHCP Snooping for the switch.
show ip helper	Displays the current DHCP configuration for the switch.
interfaces alias	Configures an alias for a port.

MIB Objects

```
iphelperDhcpSnoopingOption82FormatASCIIConfigurableEntry
iphelperDhcpSnoopingOption82FormatASCIIConfigurableIndex
iphelperDhcpSnoopingOption82FormatASCIIConfigurableField1
iphelperDhcpSnoopingOption82FormatASCIIConfigurableField1StringValue
iphelperDhcpSnoopingOption82FormatASCIIConfigurableConfigurableField2
iphelperDhcpSnoopingOption82FormatASCIIConfigurableField2StringValue
iphelperDhcpSnoopingOption82FormatASCIIConfigurableField3
iphelperDhcpSnoopingOption82FormatASCIIConfigurableField3StringValue
iphelperDhcpSnoopingOption82FormatASCIIConfigurableField4
iphelperDhcpSnoopingOption82FormatASCIIConfigurableField4StringValue
iphelperDhcpSnoopingOption82FormatASCIIConfigurableField5
iphelperDhcpSnoopingOption82FormatASCIIConfigurableField5StringValue
iphelperDhcpSnoopingOption82FormatASCIIConfigurableDelimiter
```

ip helper dhcp-snooping bypass option-82-check

Enables or disables checking for an Option-82 field in DHCP packets ingressing on untrusted ports.

ip helper dhcp-snooping bypass option-82-check {enable | disable}

Syntax Definitions

enable	Bypasses the Option-82 field check.
disable	Checks DHCP packets for the Option-82 field.

Defaults

By default, this feature is disabled.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- When this feature is disabled (the default), DHCP packets ingressing on untrusted ports are checked to see if they contain the Option-82 field. If this field is present, the DHCP packet is discarded.
- When this feature is enabled, DHCP packets ingressing on untrusted ports are *not* checked to see if they contain the Option-82 field. In this case, the Option-82 field is ignored and all DHCP packets are processed.
- Using this command is only allowed when DHCP Snooping is enabled globally for the switch or at the VLAN level.

Examples

```
-> ip helper dhcp-snooping bypass option-82-check enable
-> ip helper dhcp-snooping bypass option-82-check disable
```

Release History

Release 6.1.5; command introduced.

Related Commands

ip helper dhcp-snooping	Globally enables or disables DHCP Snooping for the switch.
show ip helper	Displays the current DHCP configuration for the switch.

MIB Objects

```
iphelperDHCPSnoopingBypassOpt82CheckStatus
```

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 6400, 6850E, 6855, 9000E

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 prevents 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 6.1.2; command introduced.

Related Commands

ip helper dhcp-snooping	Globally enables or disables DHCP Snooping for the switch.
ip helper dhcp-snooping ip-source-filter	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 (for example, 3/1 specifies port 1 on slot 3). Use a hyphen to specify a range of ports (for example, 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 6400, 6850E, 6855, 9000E

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 **show 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 6.1.2; command 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 linkagg

Configures the DHCP Snooping trust mode for the link aggregate. The trust mode determines if the link-aggregate will accept all DHCP traffic, block all DHCP traffic, or accept only client DHCP traffic.

ip helper dhcp-snooping linkagg *num* **{block | client-only | trust| ip-source-filtering}**

Syntax Definitions

num	Specifies the link aggregate ID number.
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 link aggregate. The port behaves as if DHCP Snooping was not enabled.
ip-source-filter	Traffic on the port is restricted to packets received on the port that contain the client MAC address and IP address. All other packets are dropped.

Defaults

By default, the trust mode for a link aggregate is set to **client-only** when the DHCP Snooping feature is enabled for the switch or for a VLAN.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 link aggregates.
- If DHCP Snooping is enabled for a specific VLAN, then the trust mode applies to only those link aggregates that are associated with that VLAN.
- Use the **show ip helper dhcp-snooping port** command to display the current trust mode for a link aggregate and statistics regarding the number of packets dropped due to DHCP Snooping violations.

Examples

```
-> ip helper dhcp-snooping linkagg 1 trust
-> ip helper dhcp-snooping linkagg 2 block
-> ip helper dhcp-snooping linkagg 3 client-only
```

Release History

Release 6.1.2; command introduced.

Release 6.4.4; ip-source-filtering parameter deprecated, use **ip helper dhcp-snooping ip-source-filter**.

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 port traffic-suppression

Configures the traffic suppression status for the port. When this function is enabled, DHCP packets are not flooded on the default VLAN for the specified port. This will prevent DHCP communications between a DHCP server and a client when both devices belong to the same VLAN domain.

This command is currently not supported. Traffic suppression is automatically enabled when DHCP Snooping is enabled for the switch or for specific VLANs.

ip helper dhcp-snooping port *slot1/port1***[-***port1a***] traffic-suppression {enable | disable}**

Syntax Definitions

*slot1/port1***[-***port1a***]**	Specifies the slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3). Use a hyphen to specify a range of ports (for example, 3/1-16).
enable	Enables traffic suppression for the specified port.
disable	Disables traffic suppression for the specified port.

Defaults

By default, traffic suppression is disabled for the port.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Traffic suppression applies only to ports that are associated with a VLAN that has DHCP Snooping enabled or to all ports when DHCP Snooping is globally enabled for the switch.
- When traffic suppression is disabled, then DHCP packets are flooded on the default VLAN for the port. Any DHCP server in the same VLAN domain as the client will receive and respond to such packets; DHCP Snooping is not invoked in this scenario.

Examples

```
-> ip helper dhcp-snooping port 1/24 traffic-suppression enable
-> ip helper dhcp-snooping port 2/1-10 traffic-suppression enable
-> ip helper dhcp-snooping port 4/8 traffic-suppression disable
-> ip helper dhcp-snooping port 3/1-5 traffic-suppression disable
```

Release History

Release 6.1.2; command introduced.
Release 6.1.5; command was deprecated.

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.
ip helper dhcp-snooping port	Configures the DHCP Snooping trust mode for a port.
ip helper dhcp-snooping port ip-source-filtering	Configures the IP source filtering status for a DHCP Snooping port.

MIB Objects

```
iphelperDhcpSnoopingPortTable
   iphelperDhcpSnoopingPortIfIndex
   iphelperDhcpSnoopingPortIpTrafficSuppression
```

ip helper dhcp-snooping port ip-source-filtering

Configures the IP source filtering status for the port. When this function is enabled, traffic on the port is restricted to packets received on the port that contain the client MAC address and IP address. All other packets are dropped.

ip helper dhcp-snooping port *slot1/port1***[-***port1a***] ip-source-filtering {enable | disable}**

Syntax Definitions

*slot1/port1***[-***port1a***]**	Specifies the slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3). Use a hyphen to specify a range of ports (for example, 3/1-16).
enable	Enables IP source filtering for the specified port.
disable	Disables IP source filtering for the specified port.

Defaults

By default, IP source filtering is disabled for the port.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- IP source filtering applies only to ports that are associated with a VLAN that has DHCP Snooping enabled or to all ports when DHCP Snooping is globally enabled for the switch.
- The DHCP Snooping binding table is used to verify client information.
- If a device connected to a DHCP Snooping port with IP source filtering enabled does not have a valid IP address lease from the trusted DHCP server, then all IP traffic for that device is blocked on the port.
- Disable IP source filtering for the DHCP Snooping port to allow a device to obtain a valid IP address lease.
- Once a device obtains a valid lease or if a device already has a valid lease, then only source bound traffic is allowed.

Examples

```
-> ip helper dhcp-snooping port 1/24 ip-source-filtering enable
-> ip helper dhcp-snooping port 2/1-10 ip-source-filtering enable
-> ip helper dhcp-snooping port 4/8 ip-source-filtering disable
-> ip helper dhcp-snooping port 3/1-5 ip-source-filtering disable
```

Release History

Release 6.1.2; command introduced.
Release 6.4.4; ip-source-filtering parameter deprecated, use **ip helper dhcp-snooping ip-source-filter**.

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.
ip helper dhcp-snooping port	Configures the DHCP Snooping trust mode for a port.
ip helper dhcp-snooping port traffic-suppression	Configures the traffic suppression status for a DHCP Snooping port.

MIB Objects

```
iphelperDhcpSnoopingPortTable
   iphelperDhcpSnoopingPortIfIndex
   iphelperDhcpSnoopingPortIpSourceFiltering
```

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* **vlan** *vlan_id***]}**

no ip helper dhcp-snooping port binding *mac_address* **port** *slot/port* **address** *ip_address* **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.
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 6400, 6855, 9000E

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 6.1.2; command introduced.
Release 6.3.4; **lease-time** parameter was removed.

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
   iphelperDhcpSnoopingBindingVlan
   iphelperDhcpSnoopingBindingType
```

ip helper dhcp-snooping ip-source-filter

Enables or disables the IP source filtering capability at a port, link aggregation, or VLAN level. When this function is enabled, the switch allows the traffic that matches the client IP address, MAC address, port, and VLAN combination obtained from the DHCP snooping binding table entry.

ip helper dhcp-snooping ip-source-filter {vlan *num* **| port** *slot/port***[-***port2***] | linkagg** *num***} {enable | disable}**

Syntax Definitions

vlan	The VLAN identification number (1–4094).
linkagg *num*	Specifies the link aggregate identification number.
*slot1/port1***[-***port1a***]**	Specifies the slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3). Use a hyphen to specify a range of ports (for example, 3/1-16).
enable	Enables IP source filtering for the specified port, link aggregation, or VLAN.
disable	Disables IP source filtering for the specified port, link aggregation, or VLAN level.

Defaults

By default, IP source filtering is disabled for a port or link aggregate, or VLAN.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Source filtering can be enabled only on the VLANs on which the DHCP Snooping is enabled.
- Source filtering can be enabled
  - on the ports that are associated with a VLAN on which DHCP Snooping is enabled.
  - on all the ports when DHCP Snooping is globally enabled for the switch.

Examples

```
-> ip helper dhcp-snooping ip-source-filter port 1/1 enable
-> ip helper dhcp-snooping ip-source-filter linkagg 2 enable
-> ip helper dhcp-snooping ip-source-filter vlan 10 enable
-> ip helper dhcp-snooping ip-source-filter vlan 20 disable
```

Release History

Release 6.4.4; command introduced.

Related Commands

show ip helper dhcp-snooping ip-source-filter	Displays the ports or VLANs on which IP source filtering is enabled.

MIB Objects

```
iphelperDhcpSnoopingPortIpSourceFiltering
   iphelperDhcpSnoopingPortIfIndex
   iphelperDhcpSourceFilterVlanNumber
   iphelperDhcpSourceFilterVlanFilteringStatus
```

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 6400, 6850E, 6855, 9000E

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 6.1.2; command introduced.

Related Commands

ip helper dhcp-snooping ip-source-filter	.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 6400, 6850E, 6855, 9000E

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 6.1.2; command introduced.

Related Commands

ip helper dhcp-snooping ip-source-filter	.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 dhcp-snooping binding persistency

Retains the entries in the DHCP Snooping binding table for the duration of the lease regardless of the existence of the MAC address in the MAC address table.

ip helper dhcp-snooping binding persistency {enable | disable}

Syntax Definitions

enable	Enables DHCP Snooping binding persistency.
disable	Disables DHCP Snooping binding persistency.

Defaults

By default, DHCP Snooping binding persistency is disabled.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- When this option is disabled, the client MAC address entry in the MAC table is removed. If the MAC address is missing from the MAC address table then the binding entry is removed.
- Use the **show ipv6 helper** command to display the current status.

Examples

```
-> ip helper dhcp-snooping binding persistency enable
-> ip helper dhcp-snooping binding persistency disable
```

Release History

Release 6.3.3; command introduced.

Related Commands

ip helper dhcp-snooping ip-source-filter	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.

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 6400, 6850E, 6855, 9000E

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 6.1; command introduced.
Release 6.4.3; command deprecated; use **ip interface dhcp-client**.

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 6400, 6850E, 6855, 9000E

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 6.1; command introduced.
Release 6.4.3; command deprecated; use **ip interface dhcp-client**.

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 (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 [*port_num* | *name***]} {vlan** *vlan_id* **| address** *ip_address***}**

no ip udp relay {BOOTP | NBDD | NBNSNBDD | DNS | TACACS | TFTP | NTP | port [*port_num* | *name***]} {vlan** *vlan_id* **| address** *ip_address***}**

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_num	Any number that is not a well-known port number.
name	Text string description up to 30 characters.
ip_address	IPv4 address of the configured UDP relay server.

Defaults

By default, relay is enabled on the BOOTP/DHCP well-known ports.

parameter	default
name	User Service number Other #

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to disable UDP Relay for the specified service port.
- Only one IP address can be configured per UDP 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 automatic IP configuration for VLAN 1, (Telnet and HTTP client authentication, and so on.) 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 address 125.254.34.1
-> ip udp 3047 “Generic Service”
-> no ip udp relay BOOTP
-> no ip udp relay 3047
```

Release History

Release 6.1; command introduced.
Release 6.4.5; **address** option added to command

Related Commands

ip udp relay vlan	Specifies the VLAN to which traffic from the specified UDP service port is forwarded.
show ip udp relay destination	Displays the VLAN assignments to which the traffic received on the specified UDP service port is forwarded.

MIB Objects

```
iphelperEntry
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 *port_num***} vlan** *vlan_id*

no ip udp relay {BOOTP | NBDD | NBNSNBDD | DNS | TACACS | TFTP | NTP | port *port_num***} 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 (for example, 1-5).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 is not supported.

Examples

```
-> ip udp relay DNS vlan 10
-> ip udp 3047 vlan 500
-> no ip udp relay DNS vlan 10
```

Release History

Release 6.1; command introduced.

Related Commands

ip udp relay	Enables or disables relay for UDP service ports.

MIB Objects

```
iphelperxPortServiceAssociationTable
   iphelperxPortServiceAssociationService
```

ipv6 helper address

Adds or deletes a DHCPv6 server address. DHCPv6 relay forwards DHCPv6 packets to and from the specified address. If multiple DHCPv6 servers are used, one IPv6 address must be configured for each server.

ipv6 helper address *ipv6_address*

ipv6 helper no address [*ipv6_address***]**

Syntax Definitions

ipv6_address	DHCPv6 server address (for example, 5001::6).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to delete an IPv6 address from the DHCPv6 Relay service. If an address is not specified, then all addresses are deleted.
- Using this command enables a Global DHCPv6 Relay service on the switch. When the DHCPv6 Relay is specified by the DHCPv6 server IPv6 address, the service is called Global DHCPv6 Relay.
- When the DHCPv6 Relay is specified by the VLAN number of the DHCPv6 request, the service is referred to as Per-VLAN DHCPv6. You can either configure Global DHCPv6 or Per-VLAN DHCPv6 but not noth together.
- UDPv6 Relay is automatically enabled on a switch when a DHCPv6 server IPv6 address is defined. There is no separate command for enabling or disabling the relay service.
- Configure DHCPv6 Relay on switches where packets are routed between IPv6 networks. You can configure up to 256 server IPv6 addresses for one relay service.

Example

```
-> ipv6 helper address 2001::5
-> ipv6 helper no address 3001::3
```

Release History

Release 6.4.5; command introduced.

Related Commands

ipv6 helper address	Configures an IPv6 address for an IPv6 interface on a VLAN, configured tunnel, or a 6to4 tunnel.
ipv6 helper address vlan	Configures DHCPv6 relay for the specified VLAN.
ipv6 helper maximum hops	Sets the maximum number of hops value for the DHCPv6 Relay configuration.
show ipv6 helper	Displays the current DHCPv6 Relay, Relay Agent information and DHCPv6 snooping configurations.

MIB Objects

```
ipv6helperTable
   ipv6helperForwAddr
```

ipv6 helper standard

Sets DHCPv6 Relay forwarding option to standard. All DHCPv6 packets are processed by a global relay.

ipv6 helper standard

Syntax Definitions

N/A

Defaults

By default, the DHCPv6 relay forwarding option is set to standard

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

All DHCPv6 packets are processed by a global relay. When the DHCPv6 Relay is specified by the DHCPv6 server, the service is called Global DHCPv6 Relay.

Example

```
-> ipv6 helper standard
```

Release History

Release 6.4.5; command introduced.

Related Commands

ipv6 helper per-vlan only	Sets the DHCPv6 Relay forwarding option to process only DHCPv6 packets received from a specific identified VLAN. This option allows each VLAN to have its own relay.
show ipv6 helper	Displays the current DHCPv6 Relay, Relay Agent information and DHCPv6 snooping configurations.

MIB Objects

```
ipv6helperTable
   ipv6helperForwardOption
```

ipv6 helper per-vlan only

Sets the DHCPv6 Relay forwarding option to process only DHCPv6 packets received from a specific identified VLAN. This option allows each VLAN to have its own relay.

ipv6 helper per-vlan only

Syntax Definitions

N/A

Defaults

By default, forwarding option is set to standard.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- When the forwarding option is set to Per-VLAN only, the standard (global) DHCPv6 relay service must not be active.
- Using the **per-vlan only** forwarding option requires you to specify a DHCPv6 server IPv6 address for each VLAN that provides a relay service. The **ipv6 helper address vlan** command performs this function and at the same time enables relay for the specified VLAN.

Example

```
-> ipv6 helper per-vlan only
```

Release History

Release 6.4.5; command introduced.

Related Commands

ipv6 helper address vlan	Configures DHCPv6 relay for the specified VLAN. This command can be used when a Per-VLAN only relay service is active on the switch.
show ipv6 helper	Displays current DHCPv6 Relay configuration information.

MIB Objects

```
ipv6helperTable
   ipv6helperForwardOption
```

ipv6 helper address vlan

Configures DHCPv6 relay for the specified VLAN. This command can be used when a Per-VLAN only relay service is active on the switch.

ipv6 helper address *ipv6_address* **vlan** *vlan_id*

ipv6 helper no address *ipv6_address* **vlan** *vlan_id*

Syntax Definitions

ipv6_address	DHCPv6 server IPv6 address (for example, 5001::6).
vlan_id	VLAN Identification number of per-VLAN

Defaults

If no VLAN identification number is entered, VLAN ID 0 is used by default

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to delete the DHCPv6 server VLAN from the DHCPv6 Relay.
- This command does not apply when using a standard relay service.
- Specifying multiple VLAN IDs or a range of VLAN IDs on the same command line is allowed.
- Use a hyphen to indicate a contiguous range and a space to separate multiple VLAN ID entries (for example, 10-15, 500-510, 850).
- The **ipv6 helper address vlan** command does not work if the **per-vlan only** forwarding option is not active. Use the **ipv6 helper per-vlan only** command to enable this option.
- The per-VLAN only relay service supports a maximum of 256 VLANs.

Example

```
-> ipv6 helper address 2001::5 vlan 100
-> ipv6 helper address 2001::5 vlan 100-105
-> ipv6 helper no address 2001::5 vlan 103
```

Release History

Release 6.4.5; command introduced.

Related Commands

ipv6 helper per-vlan only	Sets the DHCPv6 Relay forwarding option to process only DHCPv6 packets received from a specific identified VLAN. This option allows each VLAN to have its own relay.
show ipv6 helper	Displays the current DHCPv6 Relay, Relay Agent information and DHCPv6 snooping configurations.

MIB Objects

```
ipv6helperTable
   ipv6helperVlan
   ipv6helperStatus
```

ipv6 helper maximum hops

Sets the maximum number of hops value for the DHCPv6 Relay configuration.

ipv6 helper maximum hops *hops*

Syntax Definitions

hops	Maximum number of relays (1-32).

Defaults

By default, the maximum number of hops is set to 32.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- The **hops** value specifies the maximum number of relays a DHCPv6 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.
- If a packet contains a hop count equal to or greater than the **hops** value, DHCPv6 Relay discards the packet.

Example

```
-> ipv6 helper maximum hops 1
-> ipv6 helper maximum hops 12
```

Release History

Release 6.4.5; command introduced.

Related Commands

show ipv6 helper	Displays the current DHCPv6 Relay, Relay Agent information and DHCPv6 snooping configurations.

MIB Objects

```
ipv6helperTable
   ipv6helperMaxHops
```

ipv6 helper dhcp-snooping

Globally enables or disables DHCPv6 Snooping for the switch. When this feature is enabled, all DHCPv6 packets received on all switch ports are filtered.

ipv6 helper dhcp-snooping {enable | disable}

Syntax Definitions

enable	Enables DHCPv6 snooping for the switch.
disable	Disables DHCPv6 snooping for the switch.

Defaults

By default, this feature is disabled.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- If the DHCPv6 Snooping feature is globally enabled for the switch, then configuring snooping on a Per-VLAN basis is not allowed.
- If Per-VLAN based snooping is enabled, switch level snooping cannot be enabled.

Example

```
-> ipv6 helper dhcp-snooping enable
-> ipv6 helper dhcp-snooping disable
```

Related Commands

ipv6 helper address	Adds or deletes a DHCPv6 server address. DHCPv6 relay forwards DHCPv6 packets to and from the specified address.
show ipv6 helper	Displays the current DHCPv6 Relay, Relay Agent information and DHCPv6 snooping configurations.

Release History

Release 6.4.5; command introduced.

MIB Objects

```
ipv6helperTable
   ipv6helperDhcpSnooping
```

ipv6 helper dhcp-snooping vlan

Enables or disables DHCPv6 Snooping on a Per-VLAN basis. When this feature is enabled, all DHCPv6 packets received on ports associated with the VLAN are filtered.

ipv6 helper dhcp-snooping vlan *vlan_id*

no ipv6 helper dhcp-snooping vlan *vlan_id*

Syntax Definitions

vlan_id	VLAN Identification Number (1 to 4094).

Defaults

By default, DHCPv6 snooping is disabled.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to disable DHCPv6 Snooping for the specified VLAN.
- If the DHCPv6 Snooping feature is globally enabled for the switch, then configuring snooping on a Per-VLAN basis is not allowed.
- If per-VLAN based snooping is enabled for the switch, then DHCPv6 snooping cannot be enabled.

Example

```
-> ipv6 helper dhcp-snooping vlan 100
-> no ipv6 helper dhcp-snooping vlan 100
```

Release History

Release 6.4.5; command introduced.

Related Commands

show ipv6 helper dhcp-snooping vlan Displays a list of VLANs that have DHCPv6 Snooping enabled.

MIB Objects

```
ipv6helperDhcpSnoopingVlanTable
```

ipv6 helper dhcp-snooping port

Configures the DHCPv6 Snooping trust mode for the port. The trust mode determines if the port accepts all DHCPv6 traffic, blocks all DHCPv6 traffic, or accepts only client DHCPv6 traffic.

ipv6 helper dhcp-snooping port *slot / port1* [- *port 1a*] **{block | client-only-trusted | client-only-untrusted | trusted}**

Syntax Definitions

slot / port1 [- *port1a*]	Specifies the slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3). Use a hyphen to specify a range of ports (for example, 3/1-16).
block	Blocks all DHCPv6 traffic on the port.
client-only-trusted	Allows only DHCPv6 client traffic on the port along with the Relay forward message
client-only-untrusted	Allows only DHCPv6 client traffic on the port with DHCPv6 snooping enabled.
trusted	Allows all DHCPv6 traffic on the port. The port behaves as if DHCPv6 Snooping is not enabled.

Defaults

By default, the trust mode for a port is set to **client-only-untrusted** when the DHCPv6 Snooping feature is enabled for the switch or for a VLAN.

Usage Guidelines

- The DHCPv6 trust mode only applies when the DHCPv6 Snooping feature is enabled for the switch or for a VLAN.
- If DHCPv6 Snooping is enabled at the switch level, the trust mode applies to all switch ports.
- If DHCPv6 Snooping is enabled for a specific VLAN, then the trust mode applies to only those ports that are associated with that VLAN.
- Use the **show ipv6 helper dhcp-snooping port** command to display the current trust mode for a port and statistics regarding the number of packets dropped due to DHCPv6 Snooping violations.

Example

```
-> ipv6 helper dhcp-snooping port 1/24 trusted
-> ipv6 helper dhcp-snooping port 2/1-5 block
-> ipv6 helper dhcp-snooping port 4/7 client-only-untrusted
```

Release History

Release 6.4.5; command introduced.

Related Commands

show ipv6 helper dhcp-snooping port	Displays the trust mode and DHCPv6 Snooping violation statistics for all switch ports that are filtered by DHCPv6 Snooping.

Related MIB Objects

```
Ipv6helperDhcpSnoopingPortTable
   ipv6helperDhcpSnoopingPortEntry
   ipv6helperDhcpSnoopingPortIfIndex
   ipv6helperDhcpSnoopingPortTrustMode
```

ipv6 helper dhcp-snooping linkagg

Configures the DHCPv6 Snooping trust mode for the link aggregate. The trust mode determines if the link aggregate will accept all DHCPv6 traffic, block all DHCPv6 traffic, or accept only client DHCPv6 traffic.

ipv6 helper dhcp-snooping linkagg *num* **{block | client-only-trusted | client-only-untrusted | trusted}**

Syntax Definitions

num	Specifies the link aggregate ID number
block	Blocks all DHCPv6 traffic on the ports of the specified link aggregate.
client-only-trusted	Allows only DHCPv6 client traffic on the link aggregate ports along with the Relay forward message.
client-only-untrusted	Allows only DHCPv6 client traffic on the link aggregate ports with DHCPv6 snooping enabled.
trusted	Allows all DHCPv6 traffic on the link aggregate ports. The port behaves as if DHCPv6 Snooping was not enabled.

Defaults

By default, the trust mode for link aggregate is set to **client-only-untrusted** when the DHCPv6 Snooping feature is enabled for the switch or for a VLAN.

Usage Guidelines

- The DHCPv6 trust mode only applies when the DHCPv6 Snooping feature is enabled for the switch or for a VLAN.
- If DHCPv6 Snooping is enabled at the switch level, the trust mode applies to all link aggregates.
- If DHCPv6 Snooping is enabled for a specific VLAN, then the trust mode applies to only those link aggregates that are associated with that VLAN.
- Use the **show ipv6 helper dhcp-snooping port** command to display the current trust mode for link aggregate and statistics regarding the number of packets dropped due to DHCPv6 Snooping violations.

Example

```
-> ipv6 helper dhcp-snooping linkagg 1 trust
-> ipv6 helper dhcp-snooping linkagg 2 block
-> ipv6 helper dhcp-snooping linkagg 3 client-only-trusted
```

Release History

Release 6.4.5; command introduced.

Related Commands

show ipv6 helper dhcp-snooping port	Displays the trust mode and DHCPv6 Snooping violation statistics for all switch ports that are filtered by DHCPv6 Snooping.

MIB Objects

```
Ipv6helperDhcpSnoopingPortTable
   ipv6helperDhcpSnoopingPortEntry
   ipv6helperDhcpSnoopingPortIfIndex
   ipv6helperDhcpSnoopingPortTrustMode
```

ipv6 helper dhcp-snooping binding

Enables or disables the DHCPv6 Snooping binding table functionality. The binding table contains the link local address, IPv6 address, lease time, VLAN number, and the interface information that corresponds to a local untrusted port on the switch.

ipv6 helper dhcp-snooping binding [enable | disable]

Syntax Definitions

enable	Enables the creation of binding table entries.
disable	Disables the creation of binding table entries.

Defaults

By default, the binding table functionality is enabled when the DHCPv6 Snooping feature is enabled for the switch or for a VLAN.

Usage Guidelines

- 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.
- Dynamic binding table entries are created when the relay agent receives a DHCPv6 Reply packet.

Example

```
-> ipv6 helper dhcp-snooping binding disable
-> ipv6 helper dhcp-snooping binding enable
```

Release History

Release 6.4.5; command introduced.

Related Commands

show ipv6 helper dhcp-snooping binding	Displays the trust mode and DHCPv6 Snooping violation statistics for all switch ports that are filtered by DHCPv6 Snooping.

MIB Objects

```
ipv6helperDhcpSnoopingBindingTable
   ipv6helperDhcpSnoopingBindingStatus
```

ipv6 helper dhcp-snooping binding timeout

Configures the amount of time between each automatic save of the DHCPv6 Snooping binding table contents maintained in memory to a file on the switch. This functionality preserves binding table contents across switch reboots.

ipv6 helper dhcp-snooping binding timeout seconds

Syntax Definitions

seconds	The number of seconds (180 to 600) to wait before the next save.

Defaults

By default, timeout value is set to 300 seconds.

Usage Guidelines

- The timeout value is only valid if the DHCPv6 Snooping binding table functionality is enabled.
- The contents of the binding table are saved to the **dhcpv6bind.db** file in the **/flash/switch** directory.
- The **dhcpv6bind.db** file is time stamped when a save of the binding table contents is successfully completed.

Example

```
-> ipv6 helper dhcp-snooping binding timeout 600
-> ipv6 helper dhcp-snooping binding timeout 240
```

Release History

Release 6.4.5; command introduced.

Related Commands

show ipv6 helper	Displays the current DHCPv6 Relay, Relay Agent information and DHCPv6 snooping configurations.

MIB Objects

```
ipv6helperDhcpSnoopingBindingTable.
   ipv6helperDhcpSnoopingBindingDatabaseSyncTimeout
   ipv6helperDhcpSnoopingBindingDatabaseLastSyncTime
```

ipv6 helper dhcp-snooping binding action

Triggers a purge or renew action against the DHCPv6 Snooping binding table. A purge action clears the contents of the table. A renew action populates the table with entries saved in the DHCPv6 binding table.

ipv6 helper dhcp-snooping 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 **dhcpv6bind.db** file located in **/flash/switch** directory on the switch.

Defaults

N/A

Usage Guidelines

The DHCPv6 Snooping binding table is maintained in the switch memory. Binding table entries are saved on a periodic basis to the **dhcpv6bind.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 **dhcpv6bind.db** file.

Example

```
-> ipv6 helper dhcp-snooping binding action purge
-> ipv6 helper dhcp-snooping binding action renew
```

Release History

Release 6.4.5; command introduced.

Related Commands

N/A

MIB Objects

```
ipv6helperDhcpSnoopingBindingTable
   ipv6helperDhcpSnoopingBindingDatabaseAction
```

ipv6 helper dhcp-snooping binding persistency

Retains the entries in the DHCPv6 Snooping binding table for the duration of the lease, regardless of the existence of the MAC address in the MAC address table.

ipv6 helper dhcp-snooping binding persistency {enable | disable}

Syntax Definitions

enable	Enables DHCPv6 snooping binding persistency.
disable	Disables DHCPv6 snooping binding persistency.

Defaults

By default, DHCPv6 snooping binding persistency is disabled.

Usage Guidelines

- When this option is disabled, the client MAC address entry in the MAC table is removed. If the MAC address is missing from the MAC address table then binding entry will be removed.
- Use the **show ipv6 helper** command to display the current status.

Example

```
-> ipv6 helper dhcp-snooping binding persistency enable
-> ipv6 helper dhcp-snooping binding persistency disable
```

Release History

Release 6.4.5; command introduced.

Related Commands

show ipv6 helper	Displays the current DHCPv6 Relay, Relay Agent information and DHCPv6 snooping configurations.

MIB Objects

```
ipv6helperDhcpSnoopingBindingTable
   ipv6helperDhcpSnoopingBindingPersistencyStatus
```

ipv6 helper interface-id prefix

This command can be used to configure Interface ID manually.

ipv6 helper interface-id prefix *string*

ipv6 helper no interface-id prefix

Syntax Definitions

string	A user-defined text string upto 255 characters.

Defaults

- By default, **interface-id** option is added with value containing VLAN ID and Ifindex.
- When MCLAG is enabled, by default, **interface-id** option is added with value containing Chassis group ID, chassis ID, and Ifindex.

Usage Guidelines

When the **interface-id** prefix is configured, the user defined Interface ID is inserted into the relay-forward message.

Example

```
-> ipv6 helper interface-id prefix pool-1
-> ipv6 helper no interface-id prefix
```

Release History

Release 6.4.5; command introduced.

Related Commands

show ipv6 helper	Displays the current DHCPv6 Relay, Relay Agent information and DHCPv6 snooping configurations.

MIB Objects

```
ipv6helperTable
   ipv6helperInterfaceIdPrefixValue
```

ipv6 helper remote-id format

Configures the type of information that is inserted into the Remote ID suboption. The information is inserted into the Remote ID field in ASCII text string format.

ipv6 helper remote-id format { base-mac | system-name | vlan | user-string *string* **| interface-alias | auto-interface-alias | disable}**

ipv6 helper remote-id enterprise-number *num*

Syntax Definitions

base-mac	The base MAC address of the switch.
system-name	The system name of the switch.
vlan	The VLAN ID of which the client is a member.
string	A user-defined text string upto 64 characters to insert into the Remote ID ASCII field.
interface-alias	The alias configured for the interface.
auto-interface-alias	The switch automatically generates the interface-alias in the following format: *systemName_slot_port.*
enterprise-number	The vendor's registered enterprise number.
disable	Disable the Remote ID format and remove the enterprise-number configuration.

Defaults

By default, this feature is disabled.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Configuring the Remote ID suboption in ASCII format allows up to five types of information within the ASCII string. However, if the contents of all the fields combined exceed 127 characters, then the ASCII string is truncated.
- Enterprise number must be set before the Remote ID format
- Specifying at least one parameter with this command is required. If multiple parameters are selected, then one of the valid delimiter characters must be specified.
- For user-defined *string*, include ambiguous characters such as hex characters and spaces in quotes so that they are interpreted as text. For example, the string "Building B Server" requires quotes because of the spaces between the words.
- The **interface-alias** parameter uses the alias configured with the **interfaces alias** command. If no alias is configured, a NULL string is inserted.

- The Remote ID format option is a global setting; the format specified is applied to all ports on the switch.
- Both Enterprise-number and format is disabled when the **disable** option is used in the Remote ID format.

Example

```
-> ipv6 helper remote-id enterprise-number 5
-> ipv6 helper remote-id format interface-alias
-> ipv6 helper remote-id format user-string "Network XYZ"
```

Release History

Release 6.4.5; command introduced.

Related Commands

interfaces alias	Configures a description (alias) for a single port.
show ipv6 helper	Displays the current DHCPv6 Relay, relay agent information and DHCPv6 snooping configurations

MIB Objects

```
ipv6helperTable
   ipv6helperRemoteIdEnterpriseNumber
   ipv6helperRemoteIdUserStringValue
   ipv6helperRemoteIdFormatType
```

show ip helper

Displays the current DHCP Relay, Relay Agent Information, and DHCPSnooping configuration.

show ip helper

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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
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 Bypass Opt82-Check   =  Disabled,
  DHCP Snooping Opt82 Format  =  Base MAC,
  DHCP Snooping Opt82 String  =  00:d0:95:ae:3b:f6,
  DHCP Snooping Binding DB Status    =  Enabled,
      Database Sync Timeout          =  300,
      Database Last Sync Time        =  Mar 19 2007 14:32,
      Binding Persistency Status = Enabled
  PXE Support                        =  Disabled,
  Forward option     = standard
      Vlan Number NA
  Bootup Option Disable
      Forwarding Address :
        1.1.1.1
        21.2.2.10
        10.19.4.1
  UDP Relay on Default VRF = Enabled
```

The following example shows what the display output looks like when the DHCP Snooping feature is enabled and the Option-82 format is set to ASCII:

```
-> show ip helper
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 Opt82 ASCII Circuit ID Field1  =  Base MAC,
  DHCP Snooping Opt82 ASCII Circuit ID Field1 String  =  00:e0:b1:91:45:d0,
  DHCP Snooping Opt82 ASCII Circuit ID Field2  =  Cvlan,
  DHCP Snooping Opt82 ASCII Circuit ID Field2 String  =   - ,
  DHCP Snooping Opt82 ASCII Circuit ID Delimiter  =  "/",
  DHCP Snooping Opt82 ASCII Remote ID Field1  =  Vlan,
  DHCP Snooping Opt82 ASCII Remote ID Field1 String  =   - ,
  DHCP Snooping Opt82 ASCII Remote ID Field2  =  Cvlan,
  DHCP Snooping Opt82 ASCII Remote ID Field2 String  =   - ,
  DHCP Snooping Opt82 ASCII Remote ID Delimiter  =  " ",

  DHCP Snooping Binding DB Status    =  Enabled,
      Database Sync Timeout          =  300,
      Database Last Sync Time        =  Mar 19 2007 14:32,
      Binding Persistency Status = Enabled
  PXE Support                        =  Disabled,
  Forward option     = standard
      Vlan Number NA
  Bootup Option Disable
      Forwarding Address :
        1.1.1.1
        21.2.2.10
        10.19.4.1
  UDP Relay on Default VRF = Enabled
```

output definitions

Forward Delay	The current forward delay time (default is three seconds). Use the **ip helper forward delay** command to change this value.
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.

output definitions

Relay Agent Information Policy	The current policy action (**Drop**, **Keep**, **Replace**) applied to DHCP packets that contain an Option-82 field. Configured through the **ip helper agent-information policy** command. Note that this field only appears when the DHCP relay agent information Option-82 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 Snooping Bypass Opt82-Check	Indicates whether or not an Option-82 check is performed for DHCP packets ingressing on untrusted ports (**Enabled** or **Disabled**). Configured through the **ip helper dhcp-snooping option-82 format ascii circuit-id** command.
DHCP Snooping Opt82 Format	The type of information (base MAC address for the switch, system name for the switch, user-defined text, or interface alias) that the switch will insert into the Option-82 suboption when Option-82 data insertion is enabled for the switch. Configured through the **ip helper dhcp-snooping option-82 format** command.
DHCP Snooping Opt 82 String	The user-defined text inserted into the Option-82 field when data insertion is enabled and a string format for the data is specified. Configure through the **ip helper dhcp-snooping option-82 format** command.
DHCP Snooping Opt82 Format = ASCII	Indicates that the switch will insert Option-82 information into the Circuit ID suboption as an ASCII text string. Configured through the **ip helper dhcp-snooping option-82 format ascii circuit-id** command.
DHCP Snooping Opt82 ASCII Field1	If the Option-82 format is set to ASCII, this field contains the type of information that the switch will insert into the Option-82 Circuit ID suboption. This field only displays when the Option-82 format is set to ASCII. The Circuit ID suboption may contain up to five ASCII text strings; a separate field is displayed for each type of string that is configured. Configured through the **ip helper dhcp-snooping option-82 format ascii circuit-id** command.

output definitions

DHCP Snooping Opt82 ASCII Field1 String	The value of the ASCII text string that is inserted into the Option-82 Circuit ID suboption field. This field only displays when the Option-82 format is set to ASCII. The Circuit ID suboption may contain up to five ASCII text strings; a separate field is displayed for each string that is configured.Configured through the **ip helper dhcp-snooping option-82 format ascii circuit-id** command.
DHCP Snooping Opt82 ASCII Delimiter	The character that is used to separate multiple ASCII text strings inserted into the Option-82 Circuit ID suboption. This field only displays when more than one ASCII text string is configured for the Circuit ID suboption. Configured through the **ip helper dhcp-snooping option-82 format ascii circuit-id** command.
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 **dhcpBinding.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.
Binding Persistency Status	Indicates whether or not the DHCP snooping binding table retains entries with MAC addresses that were cleared from the MAC address table (**Enabled** or **Disabled**). Configured through the **ip helper dhcp-snooping binding persistency** command.
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 6.1; command introduced.
Release 6.1.2; new fields added for DHCP Option 82 and DHCP Snooping features.
Release 6.1.3; new field added for global DHCP traffic suppression feature.
Release 6.1.5; **Traffic Suppression** field deprecated; new **DHCP Snooping Bypass Opt82-Check** field added.
Release 6.3.1; **DHCP Snooping Opt82 Format** and **DHCP Snooping Opt82 String** fields added.
Release 6.3.3; **Binding Persistency Status** field added.
Release 6.4.3; **DHCP Snooping Opt82 Format ASCII** fields added.

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
iphelperAgentInformation
iphelperAgentInformationPolicy
iphelperDhcpSnooping
iphelperDhcpSnoopingOpt82DataInsertionStatus
iphelperDhcpSnoopingMacAddressVerificationStatus
iphelperDHCPSnoopingBypassOpt82CheckStatus
iphelperDhcpSnoopingOption82FormatType
iphelperDhcpSnoopingOption82StringValue
iphelperDhcpSnoopingOption82FormatASCIIField1
iphelperDhcpSnoopingOption82FormatASCIIField1StringValue
iphelperDhcpSnoopingOption82FormatASCIIField2
iphelperDhcpSnoopingOption82FormatASCIIField2StringValue
iphelperDhcpSnoopingOption82FormatASCIIField3
iphelperDhcpSnoopingOption82FormatASCIIField3StringValue
iphelperDhcpSnoopingOption82FormatASCIIField4
iphelperDhcpSnoopingOption82FormatASCIIField4StringValue
iphelperDhcpSnoopingOption82FormatASCIIField5
iphelperDhcpSnoopingOption82FormatASCIIField5StringValue
iphelperDhcpSnoopingOption82FormatASCIIDelimiter
iphelperDhcpSnoopingBindingStatus
iphelperDhcpSnoopingBindingDatabaseSyncTimeout
iphelperDhcpSnoopingBindingDatabaseLastSyncTime
iphelperDhcpSnoopingVlanTable
   iphelperDhcpSnoopingVlanNumber
   iphelperDhcpSnoopingVlanMacVerificationStatus
   iphelperDhcpSnoopingVlanOpt82DataInsertionStatus
iphelperStatTable
   iphelperBootupOption
   iphelperBootupPacketOption
```

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 6400, 6850E, 6855, 9000E

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 =         12, Delta =         12,
    Forw Delay Violation :
      Total Count =          3, Delta =          3,
    Max Hops Violation :
      Total Count =          0, Delta =          0,
    Agent Info Violation :
      Total Count =          0, Delta =          0,
    Invalid Gateway IP :
      Total Count =          0, Delta =          0,
    Invalid Agent Info From Server :
      Total Count =          0, Delta =          0,
 Server Specific Statistics :
    Server  5.5.5.5
        Tx Server :
          Total Count =          9, Delta =      9
```

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.
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.
Agent Info Violation	Number of packets dropped as a result of a relay agent information (Option-82) violation. A violation occurs if an Option-82 DHCP packet contains a zero gateway IP address (giaddr) and the relay agent information policy is set to **Drop** or a DHCP packet has no Option-82 field and contains a non-zero giaddr.
Invalid Gateway IP	Number of packets dropped as a result of a gateway IP violation. A violation occurs if an Option-82 DHCP packet contains a gateway IP address (giaddr) that matches a local subnet address.
Invalid Agent Info From Server	Number of invalid Option-82 DHCP server packets dropped by the relay agent.
Delta	Total number of packets processed since the last time the **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 6.1; command introduced.
Release 6.1.2; new fields added.

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 6400, 6850E, 6855, 9000E

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 6.1.2; command 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 6400, 6850E, 6855, 9000E

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        IP Src    Opt82       MAC      Server     Relay    Binding
Port      Mode       Filtering Violation  Violation  Violation  Violation Violation
-----+-------------+----------+----------+----------+----------+---------|---------
1/1        Blocked    Disabled      0          0          0          0        0
1/2    Client-Only    Enabled       0          0          0          0        0
1/3    Client-Only    Enabled       0          0          0          0        0
1/4    Client-Only    Enabled       0          0          0          0        0
1/5    Client-Only    Enabled       0          0          0          0        0
1/6        Blocked    Disabled      0          0          0          0        0
1/7    Client-Only    Enabled       0          0          0          0        0
1/8    Client-Only    Enabled       0          0          0          0        0
1/9    Client-Only    Enabled       0          0          0          0        0
1/10       Trusted    Disabled      0          0          0          0        0
1/11       Trusted    Disabled      0          0          0          0        0
1/12       Trusted    Disabled      0          0          0          0        0
```

output definitions

Slot/Port	The slot number for the module and the physical port number on that module (for example, 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.
IP Src Filtering	Indicates whether or not IP source filtering is enabled for the port (**Enabled** or **Disabled**). Configured through the **ip helper dhcp-snooping port ip-source-filtering** 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 6.1.2; command 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
   iphelperDhcpSnoopingPortIpSourceFiltering
   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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **ip helper dhcp-snooping ip-source-filter** 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           Slot        IP          Lease    VLAN     Binding
     Address         Port      Address       Time      ID       Type
------------------+------+--------------+---------+-------+-----------
00:ae:22:e4:00:08    1/4    10.255.11.23     2000      5      Dynamic
10:fe:a2:e4:32:08    2/15   10.255.91.53     2000      2      Dynamic
```

output definitions

MAC Address	The MAC address of the client.
Slot/Port	The slot/port designation for the switch port that received the DHCP request
IP Address	The IP address offered by the DHCP server.
Lease Time	The IP address lease time assigned by the DHCP server. A value of 0 indicates a static entry.
VLAN ID	The VLAN ID of the VLAN to which the client belongs.
Binding Type	Indicates whether the binding table entry is **dynamic** or **static**. Static entries are created using the **ip helper dhcp-snooping ip-source-filter** command.

Release History

Release 6.1.2; command 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 6400, 6850E, 6855, 9000E

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 (NBNS/NBDD, DNS, and so on.).

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 6.1; command 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 6400, 6850E, 6855, 9000E

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 (NBNS/NBDD, DNS, and so on.).

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 6.1; command 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 6400, 6855, 6850E, 9000E

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 (NBNS/NBDD, DNS, and so on.).

Examples

```
-> show ip udp relay destination

Service          Port     VLANs           Server IP Address
---------------+--------+---------------+------------
BOOTP            67
DNS              53       2  4
TACACS           65       3

-> show ip udp relay destination dns

Service          Port     VLANs       Server IP Address
---------------+--------+------------+---------------
DNS              53       2  4
```

```
-> show ip udp relay destination
 Service              Port  Vlans          Server Address
--------------------+-----+--------------+---------------
 1:BOOTP              68
 8:OTHER1             5001                 10.168.58.21
```

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.
Server Address	The Server IPv4 address assigned to the port

Release History

Release 6.1; command 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
```

dhcp-server

Enables, disables, or restarts the DHCP server operation.

dhcp-server {enable | disable | restart}

Syntax Definitions

enable	Enables operation status of the DHCP server.
disable	Disables operation status of the DHCP server.
restart	Restarts the DHCP Server.

Defaults

The DHCP server is disabled by default.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Restart the DHCP server after making changes to the *dhcpd.conf* file.

Examples

```
-> dhcp-server enable
-> dhcp-server disable
-> dhcp-server restart
```

Release History

Release 6.4.3; command introduced.

Related Commands

show dhcp-server statistics	Displays the DHCP Server lease statistics.

MIB Objects

```
alaDhcpSrvGlobalConfigStatus
alaDhcpSrvGlobalRestart
```

clear dhcp-server statistics

Clears the packet counters of dhcp-server statistics.

clear dhcp-server statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use this command to clear the packet counters of dhcp-server statistics.

Examples

```
-> clear dhcp-server statistics
```

Release History

Release 6.4.3; command introduced.

Related Commands

show dhcp-server statistics	Displays the DHCP Server lease statistics.

MIB Objects

N/A

show dhcp-server leases

Displays the leases offered by the DHCP server.

show dhcp-server leases [*ip_address* **|** *mac_address***] [type {static | dynamic}]**

Syntax Definitions

ip_address	Specifies IP address of the interface configured with DHCP server.
mac_address	Specifies MAC address of the interface configured with DHCP server.
static	Displays only static leases.
dynamic	Displays only dynamic leases.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

DHCP server should be enabled first before using this command.

Examples

```
-> show dhcp-server leases

IP address     MAC address      Lease Granted           Lease Expiry     Type
-------------+-----------------+-------------------+-------------------+---------
10.255.91.53  10:fe:a2:e4:32:08  2010-01-16 11:38:47 2010-01-17 11:38:47 Dynamic
10.255.91.55  20:fe:a2:e4:32:08  2010-01-16 10:30:00 2010-01-18 10:30:00 Static
10.255.91.58  20:fe:a2:e4:34:08 2010-01-16 10:30:00 2010-01-18 10:30:00 Dynamic

-> show dhcp-server leases ipaddr 10.255.91.53

IP address   MAC address        Lease Granted        Lease Expiry     Type
------------+-----------------+-------------------+-------------------+---------
10.255.91.53 10:fe:a2:e4:32:08 2010-01-16 11:38:47  2010-01-17 11:38:47 Dynamic

-> show dhcp-server leases type static

IP address   MAC address        Lease Granted        Lease Expiry     Type
------------+-----------------+-------------------+-------------------+---------
10.255.91.55 20:fe:a2:e4:32:08 2010-01-16 10:30:00   2010-01-18 10:30:00   Static
```

output definitions

IP address	The IP address allocated to the client.
MAC address	The MAC address of the client for which the lease is allocated.

output definitions (continued)

Lease Granted	The date and time at which lease is granted.
Lease Expiry	The date and time at which lease expires.
Type	The type of lease offered.

Release History

Release 6.4.3; command introduced.

Related Commands

clear dhcp-server statistics	Clears the DHCP Server lease statistics.

MIB Objects

```
alaDhcpSrvLeaseTable
   alaDhcpSrvLeaseMACAddress
   alaDhcpSrvLeaseIpAddress
   alaDhcpSrvLeaseLeaseGrant
   alaDhcpSrvLeaseLeaseExpiry
   alaDhcpSrvLeaseType
```

show dhcp-server statistics

Displays the statistics of the DHCP server.

show dhcp-server statistics [packets | hosts | subnets | all]

Syntax Definitions

packets	Displays general statistical information along with specific information about data packets received, dropped and transmitted.
hosts	Displays general statistical information along with specific information about hosts related to all the subnets.
subnets	Displays general statistical information along with specific information about all the subnets.
all	Displays all statistical information related to the DHCP server.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

DHCP server should be enabled first before using this command.

Examples

```
-> Show dhcp-server stats all
General stats:
  DHCP Server Name: mample.example.com
  DHCP Server Status: Enabled
  Total Subnets Managed: 7
  Total Subnets Used: 0
  Total Subnets Unused: 7
  Total Subnets Full: 0
  DHCP Server System Up Time: TUE DEC 29 07:52:37.35120
  Sync time: 0
  Last sync time: 0
  Next sync time: 0

Packet stats:
  Total DHCP Discovers: 0
  Total DHCP Offers: 0
  Total DHCP Requests: 0
  Total DHCP Request Grants: 0
  Total DHCP Request Renews: 0
  Total DHCP Declines: 0
  Total DHCP Acks: 0
  Total DHCP Nacks: 0
```

```
    Total DHCP Releases: 0
    Total DHCP Informs: 0
    Total Bootp requests: 0
    Total Bootp response: 0
    Total Unknown packets: 0

  Leases stats:
    Total:
      Hosts Managed: 633
      Hosts used: 0
      Hosts unused: 633
      Hosts Pending: 0
      Hosts unavailable: 0

    Static DHCP:
      Hosts Managed: 0
      Hosts used: 0
      Hosts unused: 0
      Hosts Pending: 0
      Hosts unavailable: 0

    Dynamic DHCP:
      Hosts Managed: 633
      Hosts used: 0
      Hosts unused: 633
      Hosts Pending: 0
      Hosts unavailable: 0

    Automatic DHCP:
      Hosts Managed: 0
      Hosts used: 0
      Hosts unused: 0
      Hosts Pending: 0
      Hosts unavailable: 0

    Static Bootp:
      Hosts Managed: 0
      Hosts used: 0
      Hosts unused: 0
      Hosts Pending: 0
      Hosts unavailable: 0

    Automatic Bootp:
      Hosts Managed: 0
      Hosts used: 0
      Hosts unused: 0
      Hosts Pending: 0
      Hosts unavailable: 0
```

```
Subnets stats:
  Subnet: 200.0.0.0
    Total: 4
    Static DHCP: 0
    Dynamic DHCP: 4
    Automatic DHCP: 0
    Static Bootp: 0
    Automatic Bootp: 0
    Ranges:
    Range: 200.0.0.10 to 200.0.0.11 Mask: 255.255.255.0 Type: 5
           Unused: 2; Used: 0; Pending: 0; Unavailable: 0

  Subnet: 220.0.0.0
    Total: 62
    Static DHCP: 0
    Dynamic DHCP: 62
    Automatic DHCP: 0
    Static Bootp: 0
    Automatic Bootp: 0
    Ranges:
        Range: 220.0.0.100 to 220.0.0.130 Mask: 255.255.255.0 Type: 5
              Unused: 2; Used: 0; Pending: 0; Unavailable: 0
```

output definitions

General stats	Denotes General DHCP Server statistics.
Name	Specifies the name assigned to the DHCP Server.
Status	Specifies up or down status of the DHCP Server.
Total subnets used	Specifies the total number of subnets being used.
Total subnets managed	Specifies the total number of subnets being managed by the DHCP server.
Total subnets unused	Specifies the total number of subnets being unused
Total subnets full	Specifies the total number of subnets wherein all of the IP addresses are used.
DHCP Server System Up Time	Shows the DHCP Server System Up Time Performance Monitor counter.
Sync time	Specifies the time for DHCP server to contact and synchronize with the designated time server
Last sync time	Specifies the last time the synchronization occured.
Next sync time	Specifies the next time the synchronization should be scheduled.
Packet stats	Denotes statististical information about the data packet transmission
Total DHCP Discovers	Specifies the total number of DHCPDISCOVER packets sent by the clients to the DHCP server.
Total DHCP Offers	Specifies the total number of DHCPOFFER packets sent by the server to the clients.
Total DHCP Requests	Specifies the total number of DHCPREQUEST packets sent by the clients in response to the DHCPOFFER packets.
Total DHCP Request Grants	Specifies the total number of DHCP request grants provided by the server to the clients.

output definitions (continued)

Total DHCP Request Renews	Specifies the total number of DHCP lease renew requests sent by the clients to the DHCP server.
Total DHCP Declines	Specifies the total number of DHCP requests declined by the DHCP server.
Total DHCP Acks	Specifies the total number of DHCPACK acknowledgement packets sent by the DHCP server to the clients.
Total DHCP Nacks	Specifies the total number of DHCP Negative acknowledgements sent from the DHCP server to the clients. The DHCPNACK message is sent when all the IP addresses available to the server are exhausted and the client sends a DHCPREQUEST.
Total DHCP Releases	Specifies the total number of DHCPRELEASE packets sent by the DHCP server to release IP addresses from its clients.
Total DHCP Informs	Specifies the total number of DHCPINFORM packets sent by the clients to obtain DHCP options from the DHCP server.
Total Bootp requests	Specifies the total number of BOOTP requests sent by the clients to the DHCP server.
Total Bootp response	Specifies the total number of BOOTP response packets sent by the DHCP server to the clients.
Total Unknown packets	Specifies the total number of unknown or badly formatted DHCP packets received by the DHCP server.
Leases stats	Denotes statististical information about leases provided by the DHCP server.
Hosts Managed	Specifies the total number of clients managed by the DHCP server.
Hosts used	Specifies the total number of clients using the IP addresses provided by the DHCP server.
Hosts unused	Specifies the total number of clients managed by the DHCP server which are not being used.
Hosts Pending	Specifies the total number of DHCP IP address requests which are pending by the DHCP server.
Hosts unavailable	Specifies the total number of DHCP hosts which are unavailable i.e; whose lease period have expired.
Static DHCP	Denotes statististical information about the hosts configured with Static DHCP.
Automatic DHCP	Denotes statististical information about the hosts configured with Automatic DHCP.
Static BootP	Denotes statististical information about the hosts configured under Static BootP. **Note:** BootP Relay is disabled when DHCP server is enabled on the switch.
Automatic BootP	Denotes statististical information about the hosts configured with Automatic BootP.
Subnet statistics	Denotes all DHCP related statististical information for individual subnets.
Range	Specifies the range of IP addresses in the individual subnet

output definitions (continued)

Mask	Specifies the subnet mask
Type	Specifies whether the type of IP address allocation is dynamic or Static.

Release History

Release 6.4.3; command introduced.

Related Commands

clear dhcp-server statistics	Clears the DHCP Server lease statistics.

MIB Objects

N/A

show ip helper dhcp-snooping ip-source-filter

Displays the ports or VLANs on which IP source filtering is enabled.

show ip helper dhcp-snooping ip-source-filter {vlan | port}

Syntax Definitions

vlan	Displays the VLANs on which IP source filtering is enabled.
port	Displays the ports on which IP source filtering is enabled.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The show output displays only those ports or VLANs on which IP source filtering is enabled.
- This command also displays the status of the link aggregate ports when source filtering is enabled at VLAN or port level.

Examples

```
-> show ip helper dhcp-snooping ip-source-filter port
Slot   IP Src
Port  Filtering
------+-----------
1/7    Enabled
1/12   Enabled
```

output definitions

Slot/Port	Specifies the slot and port number.
IP Src Filtering	Specifies if IP source filtering status. **Enabled** or **Disabled**.

```
-> show ip helper dhcp-snooping ip-source-filter vlan
Vlan   IP Src Filtering
------+-----------
 10    Enabled
 11    Enabled
 12    Enabled
 13    Enabled
```

output definitions

Vlan	VLAN number.
IP Src Filtering	Specifies if IP source filtering status. **Enabled** or **Disabled**.

Release History

Release 6.4.4; command introduced.

Related Commands

ip helper dhcp-snooping ip-source-filter	Enables or disables the IP source filtering at a port, link aggregation, or VLAN level.

MIB Objects

```
iphelperDhcpSnoopingPortIpSourceFiltering
   iphelperDhcpSnoopingPortIfIndex
   iphelperDhcpSourceFilterVlanNumber
   iphelperDhcpSourceFilterVlanFilteringStatus
```

show ipv6 helper

Displays the current DHCPv6 Relay, Relay Agent information and DHCPv6 snooping configurations.

show ipv6 helper

Syntax Definitions

N/A

Defaults

N/A

Usage Guidelines

Displays information for all IPv6 server addresses configured

Example

```
-> show ipv6 helper
IPv6 helper :
  Max number of hops     = 32,
  DHCPV6 Snooping Status               =  Disabled,
  DHCPV6 Snooping Remote-id            =  Enabled,
  DHCPV6 Snooping Interface-id Prefix =  OS6,
  DHCPv6 Snooping Binding DB Status = Enabled,
  Database Sync Timeout = 300,
  Database Last Sync Time = Mar 19 2012 14:32,
  Binding Persistency Status = Enabled
  Forward option = standard
  Vlan Number:
  2001::5
```

output definitions

Ipv6 helper	Specifies the configured IPv6 helper address.
Max number of hops	Specifies the maximum number of hops configured.
DHCPv6 Snooping Status	Specifies DHCPv6 snooping status **Switch-Level Enabled** or **Switch-Level Disabled, VLAN-Level Enabled**
DHCPv6 Snooping Binding DB Status	Specifies DHCPv6 Snooping Binding DB Status **Enabled,** or **Disabled**
Database Sync Timeout	Specifies the assigned Database Sync Timeout
Database Last Sync Time	Specifies the last time, database synchronization was performed on the switch in date tiem and year format.
Binding Persistency Status	Specifies if Binding Persistency Status **Enabled** or **Disabled**
Forward option	Specifies the configured Forwarding option - **Standard** or **per-vlan only**

output definitions

Vlan Number	Specifies the assigned VLAN Numbers in **per-vlan only** mode.
Forwarding Address	Specifies the assigned Forwarding Address

Release History

Release 6.4.5; command introduced.

Related Commands

ipv6 helper address	Adds or deletes a DHCPv6 server address. DHCPv6 relay forwards DHCPv6 packets to and from the specified address.
ipv6 helper standard	Sets DHCPv6 Relay forwarding option to standard. All DHCPv6 packets are processed by a global relay.
ipv6 helper per-vlan only	Sets the DHCPv6 Relay forwarding option to process only DHCPv6 packets received from a specific identified VLAN.
ipv6 helper address vlan	Configures DHCPv6 relay for the specified VLAN.
ipv6 helper maximum hops	Sets the maximum number of hops value for the DHCPv6 Relay configuration.
ipv6 helper dhcp-snooping	Globally enables or disables DHCPv6 Snooping for the switch. When this feature is enabled, all DHCPv6 packets received on all switch ports are filtered.
ipv6 helper dhcp-snooping binding	Enables or disables the DHCPv6 Snooping binding table functionality.
ipv6 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.
ipv6 helper dhcp-snooping binding persistency	Retains the entries in the DHCPv6 Snooping binding table for the duration of the lease, regardless of the existence of the MAC address in the MAC address table.

MIB Objects

```
ipv6helperTable
   ipv6helperForwAddr
   ipv6helperForwardOption
   ipv6helperMaxHops
   ipv6helperDhcpSnooping
ipv6helperDhcpSnoopingBindingTable
   ipv6helperDhcpSnoopingBindingStatus
   ipv6helperDhcpSnoopingBindingDatabaseSyncTimeout
   ipv6helperDhcpSnoopingBindingDatabaseLastSyncTime
   ipv6helperDhcpSnoopingBindingPersistencyStatus
```

show ipv6 helper stats

Displays the IPv6 helper statistics information.

show ipv6 helper stats

ipv6 helper no stats

Syntax Definitions

N/A

Defaults

N/A

Usage Guidelines

- Use the **no** form of this command to clear the DHCPv6 relay statistics
- The number of packets DHCPv6 Relay has received, the number of packets dropped due to 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 DHCPv6 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.

Example

```
-> show ipv6 helper stats
Global Statistics :
    Reception From Client :
      Total Count =          0, Delta =          0,
    Max Hops Violation :
      Total Count =          0, Delta =          0,
 Server Specific Statistics :
    Server  2001::1
        Tx Server :
          Total Count =      0, Delta =          0
```

output definitions

Global Statistics	Specifies Global DHCPv6 statistics
Reception From Client	Specifies statistics of data reception from Client. **Total Count** and **Delta.**
Max Hops Violation	Specifies Max Hops Violation statistics **Total Count** and **Delta**
Server Specific Statistics	Server details and Server Specific Statistics 5001::5
Tx Server	Specifies Tx Server details **Total Count** and **Delta.**

Release History

Release 6.4.5; command introduced.

Related Commands

ipv6 helper address	Displays the DHCPv6 Relay statistics.
ipv6 helper address vlan	Configures DHCPv6 relay for the specified VLAN. This command is used when a per-VLAN only relay service is active on the switch.
ipv6 helper standard	Sets DHCPv6 Relay forwarding option to standard. All DHCPv6 packets are processed by a global relay.
ipv6 helper per-vlan only	Sets the DHCPv6 Relay forwarding option to process only DHCPv6 packets received from a specific identified VLAN. This option allows each VLAN to have its own relay.
ipv6 helper maximum hops	Sets the maximum number of hops value for the DHCPv6 Relay configuration.

MIB Objects

```
ipv6helperTable
   ipv6helperForwAddr
   ipv6helperForwardOption
   ipv6helperMaxHops
   ipv6helperVlan
   ipv6helperStatus
```

show ipv6 helper dhcp-snooping vlan

Displays a list of VLANs that have DHCPv6 Snooping enabled.

show ipv6 helper dhcp-snooping vlan

Syntax Definitions

N/A

Defaults

N/A

Usage Guidelines

- This command only applies if DHCPv6 snooping is enabled at VLAN level.
- Use **show ipv6 helper** command to determine the status of DHCPv6 snooping at the switch level

Example

```
-> show ipv6 helper dhcp-snooping vlan
VLAN ID  Status
----------------
1       Enabled
2       Enabled
100     Disabled
200     Disabled
```

output definitions

VLAN ID	Specifies all the configured VLAN IDs
Status	Specifies whether DHCPv6 snooping binding is **Enabled** or **Disabled** on the related VLAN.

Release History

Release 6.4.5; command introduced.

Related Commands

ipv6 helper dhcp-snooping vlan	Enables or disables DHCPv6 Snooping on a Per-VLAN basis.

MIB Objects

```
ipv6helperDhcpSnoopingVlanTable
   ipv6helperDhcpSnoopingVlanNumber
    ipv6helperDhcpSnoopingVlanStatus
```

show ipv6 helper dhcp-snooping port

Displays the trust mode and DHCPv6 Snooping violation statistics for all switch ports that are filtered by DHCPv6 Snooping.

show ipv6 helper dhcp-snooping port

Syntax Definitions

N/A

Defaults

N/A

Usage Guidelines

- If DHCPv6 Snooping is operating at the switch level, then information for all switch ports is displayed.
- If DHCPv6 Snooping is operating at the VLAN level, then information for only those ports that are associated with a DHCPv6 Snooping VLAN is displayed

Example

```
-> show ipv6 helper dhcp-snooping port
 Slot      Trust             Client     Server     Binding   Interface-id
 Port      Mode             Violation  Violation  Violation   Violation
------+--------------------+----------+----------+----------+-------------
 1/1  Client-Only-UnTrusted       0          0          0          0
 1/2  Client-Only-UnTrusted       0          0          0          0
 1/3  Client-Only-UnTrusted       0          0          0          0
 1/4  Client-Only-UnTrusted       0          0          0          0
 1/5  Client-Only-UnTrusted       0          0          0          0
```

output definitions

Slot/Port	Specifies Slot/Port of DHCPv6 snooping port
Trust Mode	Specifies Trust Mode configured on the DHCPv6 snooping port. The different types of modes are - **Client-Only-Trusted**, **Client-Only-Untrusted, Trusted, Blocked**
Client Violation	Specifies the number of Client Violations on the DHCPv6 snooping port.
Server Violation	Specifies the number of Server Violations on the DHCPv6 snooping port.
Binding Violation	Specifies the number of Binding Violations on the DHCPv6 snooping port.
Interface-id Violation	Specifies the number of Interface Id Violations on the DHCPv6 snooping port.

Release History

Release 6.4.5; command introduced.

Related Commands

ipv6 helper interface-id prefix	This command can be used to configure Interface ID manually.
ipv6 helper dhcp-snooping port	Configures the DHCPv6 Snooping trust mode for the port.
ipv6 helper dhcp-snooping linkagg	Configures the DHCPv6 Snooping trust mode for the link aggregate.
ipv6 helper dhcp-snooping binding	Enables or disables the DHCPv6 Snooping binding table functionality.

MIB Objects

```
ipv6helperTable
   ipv6helperInterfaceIdPrefixValue
ipv6helperDhcpSnoopingPortTable
   ipv6helperDhcpSnoopingPortEntry
   ipv6helperDhcpSnoopingPortIfIndex
   ipv6helperDhcpSnoopingPortTrustMode
```

show ipv6 helper dhcp-snooping binding

Displays the contents of DHCPv6 Snooping binding table (database)

show ipv6 helper dhcp-snooping binding

Syntax Definitions

N/A

Defaults

N/A

Usage Guidelines

Dynamic binding table entries are created when the relay agent receives a DHCPv6 REPLY packet.

Example

```
-> show ipv6 helper dhcp-snooping binding

   Link-local            Slot       IPv6           Valid      VLAN
     Address             Port       Address        LifeTime    ID
------------------------+------+----------------+----------+-----
fe80::200:ff:fe00:101     1/4        2300::5         2000      5
fe80::200:16ff:fe0e:a785  2/15       4001::2         2000      2
```

Example output with remote flag when Multi Chassis Mode is enabled

```
-> show ipv6 helper dhcp-snooping binding

Total Number of Binding Entries: 11

Link-local              Slot    IPv6              Valid       VLAN       Remote
Address                 Port    Address           LifeTime     ID        Entry
----------------------+------+----------------+----------+----------+-----------
fe80::200:ff:fe00:101    3/2   2001:1001:21::1c8   360        1109      Local
fe80::200:16ff:fe0e:a785 3/2   2001:1001:21::18a   360        1109      Local
fe80::200:16ff:fe0e:a786 3/2   2001:1001:21::1e8   360        1109      Local
fe80::200:16ff:fe0e:a787 3/2   2001:1001:21::13c   360        1109      Local
```

output definitions

Link-local address	Specifies the IPv6 Address configured for DHCPv6 Snooping Binding
Slot/Port	Specifies the Slot and Port on which DHCPv6 Snooping Binding is configured
IPv6 Address	Specifies the forwarding IPv6 address specified by the **ipv6 helper address** command
Valid LifeTime	Specifies the valid binding lease life time.

output definitions

VLAN ID	Specifies the VLAN IDs on which DHCPv6 snooping binding is active.
Remote Entry	This column is available only when Multi-Chassis mode is active. Specifies the chassis through which the Binding entries are learned. Options that can be displayed are - **Remote** (if entry learned from remote chassis), **Local** (if entry learned from local chassis).

Release History

Release 6.4.5; command introduced.

Related Commands

ipv6 helper dhcp-snooping binding	Enables or disables the DHCPv6 Snooping binding table functionality.
ipv6 helper dhcp-snooping binding action	Triggers a purge or renew action against the DHCPv6 Snooping binding table. A purge action clears the contents of the table. A renew action populates the table with entries saved in the DHCPv6 binding table.
ipv6 helper dhcp-snooping binding persistency	Retains the entries in the DHCPv6 Snooping binding table for the duration of the lease, regardless of the existence of the MAC address in the MAC address table.

MIB Objects

```
ipv6helperDhcpSnoopingBindingTable
   ipv6helperDhcpSnoopingBindingStatus
   ipv6helperDhcpSnoopingBindingDatabaseAction
   ipv6helperDhcpSnoopingBindingPersistencyStatus
```

26 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/VRRP3 routers on the LAN. The VRRP/VRRP3 router, which controls the IP/IPv6 address associated with a virtual router is called the master router, and forwards packets to that IP/IPv6 address. If the master router becomes unavailable, the highest priority backup router will transition to the master state. The Alcatel-Lucent implementation of VRRP also supports the collective management of virtual routers on a switch.

Note. VRRP3 does not support the collective management functionality.

The VRRP and VRRP3 commands comply with RFC 2787 and RFC 3768, respectively.

MIB information is as follows:

Filename: IETF-VRRP.MIB
Module: VRRP-MIB

Filename: AlcatelIND1VRRP.MIB
Module: ALCATEL-IND1-VRRP-MIB

Filename: AlcatelIND1VRRP3.MIB
Module: ALCATEL-IND1-VRRP3-MIB

The VRRP CLI commands are listed here:

vrrp
vrrp address
vrrp track
vrrp track-association
vrrp trap
vrrp delay
vrrp interval
vrrp priority
vrrp preempt
vrrp all
vrrp set
vrrp group
vrrp group all
vrrp group set
vrrp group-association
vrrp3
vrrp3 address
vrrp3 trap
vrrp3 track-association
show vrrp
show vrrp statistics
show vrrp track
show vrrp track-association
show vrrp group
show vrrp group-association
show vrrp3
show vrrp3 statistics
show vrrp3 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***]**

no vrrp *vrid vlan_id*

Syntax Definitions

vrid	The virtual router ID, in the range from 1–255.
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. The valid range is 1–255 seconds.

Defaults

parameter	default
enable | disable | on | off	**disable** (**off**)
priority	100
preempt | no preempt	**preempt**
seconds	1

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a virtual router from the configuration.
- Use the **vrrp address** command to configure an IP address for the virtual router. This must be done before the virtual router can be enabled.
- To disable the virtual router, rather than to 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 can be modified.

Important information about configuring priority:

- A value of 255 indicates that the VRRP router owns the IP address; that is, 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. If the priority is set to 255 and the virtual router is not the IP address owner, then the priority will be set to the default value of 100. 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 6.1; command was introduced.

Related Commands

vrrp address	Configures an IP address for a virtual router.
show vrrp	Displays the virtual router configuration for all virtual routers or for a specific virtual router.

MIB Objects

```
alaVrrp3OperTable
   alaVrrp3OperAdminState
   alaVrrp3OperPriority
   alaVrrp3OperPreemptMode
   alaVrrp3OperAdvertisementinterval
   alaVrrp3OperRowStatus
```

vrrp address

Configures an IP address for a virtual router.

vrrp *vrid vlan_id* **address** *ip_address*

vrrp *vrid vlan_id* **no address** *ip_address*

Syntax Definitions

vrid	The virtual router ID, in the range from 1–255.
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 6850E, 6855, 9000E

Usage Guidelines

A virtual router IP address must be configured before the virtual router can be enabled.

Examples

```
-> vrrp 1 3 address 10.10.3.2
-> vrrp 1 3 no address 10.10.3.2
```

Release History

Release 6.1; command was introduced.
Release 6.1.3; command modified; *ip* parameter is replaced by *address* parameter.

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 about VRRP packets for all virtual routers configured on the switch or for a specific virtual router.

MIB Objects

```
alaVrrp3AssoIpAddrTable
   alaVrrp3AssoIpAddrRowStatus
```

vrrp track

Creates a new tracking policy or modifies an existing tracking policy.

vrrp track *track_id* **[enable | disable] [priority** *value***] [ipv4-interface** *name* | **ipv6-interface** *name* **| port** *slot/port* **| address** *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. The valid range is 0–255.
name	The name of the IPv4 or IPv6 interface that this policy will track.
slot/port	The slot/port number that this policy will track.
address	The remote IP or IPv6 address that this policy will track.

Defaults

parameter	default
enable | disable	**enable**
value	25

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a tracking policy.
- Use the **disable** option to disable the tracking policy, rather than removing it from the switch.

Examples

```
-> vrrp track 2 enable priority 50 ipv4-interface Marketing
-> vrrp track 3 enable priority 60 ipv6-interface Sales
-> vrrp track 3 disable
```

Release History

Release 6.1; command was introduced.
Release 6.1.3; *ip* parameter is replaced by *address* parameter.

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
   alaVrrpTrackState
   alaVrrpTrackAdminState
   alaVrrpTrackPriority
   alaVrrpTrackEntityType
   alaVrrpTrackEntityVlan
   alaVrrpTrackEntityPort
   alaVrrpTrackEntityIpAddress
   alaVrrpTrackEntityIpv6Interface
   alaVrrpTrackEntityInterface
   alaVrrpTrackRowStatus
```

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.
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 6850E, 6855, 9000E

Usage Guidelines

Use the **no** form of this 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 6.1; 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 track-association	Displays the tracking policies associated with virtual routers.

MIB Objects

```
alaVrrpAssoTrackTable
   alaVrrpAssoTrackId
   alaVrrpTrackRowStatus
```

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 6850E, 6855, 9000E

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 6.1; command was introduced.

Related Commands

snmp trap filter	Enables or disables SNMP trap filtering.

MIB Objects

```
vrrpOperGroup
   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 6850E, 6855, 9000E

Usage Guidelines

Use this command to prevent loss of workstation connectivity before a virtual router becomes master.

Examples

```
-> vrrp delay 50
```

Release History

Release 6.1; 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 specific virtual router.

MIB Objects

```
alaVRRPStartDelay
```

vrrp interval

Modifies the default advertising interval value assigned to the virtual routers on the switch.

vrrp interval *seconds*

Syntax Definitions

seconds	The default advertising interval for the virtual routers. The valid range is 1–255 seconds.

Defaults

parameter	default
seconds	1

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Modifying the default advertising interval value will affect the value assigned by default to any new virtual routers that are created.
- To apply the new default value to the existing virtual routers, you must first disable the virtual routers, then apply the new default value using **vrrp set** command and enable the virtual routers again.
- If any of the virtual routers are running with their own configured value or group value, then that value will take priority over the new default value. To override the configured value with the new default value, you must first disable the virtual routers, then override the configured value using the **vrrp set** command with the **override** option and enable the virtual routers again.

Examples

```
-> vrrp interval 50
```

Release History

Release 6.3.1; command was introduced.

Related Commands

vrrp all	Changes the administrative status of all the virtual routers on the switch.
vrrp set	Sets the new default parameter values to existing virtual routers on the switch.
show vrrp	Displays the virtual router configuration for all virtual routers or for a specific virtual router.

MIB Objects

```
alaVrrpv2Config
   alaVrrpDefaultInterval
```

vrrp priority

Modifies the default priority value assigned to the virtual routers on the switch.

vrrp priority *priority*

Syntax Definitions

priority	The default priority value for the virtual routers. The valid range is 1–254.

Defaults

parameter	default
priority	100

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Modifying the default priority value will affect the value assigned by default to any new virtual routers that are created.
- To apply the new default value to the existing virtual routers, you must first disable the virtual routers, then apply the new default value using the **vrrp set** command and enable the virtual routers again.
- If any of the virtual routers are running with their own configured value or group value, then that value will take priority over the new default value. To override the configured value with the new default value, you must first disable the virtual routers, then override the configured value using the **vrrp set** command with the **override** option and enable the virtual routers again.

Examples

```
-> vrrp priority 50
```

Release History

Release 6.3.1; command was introduced.

Related Commands

vrrp all	Changes the administrative status of all the virtual routers on the switch.
vrrp set	Sets the new default parameter values to existing virtual routers on the switch.
show vrrp	Displays the virtual router configuration for all virtual routers or for a specific virtual router.

MIB Objects

```
alaVrrpv2Config
   alaVrrpDefaultPriority
```

vrrp preempt

Modifies the default preempt mode assigned to the virtual routers on the switch.

vrrp [preempt | no preempt]

Syntax Definitions

preempt	Specifies that a higher priority router may preempt a lower priority master router by default.
no preempt	Specifies that a higher priority router may not preempt a lower priority master router by default.

Defaults

parameter	default
preempt | no preempt	**preempt**

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Modifying the default preempt mode will affect the mode assigned by default to any new virtual routers that are created.
- To apply the new default value to the existing virtual routers, you must first disable the virtual routers, then apply the new default value using the **vrrp set** command and enable the virtual routers again.
- If any of the virtual routers are running with their own configured value or group value, then that value will take priority over the new default value. To override the configured value with the new default value, you must first disable the virtual routers, then override the configured value using the **vrrp set** command with the **override** option and enable the virtual routers again.

Examples

```
-> vrrp preempt
-> vrrp no preempt
```

Release History

Release 6.3.1; command was introduced.

Related Commands

vrrp all	Changes the administrative status of all the virtual routers on the switch.
vrrp set	Sets the new default parameter values to existing virtual routers on the switch.
show vrrp	Displays the virtual router configuration for all virtual routers or for a specific virtual router.

MIB Objects

```
alaVrrpv2Config
   alaVrrpDefaultPreemptMode
```

vrrp all

Changes the administrative status of all the virtual routers on the switch.

vrrp [disable | enable | enable all]

Syntax Definitions

disable	Disables all the virtual routers on the switch.
enable	Enables the virtual routers that have not previously been disabled individually or collectively via the **vrrp group all** command.
enable all	Enables all the virtual routers on the switch including those virtual routers that have been disabled individually or collectively via the **vrrp group all** command.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- This command changes the administrative status of all the virtual routers on the switch by executing a single command.
- This command will not affect the ability to change the administrative status of an individual virtual router.

Examples

```
-> vrrp disable
-> vrrp enable
-> vrrp enable all
```

Release History

Release 6.3.1; command was introduced.

Related Commands

vrrp interval	Modifies the default advertising interval value assigned to the virtual routers on the switch.
vrrp priority	Modifies the default priority value assigned to the virtual routers on the switch.
vrrp preempt	Modifies the default preempt mode assigned to the virtual routers on the switch.
vrrp set	Sets the new default parameter values to existing virtual routers on the switch.
show vrrp	Displays the virtual router configuration for all virtual routers or for a specific virtual router.

MIB Objects

```
alaVrrpv2Config
   alaVrrpAdminState
```

vrrp set

Sets the new default parameter values to existing virtual routers on the switch.

vrrp set [interval | priority | preempt | all] [override]

Syntax Definitions

interval	Sets the VRRP advertisement interval value to the new default value.
priority	Sets the priority value to the new default value.
preempt	Sets the preempt mode to the new default mode.
all	Sets all the parameters value to the new default value.
override	Overrides the specified parameters configured value with the new default value.

Defaults

parameter	default
interval | priority | preempt | all	**all**

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- All the virtual routers must be disabled before using this command.
- To apply the new default value to the existing virtual routers, you must first disable the virtual routers, then apply the new default value using the **vrrp set** command and enable the virtual routers again.
- If any of the virtual routers are running with their own configured value or group value, then that value will take priority over the new default value. To override the configured value with the new default value, you must first disable the virtual routers, then override the configured value using the **vrrp set** command with the **override** option and enable the virtual routers again.

Examples

```
-> vrrp set priority
-> vrrp set priority override
```

Release History

Release 6.3.1; command was introduced.

Related Commands

vrrp interval	Modifies the default advertising interval value assigned to the virtual routers on the switch.
vrrp priority	Modifies the default priority value assigned to the virtual routers on the switch.
vrrp preempt	Modifies the default preempt mode assigned to the virtual routers on the switch.
vrrp all	Changes the administrative status of all the virtual routers on the switch.
show vrrp	Displays the virtual router configuration for all virtual routers or for a specific virtual router.

MIB Objects

```
alaVrrpv2Config
   alaVrrpSetParam
   alaVrrpOverride
```

vrrp group

Creates a new virtual router group or modifies the configuration parameters of an existing virtual router group.

vrrp group *vrgid* **[interval** *seconds***] [priority** *priority***] [preempt | no preempt]**

no vrrp group *vrgid*

Syntax Definitions

vrgid	The virtual router group ID, in the range from 1–255.
seconds	The default advertising interval for the virtual router group. The valid range is 1–255 seconds.
priority	The default priority value for the virtual router group. The valid range is 1–254.
preempt	Specifies that a higher priority router may preempt a lower priority master router by default.
no preempt	Specifies that a higher priority router may not preempt a lower priority master router by default.

Defaults

parameter	default
seconds	1
priority	100
preempt | no preempt	**preempt**

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete the virtual router group.
- The configuration parameters can be modified at any time, but will not have any effect on the virtual routers in the group until the virtual routers are enabled again. To apply the group default value to the virtual routers in a group, you must first disable the virtual router group, then apply the group default value using the **vrrp group set** command and enable the virtual router group again.
- If any of the virtual routers in the group are running with their configured value, then that value will take priority over the new default value. To override the configured value with the new default value, you must first disable the virtual router group, then override the configured value by using the **vrrp group set** command with the **override** option and enable the virtual router group again.
- When a virtual router group is deleted, the virtual routers assigned to the group become unassigned. However, this does not have any impact on the virtual routers.

Examples

```
-> vrrp group 25 interval 50 priority 50 no preempt
-> no vrrp group 25
```

Release History

Release 6.3.1; command was introduced.

Related Commands

vrrp group all	Changes the administrative status of all the virtual routers in a virtual router group using a single command.
vrrp group set	Sets the new modified default value to all the virtual routers in a virtual router group.
vrrp group-association	Adds a virtual router to a virtual router group.
show vrrp group	Displays the default parameter values for all the virtual router groups or a specific virtual router group.

MIB Objects

```
alaVrrpGroupTable
   alaVrrpGroupInterval
   alaVrrpGroupPriority
   alaVrrpGroupPreemptMode
   alaVrrpGroupRowStatus
```

vrrp group all

Changes the administrative status of all the virtual routers in a virtual router group using a single command.

vrrp group *vrgid* **[disable | enable | enable all]**

Syntax Definitions

vrgid	The virtual router group ID, in the range from 1–255.
disable	Disables all the virtual routers in the group.
enable	Enables those virtual routers that have not previously been disabled individually in the group.
enable all	Enables all the virtual routers in the group including those virtual routers that have been disabled individually.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- If a virtual router in a group is disabled on an individual basis, it can only be reenabled by using the **enable all** option in this command.
- This command will not affect the ability to change the administrative status of an individual virtual router.

Examples

```
-> vrrp group 25 disable
-> vrrp group 25 enable
-> vrrp group 25 enable all
```

Release History

Release 6.3.1; command was introduced.

Related Commands

vrrp group	Creates a new virtual router group or modifies the configuration parameters of an existing virtual router group.
vrrp group set	Sets the new modified default value to all the virtual routers in a virtual router group.
show vrrp	Displays the virtual router configuration for all virtual routers or for a specific virtual router.
show vrrp group	Displays the default parameter values for all the virtual router groups or a specific virtual router group.

MIB Objects

```
alaVrrpGroupTable
   alaVrrpGroupAdminState
```

vrrp group set

Sets the new modified default value to all the virtual routers in a virtual router group.

vrrp group *vrgid* **set [interval | priority | preempt | all] [override]**

Syntax Definitions

vrgid	The virtual router group ID, in the range from 1–255.
interval	Sets the VRRP advertisement interval value to the new default value.
priority	Sets the priority value to the new default value.
preempt	Sets the preempt mode to the new default mode.
all	Sets all the parameters' value to the new default value.
override	Overrides the parameter's configured value with the group default value.

Defaults

parameter	default
interval | priority | preempt | all	**all**

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- All the virtual routers must be disabled before using this command.
- To apply the group default value to the virtual routers in a group, you must disable the virtual router group, then apply the group default value using the **vrrp group set** command and enable the virtual router group again.
- If any of the virtual routers in the group are running with their own configured parameter value, then that value will take priority over the group default value. To override the configured value with the group default value, you must first disable the virtual router group, then override the configured value by using the **vrrp group set** command with the **override** option and enable the virtual router group again.

Examples

```
->vrrp group 10 set priority
->vrrp group 10 set priority override
```

Release History

Release 6.3.1; command was introduced.

Related Commands

vrrp group	Creates a new virtual router group or modifies the configuration parameters of an existing virtual router group.
vrrp group all	Changes the administrative status of all the virtual routers in a virtual router group using a single command.
show vrrp	Displays the virtual router configuration for all virtual routers or for a specific virtual router.
show vrrp group	Displays the default parameter values for all the virtual router groups or a specific virtual router group.

MIB Objects

```
alaVrrpGroupTable
   alaVrrpGroupSetParam
   alaVrrpGroupOverride
```

vrrp group-association

Adds a virtual router to a virtual router group.

vrrp *vrid vlan_id* **group-association** *vrgid*

vrrp *vrid vlan_id* **no group-association** *vrgid*

Syntax Definitions

vrid	The virtual router ID, in the range from 1–255.
vlan_id	The VLAN on which the virtual router is configured. The VLAN must already be created and available on the switch.
vrgid	The virtual router group ID, in the range from 1–255.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove the virtual router from the virtual router group.
- A virtual router need not be disabled in order to be added to a virtual router group. However, the virtual router will not adopt the group's default parameter values until it is reenabled.
- A virtual router need not be disabled to be removed from a group.

Examples

```
-> vrrp 25 1 group-association 10
-> vrrp 25 1 no group-association 10
```

Release History

Release 6.3.1; command was introduced.

Related Commands

show vrrp group-association	Displays the virtual routers that are associated with a group.

MIB Objects

```
alaVrrpAssoGroupTable
   alaVrrpAssoGroupRowStatus
```

vrrp3

Configures a new VRRP3 virtual router or modifies an existing one. Used to enable or disable a virtual router.

vrrp3 *vrid vlan_id* **[enable | disable | on | off] [priority** *priority***] [preempt | no preempt][accept | no accept] [[advertising] interval** *centiseconds***]**

no vrrp3 *vrid vlan_id*

Syntax Definitions

vrid	The virtual router ID, in the range from 1–255.
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.
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.
accept	Specifies that the master router, which is not the IPv6 address owner will accept the packets addressed to the IPv6 address owner as its own.
no accept	Specifies that the master router, which is not the IPv6 address owner will not accept the packets addressed to the IPv6 address owner as its own.
centiseconds	The interval in centiseconds after which the master router will send VRRP3 advertisements. The advertising interval must be the same for all VRRP3 routers configured with the same VRID. The valid range is 1–4096 centiseconds.

Defaults

parameter	default
enable | disable | on | off	**disable (off)**
priority	100
preempt | no preempt	**preempt**
accept | no accept	**accept**
centiseconds	100

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a virtual router from the configuration.
- Use the **vrrp3 address** command to configure an IPv6 address for the virtual router.
- To disable the virtual router, rather than to remove it, use the **disable** or **off** option. Note that the **disable** or **off** options cannot be used with any other optional parameter.
- A virtual router must be disabled before it can be modified.
- The maximum number of virtual routers supported is based on the 100 centisecond interval. A smaller interval will result in a relatively lesser number of virtual routers.
- The advertising interval cannot be less than 10 centiseconds.

Examples

```
-> vrrp3 23 1 priority 75
-> vrrp3 23 1 enable
```

Release History

Release 6.1.3; command was introduced.

Related Commands

vrrp3 address	Configures an IPv6 address for a virtual router.
show vrrp3	Displays the virtual router configuration for all virtual routers or for a specific virtual router.

MIB Objects

alaVrrp3OperTable

- alaVrrp3OperAdminState
- alaVrrp3OperPriority
- alaVrrp3OperPreemptMode
- alaVrrp3OperAcceptMode
- alaVrrp3OperAdvinterval
- alaVrrp3OperRowStatus

vrrp3 address

Configures an IPv6 address for a virtual router.

vrrp3 *vrid vlan_id* **address** *ipv6_address*

vrrp3 *vrid vlan_id* **no address** *ipv6_address*

Syntax Definitions

vrid	The virtual router ID, in the range from 1–255.
vlan_id	The VLAN on which the virtual router is configured.
address	The virtual IPv6 address associated with the specified virtual router.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> vrrp3 1 3 address 213:100:1::56
-> vrrp3 1 3 no address 213:100:1::56
```

Release History

Release 6.1.3; command was introduced.

Related Commands

vrrp3	Configures a new VRRP3 virtual router or modifies an existing one. Used to enable or disable a virtual router.
show vrrp3 statistics	Displays statistics for all virtual routers configured on the switch or for a specific virtual router.

MIB Objects

```
alaVrrp3AssoIpAddrTable
   alaVrrp3AssoIpAddrRowStatus
```

vrrp3 trap

Enables or disables SNMP traps for VRRP3.

vrrp3 trap

no vrrp3 trap

Syntax Definitions

N/A

Defaults

By default, SNMP traps for VRRP3 are enabled.

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

SNMP traps must be enabled globally on the switch for VRRP3 traps to actually be sent.

Examples

```
-> vrrp3 trap
-> no vrrp3 trap
```

Release History

Release 6.1.3; command was introduced.

Related Commands

snmp trap filter	SNMP traps must be enabled with this command.

MIB Objects

```
alaVrrp3OperGroup
   alaVrrp3NotificationCntl
```

vrrp3 track-association

Associates a VRRP3 tracking policy with a virtual router.

vrrp3 *vrid vlan_id* **track-association** *track_id*

vrrp3 *vrid vlan_id* **no track-association** *track_id*

Syntax Definitions

vrid	The virtual router ID, in the range from 1–255.
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 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a tracking policy from a virtual router.
- Use the **vrrp track** command to create a tracking policy for an IPv6 interface.

Examples

```
-> vrrp3 2 4 track-association 1
-> vrrp3 2 4 no track-association 1
```

Release History

Release 6.1.3; command was introduced.

Related Commands

vrrp3	Configures a new VRRP3 virtual router or modifies an existing one. Used to enable or disable a virtual router.
show vrrp3 track-association	Displays the tracking policies associated with VRRP3 virtual routers.

MIB Objects

```
alaVrrp3AssoTrackTable
   alaVrrp3AssoTrackId
   alaVrrp3TrackRowStatus
```

show vrrp

Displays the virtual router configuration for all virtual routers or for a specific virtual router.

show vrrp [*vrid***]**

Syntax Definitions

vrid	The virtual router ID, in the range from 1–255.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

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 default advertisement interval: 5 seconds
VRRP default priority: 99
VRRP default preempt: No
VRRP trap generation: Enabled
VRRP startup delay: 45  (expired)

                IP         Admin                       Adv.
VRID VLAN   Address(es)    Status  Priority Preempt Interval
----+----+--------------+--------+--------+-------+--------
   1  101 192.60.245.240  Enabled        99      No        5
   2  102 192.60.246.240  Enabled        99      No        5

-> show vrrp 1
Virtual Router VRID = 1 on VLAN = 1
   Admin Status       = Enabled
   Priority           = 255
   Preempt            = Yes
   Adv. Interval      = 1
   Virtual MAC        = 00-00-5E-00-02-01
   IP Address(es)
      192.168.170.1
      192.168.170.2
```

output definitions

VRRP default advertisement interval	The default advertising interval for all virtual routers on the switch.
VRRP default priority	The default priority value for all virtual routers on the switch.
VRRP default preempt	The default preempt mode for all virtual routers on the switch.
VRRP trap generation	Indicates whether or not the VRRP trap generation is enabled or disabled; configured through the **vrrp track** 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 address** 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 26-3.
Preempt	Controls whether a higher priority virtual router will preempt a lower priority master router: 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. The first 5 bytes are always 00-00-5E-00-02. 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 6.1; command was introduced.
Release 6.3.1; **VRRP default advertisement interval**, **VRRP default priority**, and **VRRP default preempt** fields added.

Related Commands

vrrp	Configures a new VRRP virtual router or modifies an existing one. Used to enable or disable a virtual router.
vrrp address	Configures an IP address for a virtual router.
vrrp interval	Modifies the default advertising interval value assigned to the virtual routers on the switch.
vrrp priority	Modifies the default priority value assigned to the virtual routers on the switch.
vrrp preempt	Modifies the default preempt mode assigned to the virtual routers on the switch.
show vrrp statistics	Displays statistics for all virtual routers configured on the switch or for a specific virtual router.

MIB Objects

```
alaDispVrpp3Config
   alaVRRPDefaultInterval
   alaVRRPDefaultPriority
   alaVRRPDefaultPreemptMode
   alaVrrp3AssoIpAddr
   alaVrrp3OperAdminState
   alaVrrp3OperPriority
   alaVrrp3OperPreemptMode
   alaVrrp3OperAcceptMode
```

show vrrp statistics

Displays statistics about VRRP packets for all virtual routers configured on the switch or for a specific virtual router.

show vrrp [*vrid***] statistics**

Syntax Definitions

vrid	The virtual router ID, in the range from 1–255.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

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             44
  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 operational state of the VRRP router instance; **initialize** specifies that the interface or VLAN is either disabled or down, or if the startup delay timer has not expired; **backup** specifies that this instance is monitoring the availability of the master router; **master** specifies 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
   Advertisements received              = 0
   Type errors                          = 0
   Advertisement interval errors        = 0
   Authentication errors                = 0
   IP TTL errors                        = 0
   IP address list errors               = 0
   Packet length 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 operational state of this VRRP router instance; **initialize** specifies that the interface or VLAN is either disabled or down, or the startup delay timer has not expired; **backup** specifies that this instance is monitoring the availability of the master router; **master** specifies 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 differs from the one configured for the virtual router.
Authentication errors	The total number of VRRP packets received with an unknown or invalid authentication type.
IP TTL errors	The total number of VRRP packets received with a TTL value other than 255.

output definitions (continued)

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.
Packet length errors	The total number of VRRP packets received with a length less than the length of the VRRP header.
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 6.1; 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 specific virtual router.

MIB Objects

```
   alaVrrp3RouterChecksumErrors
   alaVrrp3RouterVersionErrors
   alaVrrp3RouterVrIdErrors
alaVrrp3RouterStatsTable
   alaVrrp3StatsBecomeMaster
   alaVrrp3StatsAdvertiseRcvd
   alaVrrp3StatsAdvIntervalErrors
   alaVrrp3StatsIpTtlErrors
   alaVrrp3StatsPriZeroPktsRcvd
   alaVrrp3StatsPriZeroPktsSent
   alaVrrp3StatsInvalidTypePktsRcvd
   alaVrrp3StatsAddressListErrors
   alaVrrp3StatsInvldAuthType
   alaVrrp3StatsPacketLengthErrors
alaVrrp3OperTable
   alaVrrp3OperUpTime
   alaVrrp3OperGroup
   alaVrrp3OperState
```

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 6850E, 6855, 9000E

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	Indicates 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 6.1; command was introduced.

Related Commands

vrrp track	Creates a new tracking policy or modifies an existing tracking policy.

MIB Objects

```
alaVRRPTrackTable
   alaVrrpTrackState
   alaVrrpTrackAdminState
   alaVrrpTrackPriority
   alaVrrpTrackEntityType
   alaVrrpTrackEntityVlan
   alaVrrpTrackEntityPort
   alaVrrpTrackEntityIpAddress
   alaVrrpTrackEntityIpv6Interface
   alaVrrpTrackEntityInterface
```

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.
track_id	The ID of the tracking policy for which you want to display information.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

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.
Admin State	The administrative state of the tracking policy configured through the **vrrp track** command.

output definitions (continued)

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 6.1; 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

```
alaVrrpAssoTrackTable
   alaVrrpAssoTrackId
alaVRRPTrackTable
   alaVrrpTrackState
   alaVrrpTrackAdminState
   alaVrrpTrackPriority
   alaVrrpTrackEntityType
   alaVrrpTrackEntityVlan
   alaVrrpTrackEntityPort
   alaVrrpTrackEntityIpAddress
   alaVrrpTrackEntityInterface
```

show vrrp group

Displays the default parameter values for all the virtual router groups or for a specific virtual router group.

show vrrp group [*vrgid***]**

Syntax Definitions

vrgid	The virtual router group ID, in the range from 1–255.

Defaults

By default, the default parameter values are displayed for all the virtual router groups.

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

Use the *vrgid* parameter with this command to display the default values for a specific virtual router group.

Examples

```
-> show vrrp group 2
Virtual Router Group GROUPID = 2
  Interval = 11
  Priority = 250
  Preempt Mode = Yes
  3 Associated Virtual Routers
```

output definitions

Group ID	The virtual router group identifier.
Adv Interval	Indicates the time interval, in seconds, between the sending of advertisement messages. Only the master router sends advertisements.
Priority	Indicates the VRRP router's priority for the virtual router group. For more information about priority, see the **vrrp** command description on page 26-3.
Preempt Mode	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.

Release History

Release 6.3.1; command was introduced.

Related Commands

vrrp group	Creates a new virtual router group or modifies the configuration parameters of an existing virtual router group.
vrrp group all	Changes the administrative status of all the virtual routers in a virtual router group using a single command.

MIB Objects

```
alaVrrpGroupTable
   alaVrrpGroupInterval
   alaVrrpGroupPriority
   alaVrrpGroupPreemptMode
```

show vrrp group-association

Displays the virtual routers that are associated with a group.

show vrrp group-association [*vrgid***]**

Syntax Definitions

vrgid	The virtual router group ID, in the range from 1–255.

Defaults

By default, all virtual router group associations are displayed.

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

Use the *vrgid* parameter with this command to display the association details of a specific virtual router group.

Examples

```
-> show vrrp group-association 2
GROUPID VRID  VLAN
-------+----+-----+
    2     3      2
          4      2
          5      2
```

output definitions

GROUPID	The virtual router group identifier.
VRID	The virtual router identifier.
VLAN	The VLAN associated with the VRRP instance. Configured through the **vrrp** command.

Release History

Release 6.3.1; command was introduced.

Related Commands

vrrp group-association	Adds a virtual router to a virtual router group.

MIB Objects

```
alaVrrpAssoGroupTable
   alaVrrp3OperVrId
```

show vrrp3

Displays the virtual router configuration for all virtual routers or for a specific virtual router.

show vrrp3 [*vrid***]**

Syntax Definitions

vrid	The virtual router ID, in the range from 1–255.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

Use the **show vrrp3** command to display information about configuration parameters, which may be set through the **vrrp3** command. Use the **show vrrp3 statistics** command to get information about VRRP3 packets.

Examples

```
-> show vrrp3
VRRP trap generation: Enabled
VRRP startup delay: 45  (expired)

                                      Admin                              Adv.
VRID VLAN     IPv6 Address(es)        Status  Priority Preempt Accept Interval
----+----+--------------------------+--------+--------+-------+------+--------
  1  101    fe80::200:5eff:fe00:201  Enabled    200      No    Yes      100
            1010::30
  2  102    fe80::200:5eff:fe00:202  Enabled    200      No    Yes      100
            1020::30
  3  103    fe80::200:5eff:fe00:203  Enabled    200      No    Yes      100
            1030::30
  4  104    fe80::200:5eff:fe00:204  Enabled    200      No    Yes      100
            1040::30
  5  105    fe80::200:5eff:fe00:205  Enabled    200      No    Yes      100
            1050::30
  6  106    fe80::200:5eff:fe00:206  Enabled    200      No    Yes      100
            1060::30
  7  107    fe80::200:5eff:fe00:207  Enabled    200      No    Yes      100
            1070::30
  8  108    fe80::200:5eff:fe00:208  Enabled    200      No    Yes      100
            1080::30
  9  109    fe80::200:5eff:fe00:209  Enabled    200      No    Yes      100
            1090::30
 10  110    fe80::200:5eff:fe00:20a  Enabled    200      No    Yes      100
            1100::30
```

output definitions

VRRP trap generation	Whether or not VRRP trap generation is enabled or disabled.
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.
VRID	Virtual router identifier. Configured through the **vrrp3** command.
VLAN	The VLAN associated with the VRRP3 instance. Configured through the **vrrp3** command.
IPv6 Address(es)	The assigned IPv6 addresses. Configured through the **vrrp3 address** 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 VRRP3 router's priority for the virtual router. For more information about priority, see the **vrrp3** command description on page 26-30.
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.
Accept	Displays whether the master router, which is not the IPv6 address owner will accept the packets addressed to the IPv6 address owner as its own.
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-00-02. 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 6.1.3; command was introduced.

Related Commands

vrrp3	Configures a new VRRP3 virtual router or modifies an existing one. Used to enable or disable a virtual router.
vrrp3 address	Configures an IPv6 address for a virtual router.
show vrrp3 statistics	Displays statistics for all virtual routers configured on the switch or for a specific virtual router.

MIB Objects

```
alaVrrp3OperTable
   alaVrrp3OperAdminState
   alaVrrp3OperPriority
   alaVrrp3OperPreemptMode
   alaVrrp3OperAcceptMode
   alaVrrp3OperAdvinterval
```

show vrrp3 statistics

Displays statistics about VRRP3 packets for all virtual routers configured on the switch or for a specific virtual router.

show vrrp3 [*vrid***] statistics**

Syntax Definitions

vrid	The virtual router ID, in the range from 1–255.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

Use the **show vrrp3 statistics** command to display information about VRRP3 packets. Use the **show vrrp3** command to display information about the virtual router configuration.

Examples

```
-> show vrrp3 statistics
 Checksum    Version     VRID
  Errors     Errors     Errors
----------+----------+----------
         0          0          0

VRID VLAN   State      UpTime   Become Master Adv. Rcvd
----+----+----------+----------+-------------+----------
   1  101 Master           2983            1           0
   2  102 Master          60675            1           0
   3  103 Master          60675            1           0
   4  104 Master          60675            1           0
   5  105 Master          60675            1           0
   6  106 Master          60675            1           0
   7  107 Master          60675            1           0
   8  108 Master          60675            1           0
   9  109 Master          60675            1           0
  10  110 Master          60675            1           0
```

output definitions

Checksum Errors	The total number of VRRP3 packets received with an invalid checksum value.
Version Errors	The total number of VRRP3 packets received with an invalid version number.
VRID Errors	The total number of VRRP3 packets received with invalid VRIDs.
VRID	The virtual router identifier.

output definitions (continued)

VLAN	The VLAN associated with the VRRP3 instance.
State	The administrative state of the VRRP3 instance; **initialize** specifies that the interface or vlan is either disabled or down and the startup delay timer has not expired; **backup** specifies that this instance is monitoring the availability of the master router; **master** specifies 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 VRRP3 advertisements received by this instance.

Release History

Release 6.1.3; command was introduced.

Related Commands

vrrp3	Configures a new VRRP3 virtual router or modifies an existing one. Used to enable or disable a virtual router.
show vrrp3	Displays the virtual router configuration for all virtual routers or for a specific virtual router.

MIB Objects

```
   alaVrrp3RouterChecksumErrors
   alaVrrp3RouterVersionErrors
   alaVrrp3RouterVrIdErrors
alaVrrp3RouterStatsTable
   alaVrrp3StatsBecomeMaster
   alaVrrp3StatsAdvertiseRcvd
   alaVrrp3StatsAdvIntervalErrors
   alaVrrp3StatsIpTtlErrors
   alaVrrp3StatsPriZeroPktsRcvd
   alaVrrp3StatsPriZeroPktsSent
   alaVrrp3StatsInvalidTypePktsRcvd
   alaVrrp3StatsAddressListErrors
   alaVrrp3StatsInvldAuthType
   alaVrrp3StatsPacketLengthErrors
alaVrrp3OperTable
   alaVrrp3OperUpTime
alaVrrp3OperGroup
   alaVrrp3OperState
```

show vrrp3 track-association

Displays the tracking policies associated with VRRP3 virtual routers.

show vrrp3 [*vrid***] track-association [***track_id***]**

Syntax Definitions

vrid	The virtual router ID, in the range from 1–255.
track_id	The ID of the tracking policy for which you want to display information.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

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 vrrp3 track-association
           Conf  Cur  Track                        Admin   Oper  Track
VRID VLAN  Pri   Pri   ID             Policy       State   State  Pri
----+----+-----+-----+-----+--------------------+--------+-----+------
   1  101  200   200     1  PORT 1/37             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 **vrrp3** 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, IPv6 address, or slot/port being tracked by this policy.
Admin State	The administrative state of the tracking policy.

output definitions (continued)

Oper State	Indicates 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 6.1.3; command was introduced.

Related Commands

vrrp3 track-association	Associates a VRRP3 tracking policy with a virtual router.

MIB Objects

```
alaVrrpTrackTable
   alaVrrpTrackState
   alaVrrpTrackAdminState
   alaVrrpTrackPriority
   alaVrrpTrackEntityType
   alaVrrpTrackEntityVlan
   alaVrrpTrackEntityPort
   alaVrrpTrackEntityIpAddress
   alaVrrpTrackEntityIpv6Interface
   alaVrrpTrackEntityInterface
   alaVrrpTrackRowStatus

alaVrrp3AssoTrackTable
   alaVrrp3AssoTrackId
   alaVrrp3TrackRowStatus
```

27 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 (that is, 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 *area*. 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-Lucent'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 exit-overflow-interval** **ip ospf extlsdb-limit** **ip ospf host** **ip ospf mtu-checking** **ip ospf default-originate** **ip ospf route-tag** **ip ospf spf-timer** **ip ospf virtual-link** **ip ospf neighbor** **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 routes** **show ip ospf virtual-link** **show ip ospf virtual-neighbor**
OSPF Area Commands	**ip ospf area** **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 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 6855, 6850E, 9000E

Usage Guidelines

The OSPF protocol must be enabled for it to route traffic.

Examples

```
-> ip ospf status enable
-> ip ospf status disable
```

Release History

Release 6.1; command was introduced.

Related Commands

show ip ospf	Displays OSPF status and general configuration parameters.

MIB Objects

```
ospfGeneralGroup
   ospfAdminStat
```

ip load ospf

Loads the OSPF software on the router.

ip load ospf

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6855, 6850E, 9000E

Usage Guidelines

N/A

Example

```
-> ip load ospf
```

Release History

Release 6.1; command was introduced.

Related Commands

N/A

MIB Objects

```
alaDrcTmConfig
   alaDrcTmIPOspfStatus
```

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 6855, 6850E, 9000E

Usage Guidelines

- The overflow interval is the time the router will wait before attempting to leave the database overflow state; the interval begins upon the router's arrival into this state.
- When the router leaves the overflow state, it can once again create non-default and external link state advertisements (LSAs) for autonomous systems (AS).
- The router will not leave the overflow state (until it is restarted) when the overflow interval value is set to 0.

Example

```
-> ip ospf exit-overflow-interval 10
```

Release History

Release 6.1; command was introduced.

Related Commands

show ip ospf	Displays the 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 6855, 6850E, 9000E

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.

Example

```
-> ip ospf extlsdb-limit 25
```

Release History

Release 6.1; 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 6855, 6850E, 9000E

Usage Guidelines

- The **no** variant of this command removes the record of the OSPF host.
- 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

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 6.1; 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 OS6855-U24X, 6850E, 9000E

Usage Guidelines

- The **no** form of this command disables MTU checking.
- 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.

Examples

```
-> ip ospf mtu-checking
-> no ip ospf mtu-checking
```

Release History

Release 6.1; command was introduced.

Related Commands

show ip ospf	Displays the OSPF status and general configuration parameters.

MIB Objects

```
alaProtocolOspf
   alaOspfMTUCheck
```

ip ospf default-originate

Configures a default external route into the OSPF routing domain.

ip ospf default-originate {only | always} [metric-type {type1 | type2}] [metric *value***]**

no ip ospf default-originate

Syntax Definitions

only	Advertises only when there is a default route in the routing table**.**
always	Advertises the default route regardless of whether the routing table has a default route.
type1	Sets the external route as type1.
type2	Sets the external route as type2.
value	The metric value.The valid range is 1-65535.

Defaults

parameter	default
type1 | type2	**type2**
value	1

Platforms Supported

OmniSwitch 6855, 6850E, 9000E

Usage Guidelines

Use the **no** form of the command to delete redistributed default routes.

Examples

```
-> ip ospf default-originate always
-> ip ospf default-originate only metric 10
-> ip ospf default-originate always metric-type type1 metric 5
-> no ip ospf default-originate
```

Release History

Release 6.1.3; command was introduced.

Related Commands

show ip ospf	Displays OSPF status and general configuration parameters.

MIB Objects

```
alaProtocolOspf
   alaOspfDefaultOriginate
   alaOspfDefaultOriginateMetricType
   alaOspfDefaultOriginateMetric
```

ip ospf route-tag

Configures a tag value for the 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 6855, 6850E, 9000E

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).

Example

```
-> ip ospf route-tag 2
```

Release History

Release 6.1; 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 an 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 6855, 6850E, 9000E

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 the 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.

Example

```
-> ip ospf spf-timer delay 20 hold 35
```

Release History

Release 6.1; command was introduced.

Related Commands

show ip ospf	Displays the 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 6855, 6850E, 9000E

Usage Guidelines

- The **no** form of the command deletes the virtual link.
- 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.

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 6.1; command was introduced.

Related Commands

show ip ospf virtual-link	Displays the 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 6855, 6850E, 9000E

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, by 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 6.1; 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 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 6855, 6850E, 9000E

Usage Guidelines

- The **no** form deletes the area.
- 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.

Examples

```
-> ip ospf area 0.0.0.1
-> ip ospf area 0.0.0.1 type stub
-> ip ospf area 0.0.0.1 type normal
-> no ip ospf area 0.0.0.1
```

Release History

Release 6.1; 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 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 6855, 6850E, 9000E

Usage Guidelines

- The **no** form deletes the default metric from the specified area.
- 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.

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 6.1; 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 6855, 6850E, 9000E

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 6.1; 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 *interface_name*

no ip ospf interface *interface_name*

Syntax Definitions

interface_name	The name of the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of the command to delete an OSPF interface.
- The interface name cannot contain spaces.

Examples

```
-> ip ospf interface vlan-101
-> no ip ospf interface vlan-101
```

Release History

Release 6.1; command was introduced.

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 administrative status on an OSPF interface.

ip ospf interface *interface_name* **status {enable | disable}**

no ip ospf interface *interface_name* **status {enable | disable}**

Syntax Definitions

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 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of the command to delete an OSPF interface.
- The OSPF interface must be enabled for it to participate in the OSPF protocol.

Examples

```
-> ip ospf interface vlan-101 status enable
-> ip ospf interface vlan-101 status disable
-> no ip ospf interface vlan-101 status enable
-> no ip ospf interface vlan-101 status disable
```

Release History

Release 6.1; command was introduced.

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 *interface_name* **area** *area_id*

Syntax Definitions

interface_name	The name of the interface.
area_id	A unique 32-bit value in IP address format.

Defaults

N/A

Platforms Supported

OmniSwitch 6855, 6850E, 9000E

Usage Guidelines

An interface must be assigned to an area to become operational.

Examples

```
-> ip ospf interface vlan-101 area 0.0.0.1
```

Release History

Release 6.1; command was introduced.

Related Commands

show ip ospf area	Displays either all the 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 an OSPF authentication key for simple authentication on an interface.

ip ospf interface *interface_name* **auth-key** *key_string*

Syntax Definitions

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 6855, 6850E, 9000E

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 27-30, set to **simple**.

Examples

```
-> ip ospf interface vlan-101 auth-key pass
```

Release History

Release 6.1; command was introduced.

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 *interface_name* **auth-type [none | simple | md5]**

Syntax Definitions

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 6855, 6850E, 9000E

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 27-29.
- 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 27-34 and page 27-36. One command enables MD5 and the other sets the key identification number.

Examples

```
-> ip ospf interface vlan-101 auth-type simple
```

Release History

Release 6.1; command was introduced.

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 *interface_name* **dead-interval** *seconds*

Syntax Definitions

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 6855, 6850E, 9000E

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 vlan-101 dead-interval 50
```

Release History

Release 6.1; command was introduced.

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 *interface_name* **hello-interval** *seconds*

Syntax Definitions

interface_name	The name of the interface.
seconds	The hello interval, in seconds. The valid range is 0–65535. A value of 0 creates a passive OSPF interface.

Defaults

parameter	default
seconds (broadcast and point-to-point)	10
seconds (NBMA and point-to-multi-point)	30

Platforms Supported

OmniSwitch 6855, 6850E, 9000E

Usage Guidelines

This is the interval between two consecutive hello packets sent out on this interface.

Examples

```
-> ip ospf interface vlan-101 hello-interval 50
```

Release History

Release 6.1; command was introduced.

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 *interface_name* **md5** *key_id* **[enable | disable]**

Syntax Definitions

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 6855, 6850E, 9000E

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 page 27-30 and page 27-36.
- The **no** variant deletes the key ID number.

Examples

```
-> ip ospf interface vlan-101 md5 100
-> ip ospf interface vlan-101 md5 10 disable
-> ip ospf interface vlan-101 md5 10 enable
```

Release History

Release 6.1; command was introduced.

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 *interface_name* **md5** *key_id* **key** *key_string*

Syntax Definitions

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 6855, 6850E, 9000E

Usage Guidelines

- This command is used in conjunction with the commands described above on page 27-30 and page 27-34.
- For MD5 authentication to function properly the same key string must be configured on the neighboring router for that interface.

Examples

```
-> ip ospf interface vlan-101 md5 100 key 1
```

Release History

Release 6.1; command was introduced.

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 *interface_name* **type {point-to-point | point-to-multipoint | broadcast | non-broadcast}**

Syntax Definitions

interface_name	The name of the 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.
broadcast	Sets the interface to be a broadcast OSPF interface.
non-broadcast	Sets the interface to be NBMA (Non Broadcast Multi Access) OSPF interface.

Defaults

parameter	default
broadcast | non-broadcast | point-to-point| point-to-multipoint	**broadcast**

Platforms Supported

OmniSwitch 6855, 6850E, 9000E

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 vlan-101 type non-broadcast
```

Release History

Release 6.1; command was introduced.

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 *interface_name* **cost** *cost*

Syntax Definitions

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 6855, 6850E, 9000E

Usage Guidelines

The configured interface cost, if any, is used during OSPF route calculations.

Examples

```
-> ip ospf interface vlan-101 cost 10
```

Release History

Release 6.1; command was introduced.

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 *interface_name* **poll-interval** *seconds*

Syntax Definitions

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 6855, 6850E, 9000E

Usage Guidelines

This parameter configures the larger time interval, in seconds, between hello packets sent to an inactive neighbor.

Examples

```
-> ip ospf interface vlan-101 poll-interval 500
```

Release History

Release 6.1; command was introduced.

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 *interface_name* **priority** *priority*

Syntax Definitions

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 6855, 6850E, 9000E

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 vlan-101 priority 100
```

Release History

Release 6.1; command was introduced.

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 *interface_name* **retrans-interval** *seconds*

Syntax Definitions

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 6855, 6850E, 9000E

Usage Guidelines

The number of seconds between link retransmission of OSPF packets on this interface.

Examples

```
-> ip ospf interface vlan-101 retrans-interval 500
```

Release History

Release 6.1; command was introduced.

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 *interface_name* **transit-delay** *seconds*

Syntax Definitions

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 6855, 6850E, 9000E

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 vlan-101 transit-delay 100
```

Release History

Release 6.1; command was introduced.

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	This parameter is currently not supported.

Defaults

Graceful restart is disabled by default.

Platforms Supported

OmniSwitch 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of the command to disable support for the graceful restart feature on an OSPF router.
- The minimum hardware configuration for this command is a redundant CMM configuration. This command is not supported on OmniSwitch chassis-based switches with a single CMM or OmniSwitch stackable switches in a standalone configuration.
- On OmniSwitch switches, a graceful restart is supported only on active ports (that is, interfaces) that 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-support planned-unplanned
-> no ip ospf restart-support
```

Release History

Release 6.1; 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 6855, 6850E, 9000E

Usage Guidelines

- The minimum hardware configuration for this command is a redundant CMM configuration. This command is not supported on OmniSwitch chassis-based switches with a single CMM or OmniSwitch stackable switches in a standalone configuration.
- On OmniSwitch stackable switches, a graceful restart is supported only on active ports (that is, interfaces) that 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.

Example

```
-> ip ospf restart-interval 600
```

Release History

Release 6.1; 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 6855, 6850E, 9000E

Usage Guidelines

- The minimum hardware configuration for this command is a redundant CMM configuration. This command is not supported on OmniSwitch chassis-based switches with a single CMM or OmniSwitch stackable switches in a standalone configuration.
- On OmniSwitch stackable switches, a graceful restart is supported only on active ports (that is, interfaces) that 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 status enable
```

Release History

Release 6.1; 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 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 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 a changed LSA will result in termination of graceful restart by a helping router.
disable	Disables a changed LSA will result in termination of graceful restart by a helping router.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6855, 6850E, 9000E

Usage Guidelines

- The minimum hardware configuration for this command is a redundant CMM configuration. This command is not supported on OmniSwitch chassis-based switches with a single CMM or OmniSwitch stackable switches in a standalone configuration.
- On OmniSwitch stackable switches, a graceful restart is supported only on active ports (that is, interfaces) that 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
-> ip ospf restart-helper strict-lsa-checking status enable
```

Release History

Release 6.1; 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 6855, 6850E, 9000E

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 chassis-based switches with a single CMM or OmniSwitch stackable switches in a standalone configuration.
- On OmniSwitch stackable switches, a graceful restart is supported only on active ports (that is, interfaces) that 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.

Example

```
-> ip ospf restart initiate
```

Release History

Release 6.1; 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 the OSPF status and general configuration parameters.

show ip ospf

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6855, 6850E, 9000E

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 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 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 6.1; 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 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 6855, 6850E, 9000E

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.

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.
ToS	The Type of Service. Only ToS value 0 is supported at this time.
Metric	The cost to the border router.

Release History

Release 6.1; command was introduced.

Related Commands

N/A

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 6855, 6850E, 9000E

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 (that is, 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 6.1; 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 the 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 6855, 6850E, 9000E

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 6.1; 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 6855, 6850E, 9000E

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 (that is, 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 6.1; command was introduced.

Related Commands

show ip ospf	Displays the 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 6855, 6850E, 9000E

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 "ineligible" 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 6.1; 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 routes

Displays the 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 6855, 6850E, 9000E

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 6.1; command was introduced.

Related Commands

show ip ospf	Displays the 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 6855, 6850E, 9000E

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 with regards 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 6.1; 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 6855, 6850E, 9000E

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           10.0.0.1          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 "ineligible" 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 6.1; 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 6855, 6850E, 9000E

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 6.1; 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 6855, 6850E, 9000E

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 6.1; 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 6855, 6850E, 9000E

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 6.1; 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 [*interface_name***]**

Syntax Definitions

interface_name	The name of the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 6855, 6850E, 9000E

Usage Guidelines

Not specifying an interface name displays all known interfaces for the OSPF router.

Examples

No interface name is specified:

```
-> 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 definitions

Interface Name	The name of the interface.
DR Address	The designated router IP address on this network segment. Make sure you configure a VLAN for the router IP. (See Chapter 4, "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 (an interface name is used in this example).

```
-> show ip ospf interface vlan-3
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
BFD Status                            = Disabled,
DR-Only Option for BFD                = Disabled
```

Note. See the table of the following page for output definitions.

The following is an example of simple authentication (an interface name is used in this example):

```
-> show ip ospf interface vlan-3
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
BFD Status                            = Disabled,
DR-Only Option for BFD                = Disabled
```

Output fields when an interface name is specified are described below:

output definitions

Interface IP Name	The name of the IP interface to which the OSPF 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.

output definitions (continued)

Designated Router RouterId	The identification number of the designated router.
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 with 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 the 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 the 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 the OSPF router will start using this key for packet generation. (This field is only displayed for MD5 authentication.)
StopGen	The time that the 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.

output definitions (continued)

# of Init State Neighbors	The number of OSPF neighbors in the initialization state.
# 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.
BFD Status	The status of BFD on this interface.
DR-Only Option for BFD	The BFD setting for this interface. If DR-Only only is disabled then the setting is All Neighbors.

Release History

Release 6.1; command was introduced.

Related Commands

ip ospf interface	Creates and deletes an OSPF interface.
ip ospf interface auth-key	Configures an 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 6855, 6850E, 9000E

Usage Guidelines

- The minimum hardware configuration for this command is a redundant CMM configuration. This command is not supported on OmniSwitch chassis-based switches with a single CMM or OmniSwitch stackable switches in a standalone configuration.
- On OmniSwitch stackable switches, a graceful restart is supported only on active ports (that is, interfaces) that 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 status of 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 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 6.1; command was introduced.

Related Commands

ip ospf interface	Creates and deletes an OSPF interface.
ip ospf restart-interval	Configures the grace period for achieving a graceful OSPF restart.
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 strict-lsa-checking status	Administratively enables and disables whether a changed Link State Advertisement (LSA) will result in termination of graceful restart by a helping router.

MIB Objects

28 OSPFv3 Commands

Open Shortest Path First version 3 (OSPFv3) routing is a shortest path first (SPF) or link-state protocol. This protocol is compatible with 128-bit IPv6 address space, while OSPF is compatible with 32-bit IPv4 address space. OSPFv3 is an interior gateway protocol (IGP) that distributes routing information between routers in a single autonomous system (AS). OSPFv3 chooses the least-cost path as the best path.

Each participating router distributes its local state (that is, 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.

OSPFv3 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.

Note. OSPFv3 is supported only on OmniSwitch 6855, OmniSwitch 6850E Series, and 9000E switches.

Alcatel-Lucent's version of OSPFv3 complies with RFCs 2740, 1826, 1827, 2553, 2373, 2374, and 2460.

MIB information for OSPFv3 is as follows:

Filename: AlcatelIND1DrcTm.mib
Module: ALCATEL-IND1-DRCTM-MIB

Filename: AlcatelIND1Ospf3.mib
Module: ALCATEL-IND1-OSPF3-MIB

Filename: IETF-OSPF-OSPFv3.MIB
Module: OSPF-OSPFv3-MIB

The following is a list of the commands for configuring OSPFv3:

Global OSPFv3 Commands	**ipv6 ospf status** **ipv6 load ospf** **ipv6 ospf host** **ipv6 ospf mtu-checking** **ipv6 ospf route-tag** **ipv6 ospf spf-timer** **ipv6 ospf virtual-link** **show ipv6 ospf** **show ipv6 ospf border-routers** **show ipv6 ospf host** **show ipv6 ospf lsdb** **show ipv6 ospf neighbor** **show ipv6 ospf routes** **show ipv6 ospf virtual-link**
OSPFv3 Area Commands	**ipv6 ospf area** **show ipv6 ospf area**
OSPFv3 Interface Commands	**ipv6 ospf interface** **ipv6 ospf interface status** **ipv6 ospf interface area** **ipv6 ospf interface dead-interval** **ipv6 ospf interface hello-interval** **ipv6 ospf interface cost** **ipv6 ospf interface priority** **ipv6 ospf interface retrans-interval** **ipv6 ospf interface transit-delay** **show ipv6 ospf interface**

ipv6 ospf status

Enables or disables the OSPFv3 administrative status for the router.

ipv6 ospf status {enable | disable}

Syntax Definitions

enable	Enables OSPFv3.
disable	Disables OSPFv3.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

The OSPFv3 protocol should be enabled to route traffic.

Examples

```
-> ipv6 ospf status enable
-> ipv6 ospf status disable
```

Release History

Release 6.1.3; command was introduced.

Related Commands

show ipv6 ospf	Displays OSPFv3 status and general configuration parameters.

MIB Objects

```
ospfv3GeneralGroup
   ospfv3AdminStat
```

ipv6 load ospf

Loads the OSPFv3 software on the router.

ipv6 load ospf

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

N/A

Example

```
-> ipv6 load ospf
```

Release History

Release 6.1.3; command was introduced.

Related Commands

N/A

MIB Objects

```
ALADRCTMCONFIG
   alaDrcTmIPOspf3Status
```

ipv6 ospf host

Creates or deletes an OSPFv3 entry for directly attached hosts.

ipv6 ospf host *ipv6_address* **[area** *area_id***] [metric** *metric***]**

no ipv6 ospf host *ipv6_address* **area** *area_id*

Syntax Definitions

ipv6_address	The 128-bit IP address of the OSPF host.
area_id	Area to which the host route belongs.
metric	The cost metric value assigned to the specified host. The valid range is 0–65535.

Defaults

parameter	default
metric	0

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of the command to remove the record of the OSPFv3 host.
- Use this command when multiple paths exist to a host. The specified host must be directly attached to the router. 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.
- This command allows you to modify the host parameter **metric**.

Examples

```
-> ipv6 ospf host 2001::1/64 metric 10
-> no ipv6 ospf host 2001::1/64 metric 10
```

Release History

Release 6.1.3; command was introduced.

Related Commands

show ipv6 ospf host	Displays information on the configured OSPFv3 hosts.

MIB Objects

```
ospfv3HostTable
   ospfv3HostStatus
   ospfv3HostAreaID
   ospfv3HostAddress
   ospfv3HostMetric
```

ipv6 ospf mtu-checking

Enables or disables Maximum Transfer Unit (MTU) checking. The MTU limits the size of a transmitted or received packet.

ipv6 ospf mtu-checking

no ipv6 ospf mtu-checking

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of the command to disable MTU checking.
- 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.

Examples

```
-> ipv6 ospf mtu-checking
-> no ipv6 ospf mtu-checking
```

Release History

Release 6.1.3; command was introduced.

Related Commands

show ipv6 ospf	Displays the OSPFv3 status and general configuration parameters.

MIB Objects

```
alaProtocolOspf3
   alaOspf3MTUCheck
```

ipv6 ospf route-tag

Configures a tag value for the Autonomous System External (ASE) routes created.

ipv6 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 6850E, 6855, 9000E

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

```
-> ipv6 ospf route-tag 2
```

Release History

Release 6.1.3; command was introduced.

Related Commands

show ipv6 ospf	Displays OSPFv3 status and general configuration parameters.

MIB Objects

```
alaProtocolOspf3
   alaOspf3RedistRouteTag
```

ipv6 ospf spf-timer

Configures timers for Shortest Path First (SPF) calculation.

ipv6 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 an 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 6850E, 6855, 9000E

Usage Guidelines

- This command allows you to configure the time interval between SPF calculations.
- Use the delay timer to determine how much time to postpone an SPF calculation after the router receives a topology change.
- Use the hold timer to configure the amount of time that must elapse between consecutive SPF calculations.
- There will be no delay in the SPF calculation if either the delay timer or hold timer is set to 0. The 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

```
-> ipv6 ospf spf-timer delay 20 hold 35
```

Release History

Release 6.1.3; command was introduced.

Related Commands

show ipv6 ospf	Displays the OSPFv3 status and general configuration parameters.

MIB Objects

```
alaProtocolOspf3
   alaOspf3TimerSpfDelay
   alaOspf3TimerSpfHold
```

ipv6 ospf virtual-link

Creates or deletes a virtual link. A virtual link restores the backbone connectivity if the backbone is not physically contiguous.

ipv6 ospf virtual-link area *area_id* **router** *router_id*
[dead-interval *seconds***] [hello-interval** *seconds***] [retrans-interval** *seconds***] [transit-delay** *seconds***]**

no ipv6 ospf virtual-link area *area_id* **router** *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.
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
dead-interval *seconds*	40
hello-interval *seconds*	10
retrans-interval *seconds*	5
transit-delay *seconds*	1

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of the command to delete the virtual link.
- You can 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 the routers on the same network. This value should be a multiple of the value provided for the **hello-interval**.

Examples

```
-> ipv6 ospf virtual-link area 0.0.0.1 router 172.22.2.115
-> ipv6 ospf virtual-link area 0.0.0.1 router 172.22.2.115 dead-interval 50
-> ipv6 ospf virtual-link area 0.0.0.1 router 172.22.2.115 hello-interval 20
-> ipv6 ospf virtual-link area 0.0.0.1 router 172.22.2.115 retrans-interval 20
-> ipv6 ospf virtual-link area 0.0.0.1 router 172.22.2.115 transit-delay 50
-> no ipv6 ospf virtual-link area 0.0.0.1 router 172.22.2.115
```

Release History

Release 6.1.3; command was introduced.

Related Commands

show ipv6 ospf virtual-link	Displays the virtual link information.

MIB Objects

```
ospfv3VirtIfTable
   ospfv3VirtIfAreaId
   ospfv3VirtIfNeighbor
   ospfv3VirtIfStatus
   ospfv3VirtIfRtrDeadInterval
   ospfv3VirtIfHelloInterval
   ospfv3VirtIfRetransInterval
   ospfv3VirtIfTransitDelay
```

ipv6 ospf area

Assigns an OSPFv3 interface to a specified area.

ipv6 ospf area *area_id* **[type {normal | stub [default-metric** *metric***]}]**

no ipv6 ospf area *area_id*

Syntax Definitions

area_id	A unique 32-bit value in IPv4 address format.
normal	Sets the area as a regular OSPFv3 area.
stub	Configures an OSPFv3 area as a stub area.
metric	Defines the metric to be used for default routes injected into the stub.

Defaults

parameter	default
normal | stub	**normal**

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of the command to delete the OSPFv3 area.
- The **default-metric** parameter defines the metric to be used for default routes injected into the stub area.

Examples

```
-> ipv6 ospf area 0.0.0.1
-> ipv6 ospf area 0.0.0.1 stub
-> ipv6 ospf area 0.0.0.1 type normal
-> no ipv6 ospf area 0.0.0.1
```

Release History

Release 6.1.3; command was introduced.

Related Commands

show ipv6 ospf area	Displays either all the OSPFv6 areas, or a specified OSPFv6 area.

MIB Objects

```
ospfv3AreaTable
   ospfv3ImportAsExtern
   ospfv3AreaSummary
   ospfv3StubMetric
   ospfv3AreaId
```

ipv6 ospf interface

Creates or deletes an OSPFv3 interface.

ipv6 ospf interface *interface_name*

no ipv6 ospf interface *interface_name*

Syntax Definitions

interface_name	The name of the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of the command to delete an OSPFv3 interface.
- The interface name cannot contain spaces.

Examples

```
-> ipv6 ospf interface vlan-101
-> no ipv6 ospf interface vlan-101
```

Release History

Release 6.1.3; command was introduced.

Related Commands

show ipv6 ospf interface	Displays the status and statistics of an OSPFv3 interface.

MIB Objects

```
ospfv3IfTable
   ospfv3IfIndex
```

ipv6 ospf interface status

Enables or disables the administration status on an OSPFv3 interface.

ipv6 ospf interface *interface_name* **status {enable | disable}**

no ipv6 ospf interface *interface_name*

Syntax Definitions

interface_name	The name of the interface.
enable	Enables the OSPFv3 interface.
disable	Disables the OSPFv3 interface.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of the command to delete an OSPFv3 interface.
- The OSPFv3 interface must be enabled to participate in the OSPFv3 protocol.

Examples

```
-> ipv6 ospf interface vlan-101 status enable
-> ipv6 ospf interface vlan-101 status disable
-> no ipv6 ospf interface vlan-101
-> no ipv6 ospf interface vlan-101
```

Release History

Release 6.1.3; command was introduced.

Related Commands

show ipv6 ospf interface	Displays the status and statistics of an OSPFv3 interface.

MIB Objects

```
ospfv3IfTable
   ospfv3IfIndex
   ospfv3IfAdminStat
```

ipv6 ospf interface area

Configures an OSPFv3 area identifier for this interface.

ipv6 ospf interface *interface_name* **area** *area_id*

Syntax Definitions

interface_name	The name of the interface.
area_id	A unique 32-bit value in IP address format.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

An interface must be assigned to an area to become operational.

Examples

```
-> ipv6 ospf interface vlan-101 area 0.0.0.1
```

Release History

Release 6.1.3; command was introduced.

Related Commands

show ipv6 ospf area	Displays either all the OSPFv3 areas, or a specified OSPFv3 area.
show ipv6 ospf interface	Displays the status and statistics of an OSPFv3 interface.

MIB Objects

```
ospfv3IfTable
   ospfv3IfIndex
   ospfv3IfAreaId
```

ipv6 ospf interface dead-interval

Configures the OSPFv3 interface dead interval.

ipv6 ospf interface *interface_name* **dead-interval** *seconds*

Syntax Definitions

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 6850E, 6855, 9000E

Usage Guidelines

- After the dead interval, 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 multiples of the hello interval.

Examples

```
-> ipv6 ospf interface vlan-101 dead-interval 50
```

Release History

Release 6.1.3; command was introduced.

Related Commands

ipv6 ospf interface hello-interval	Configures the OSPFv3 interface hello interval.
show ipv6 ospf interface	Displays the status and statistics of an OSPFv3 interface.

MIB Objects

```
ospfv3IfTable
   ospfv3IfIndex
   ospfv3IfRtrDeadInterval
```

ipv6 ospf interface hello-interval

Configures the OSPFv3 interface hello interval.

ipv6 ospf interface *interface_name* **hello-interval** *seconds*

Syntax Definitions

interface_name	The name of the interface.
seconds	The hello interval, in seconds. The valid range is 0–65535. A value of 0 create a passive OSPF interface.

Defaults

parameter	default
seconds (broadcast and point-to-point)	10
seconds (NBMA and point-to-multi-point)	30

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

This is the interval between two consecutive hello packets sent out on this interface.

Examples

```
-> ipv6 ospf interface vlan-101 hello-interval 50
```

Release History

Release 6.1.3; command was introduced.

Related Commands

ipv6 ospf interface dead-interval	Configures the OSPFv3 interface dead interval.
show ipv6 ospf interface	Displays the status and statistics of an OSPFv3 interface.

MIB Objects

```
ospfv3IfTable
   ospfv3IfIndex
   ospfv3IfHelloInterval
```

ipv6 ospf interface cost

Configures the OSPFv3 interface cost.

ipv6 ospf interface *interface_name* **cost** *cost*

Syntax Definitions

interface_name	The name of the interface.
cost	The interface cost. The valid range is 0–65535.

Defaults

parameter	default
cost	1

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

The configured interface cost (if any) is used during OSPFv3 route calculations.

Examples

```
-> ipv6 ospf interface vlan-101 cost 10
```

Release History

Release 6.1.3; command was introduced.

Related Commands

show ipv6 ospf interface	Displays the status and statistics of an OSPFv3 interface.

MIB Objects

```
ospfv3IfTable
   ospfv3IfIndex
   ospfv3IfMetricValue
```

ipv6 ospf interface priority

Configures the OSPFv3 interface priority. The priority number helps determine the eligibility of this router to become the designated router on the network.

ip ospf interface *interface_name* **priority** *priority*

Syntax Definitions

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 6850E, 6855, 9000E

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

```
-> ipv6 ospf interface vlan-101 priority 100
```

Release History

Release 6.1.3; command was introduced.

Related Commands

show ipv6 ospf interface	Displays the status and statistics of an OSPFv3 interface.

MIB Objects

```
ospfv3IfTable
   ospfv3IfIndex
   ospfv3IfRtrPriority
```

ipv6 ospf interface retrans-interval

Configures the OSPFv3 interface retransmit time interval.

ipv6 ospf interface *interface_name* **retrans-interval** *interval*

Syntax Definitions

interface_name	The name of the interface.
interval	The retransmit interval, in seconds. The valid range 0–3600.

Defaults

parameter	default
interval	5

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

The number of seconds between link retransmission of OSPFv3 packets on this interface.

Examples

```
-> ipv6 ospf interface vlan-101 retrans-interval 500
```

Release History

Release 6.1.3; command was introduced.

Related Commands

show ipv6 ospf interface	Displays the status and statistics of an OSPFv3 interface.

MIB Objects

```
ospfv3IfTable
   ospfv3IfIndex
   ospfv3IfRetransInterval
```

ipv6 ospf interface transit-delay

Configures the OSPFv3 interface transit time delay.

ipv6 ospf interface *interface_name* **transit-delay** *delay*

Syntax Definitions

interface_name	The name of the interface.
delay	The transit delay, in seconds. The valid range is 0–3600.

Defaults

parameter	default
seconds	1

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

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

```
-> ipv6 ospf interface vlan-101 transit-delay 100
```

Release History

Release 6.1.3; command was introduced.

Related Commands

show ipv6 ospf interface	Displays the status and statistics of an OSPFv3 interface.

MIB Objects

```
ospfv3IfTable
   ospfv3IfIndex
   ospfv3IfTransitDelay
```

show ipv6 ospf

Displays the OSPFv3 status and general configuration parameters.

show ipv6 ospf

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- This command is used to display the general configuration parameters of the OSPFv3 router.
- See the Related Commands section below to modify the displayed parameters.

Examples

```
-> show ipv6 ospf

Status                          = Enabled,
Router ID                       = 5.5.5.5,
# Areas                         = 2,
# Interfaces                    = 4,
Area Border Router              = Yes,
AS Border Router                = No,
External Route Tag              = 0,
SPF Hold (seconds)              = 10,
SPF Delay (seconds)             = 5,
MTU checking                    = Enabled,
# SPF calculations performed    = 3,
Last SPF run (seconds ago)      = N/A,
# of neighbors that are in:
  Full state                    = 3,
  Loading state                 = 0,
  Exchange state                = 0,
  Exstart state                 = 0,
  2way state                    = 0,
  Init state                    = 0,
  Attempt state                 = 0,
  Down state                    = 0,
```

output definitions

Status	Displays whether OSPFv3 is currently enabled or disabled on the router.
Router Id	The unique identification for the router.
# Areas	Number of areas to which the router belongs.
# Interface	Number of interfaces participating in OSPF
Area Border Router	Displays whether the router status is an area router or not.
AS Border Router	Displays whether the area Autonomous System Border Router status of this router is enabled or disabled.
External Route Tag	Displays the route tag for this router.
SPF Hold (seconds)	Displays the time in seconds between the reception of an OSPFv3 topology change and the start of a SPF calculation.
SPF Delay (seconds)	Displays the time in seconds between consecutive SPF calculations.
MTU Checking	Displays whether Maximum Transfer Unit checking is enabled or disabled. This is set using the **ipv6 ospf mtu-checking** command.
# SPF calculations performed	Displays the number of SPF calculation performed.
Last SPF run (seconds ago)	N/A
Full state	Displays the number of neighbor routers that are in Full state.
Loading state	Displays the number of neighbor routers that are in Loading state.
Exchange state	Displays the number of neighbor routers that are in Exchange state.
Exstart state	Displays the number of neighbor routers that are in Exstart state.
2way state	Displays the number of neighbor routers that are in 2way state.
Init state	Displays the number of neighbor routers that are in Init state.
Attempt state	Displays the number of neighbor routers that are in Attempt state.
Down state	Displays the number of neighbor routers that are in Down state.

Release History

Release 6.1.3; command was introduced.

Related Commands

ipv6 ospf status	Enables or disables the administration of OSPFv3 on the router.
ipv6 ospf mtu-checking	Enables or disables the use of Maximum Transfer Unit (MTU) checking.
ipv6 ospf spf-timer	Configures timers for SPF calculation.
ipv6 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

```
ospfv3GeneralGroup
   ospfv3RouterId
   ospfv3AdminStat
   ospfv3VersionNumber
   ospfv3AreaBdrRtrStatus
   ospfv3ASBdrRtrStatus
   ospfv3OriginateNewLsas
   ospfv3RxNewLsas
   ospfv3ExitOverflowInterval
alaProtocolOspf3
   alaOspf3RedistAdminStatus
   alaOspf3RedistRouteTag
   alaOspf3TimerSpfDelay
   alaOspf3TimerSpfHold
   alaOspf3MTUCheck
```

show ipv6 ospf border-routers

Displays information regarding all or specified border routers.

show ipv6 ospf border-routers [area *area_id***] [router** *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.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- This command is used to display a list of border routers known by this OSPFv3 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.

Examples

```
-> show ipv6 ospf border-routers

Router ID          Area           Metric   Type
---------------+---------------+--------+---------
6.6.6.6            0.0.0.0          2      INTRA
6.6.6.6            0.0.0.1          2      INTRA
        fe80::2d0:95ff:fee2:6bda -> pseudo1
        fe80::2d0:95ff:fee2:6bda -> pseudo2
```

output definitions

Router ID	The unique identification for the router.
Area	A unique 32-bit value, such as an IP address, that identifies a neighboring router in the Autonomous System.
Metric	The metric used by the routes.
Type	The type of routes specified (intra or inter).

Release History

Release 6.1.3; command was introduced.

Related Commands

N/A

MIB Objects

N/A

show ipv6 ospf host

Displays information on the configured OSPFv3 hosts.

show ipv6 ospf host [*ipv6_address***]**

Syntax Definitions

ipv6_address	A 128-bit IP address for a directly attached host.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- This command is used to display general information for OSPFv3 hosts directly attached to this router.
- See the Related Commands section below to modify the list.

Examples

```
-> show ipv6 ospf host

Area             Metric   Address
---------------+-------+-----------
0.0.0.1            1      2001::1/64
```

output definitions

Area	A 32-bit IP address for a directly attached host. This can be set using the **ipv6 ospf host** command.
Metric	The metric assigned to the host. Metric is set using the **ipv6 ospf host** command.
Address	IPV6 address of the host.

Release History

Release 6.1.3; command was introduced.

Related Commands

ipv6 ospf host	Creates or deletes an OSPFv3 entry for directly attached hosts.

MIB Objects

```
ospfv3HostTable
   ospfv3HostIpAddress
   ospfv3HostMetric
   ospfHostStatus
   ospfv3HostAreaID
```

show ipv6 ospf lsdb

Displays Link State Advertisements (LSAs) in the Link State Database (LSDB) associated with each area.

show ipv6 ospf lsdb [area *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 6850E, 6855, 9000E

Usage Guidelines

- This command is used to display the LSDB of the OSPF router. It can be used for OSPF debugging, specifically to narrow down sections of an area to determine which sections are receiving the specified LSAs. You can specify the parameters of only the area LSDB using the optional command parameters.
- You can view LSAs by specifying either a link state identifier or a router identifier. However, when specifying a router ID, you also need to supply a valid link state ID.

Examples

```
-> show ipv6 ospf lsdb

Area             Type       Link ID      Advertising Rtr  Sequence #   Age

-----------------+----------+------------+-----------------+----------+----------
0.0.0.0          Router     0            1.1.1.1           8000020f     1117
0.0.0.0          Router     0            3.3.3.3           80000208     1121
0.0.0.0          Router     0            5.5.5.5           800001f1     1117
0.0.0.0          Router     0            30.30.30.30       800000da     1115
```

output definitions

Area	The identification of the area to which the router belongs.
Type	The protocol type from where the route was learned.
Link Id	The Link state ID. The ID is a unique 32-bit value expressed as an IPv6 address. This number is used as a record in the link state database.
Advertising Rtr	The ID of the router that advertises the routes.
Sequence #	The advertisement sequence number (that is, 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 6.1.3; command was introduced.

Related Commands

ipv6 ospf status	Displays the OSPFv3 status and general configuration parameters.

MIB Objects

```
ospfv3AsLsdbTable
   ospfv3AsLsdbAreaId
   ospfv3AsLsdbType
   ospfv3AsLsdbLsid
   ospfv3AsLsdbRouterId
   ospfv3AsLsdbAdvertisement
   ospfv3AsLsdbSequence
   ospfv3AsLsdbAge
```

show ipv6 ospf neighbor

Displays information on OSPFv3 non-virtual neighbors.

show ipv6 ospf neighbor [router *ipv4_address***][interface** *interface_name***]**

Syntax Definitions

ipv4_address	A 32-bit router ID of the neighboring router.
interface_name	The name of the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- This command is used to display all non-virtual neighbors of the OSPF router.

Examples

```
-> show ipv6 ospf neighbor
Router ID        Area/Transit Area   State  Interface
----------------+-------------------+-----+---------------------------------
1.1.1.1          0.0.0.0              FULL  vlan-2071
3.3.3.3          0.0.0.0              FULL  vlan-2071
5.5.5.5          0.0.0.0              FULL  vlan-2071
23.23.23.23      0.0.0.1              FULL  vlan-2055
23.23.23.23      0.0.0.1              FULL  vlan-2056
24.24.24.24      0.0.0.1              FULL  vlan-2065
24.24.24.24      0.0.0.1              FULL  vlan-2066
```

output definitions

Router ID	The unique identification for the router.
Area/Transit Area	The area identifier.
State	The state of the OSPF neighbor adjacency.
Interface	The name of the interface.

```
-> show ipv6 ospf neighbor router 24.24.24.24
Router ID        Area/Transit Area   State  Interface
----------------+-------------------+-----+--------------
24.24.24.24      0.0.0.1              FULL  vlan-2070
24.24.24.24      0.0.0.1              FULL  vlan-2073
```

output definitions

Router ID	The unique identification for the router.
Area/Transit Area	The area identifier.
State	The state of the OSPF neighbor adjacency.
Interface	The name of the interface.

Release History

Release 6.1.3; command was introduced.

Related Commands

N/A

MIB Objects

```
ospfv3NbrTable
   ospfNbrAddress
   ospfv3NbrRtrId
   ospfv3NbrOptions
   ospfv3NbrPriority
   ospfv3NbrState
   ospfv3NbrEvents
   ospfv3NbrHelloSuppressed
```

show ipv6 ospf routes

Displays the OSPFv3 routes known to the router.

show ipv6 ospf routes [prefix *ipv6_address_prefix***][gateway** *gateway***]**

Syntax Definitions

ipv6_address_prefix	The 128-bit IPv6 address of the route destination in hexadecimal format.
gateway	The next hop IPv6 address for this router.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

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 ipv6 ospf routes
                                                          Path  Metric
                                                             Metric
 Prefix                                       Path Type         1 : 2
        Gateway Address -> Interface
----------------------------------------+----------+--------------------------
 ::30.30.31.0/120                            INTRA            1 : -
        :: -> v6-intf1001
 ::30.30.32.0/120                            INTRA            1 : -
        :: -> v6-intf1002
 ::30.30.33.0/120                            INTRA            1 : -
        :: -> v6-intf1003
```

output definitions

Prefix	The destination address of the IPv6 route in the hexadecimal format.
Gateway Address	The address of the gateway.
Interface	The outgoing interface on the switch.
Path Type	The type of routes specified (intra or inter).
Path Metric	The cost of the route.

Release History

Release 6.1.3; command was introduced.

Related Commands

ipv6 ospf status	Displays the OSPFv3 status and general configuration parameters.

MIB Objects

N/A

show ipv6 ospf virtual-link

Displays virtual link information. A virtual link is used to connect OSPFv3 backbone routers that are not physically contiguous.

show ipv6 ospf virtual-link [*router_id***]**

Syntax Definitions

router_id	The router ID of the remote end of the virtual link.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show ipv6 ospf virtual-link
                                    Intf   Nbr
Transit Area     Peer Router ID    State  State   Cost
----------------+----------------+------+-------+------+
0.0.0.1          6.6.6.6           P2P     FULL    2
```

output definitions

Transit Area	The area identification for the area assigned to the virtual link.
Peer Router ID	The destination router identification for the virtual link.
Intf State	The state of the virtual link with regards to the local router.
Nbr State	The state of the virtual link adjacency.
Cost	The cost metric of the route.

Release History

Release 6.1.3; command was introduced.

Related Commands

ipv6 ospf virtual-link	Creates or deletes a virtual link.

MIB Objects

```
ospfv3VirtIfTable
   ospfv3VirtIfAreaId
   ospfv3VirtIfNeighbor
   ospfv3VirtIfState
```

show ipv6 ospf area

Displays either all OSPFv3 areas, or a specified OSPFv3 area.

show ipv6 ospf area [*area_id*]

Syntax Definitions

area_id	A unique 32-bit value in IP address format.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Allows you to view the details of a specified OSPFv3 area.
- If an OSPF area is not specified, all known areas for the OSPFv3 router will be displayed.
- See the Related Commands section below for information on modifying an area.

Examples

```
-> show ipv6 ospf area

                           Stub   Number of
Area ID           Type    Metric  Interfaces
----------------+-------+-------+-------------
0.0.0.0           Normal   NA      2
0.0.0.1           Normal   NA      2

-> show ipv6 ospf area 0.0.0.0
Area Type                              = Normal,
Area Stub Metric                       = 0,
# of SPF calculations                  = 52,
# Interfaces                           = 3,
# Router LSAs                          = 2,
# Network LSAs                         = 3,
# Intra-area-prefix LSAs               = 4,
# Inter-area-prefix LSAs               = 15,
# Inter-area-router LSAs               = 0,
# hosts                                = 0,
```

output definitions

Area Type	The area type. This field will be **normal** or **stub**.
Area Stub Metric	Indicates whether the area is enabled or disabled.
# Router LSAs	The total number of Link State Advertisements for the Area.

output definitions (continued)

# Network LSAs	The total number of inter-area Link State Advertisements.
# of SPF calculations	The number of times the area has calculated the Shortest Path.
# Interfaces	The number of OSPF interfaces.
# Intra-area-prefix LSAs	The number of intra-area-prefix LSAs, which associates a list of IPv6 address prefixes with a router by referencing a router-LSA.
# Inter-area-prefix LSAs	The number of inter-area-prefix LSAs.Corresponds to Type 3 summary-LSA of OSPF.
# Inter-area-router LSAs	The number of inter-area-router LSAs. Corresponds to Type 4 summary-LSA of OSPF.
# hosts	The number of directly attached hosts.

Release History

Release 6.1.3; command was introduced.

Related Commands

ipv6 ospf area	Creates or deletes an OSPFv3 area, assigning default metric, cost, and type.
show ipv6 ospf interface	Displays OSPFv3 interface information.

MIB Objects

```
ospfv3AreaTable
   ospfv3AreaId
   ospfv3ImportAsExtern
   ospfv3SpfRuns
   ospfv3AreaBdrRtrCount
   ospfv3AreaSummary
   ospfv3AreaStatus
```

show ipv6 ospf interface

Displays OSPFv3 interface information.

show ipv6 ospf interface [*interface_name***]**

Syntax Definitions

interface_name	The name of the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

Not specifying the interface name displays all known interfaces for the OSPFv3 router.

Examples

```
-> show ipv6 ospf interface
                                                Admin     Oper
Name        DR Router ID     BDR Router ID     Status    Status     State
----------+----------------+---------------+----------+---------+---------
vlan-2071    5.5.5.5          0.0.0.0        Enabled      Up        DR

vlan-2055    7.7.7.7          5.5.5.5        Enabled      Up        BDR

vlan-2056    7.7.7.7          5.5.5.5        Enabled      Up        BDR
```

output definitions

Name	The name of the interface.
DR Router ID	The designated router address on this network segment. Make sure you configure a VLAN for the router IP. (See Chapter 4, "VLAN Management Commands," for more information.)
BDR Router ID	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	Indicates whether the interface is an active OSPF interface.
State	The current state of the OSPF interface. It will be **DR, BDR, other.**

```
-> show ipv6 ospf interface vlan-2071
Type                              = BROADCAST,
Admin Status                      = Enabled,
IPv6 Interface Status             = Up,
Oper Status                       = Up,
State                             = DR,
Area                              = 0.0.0.0,
Priority                          = 100,
Cost                              = 1,
Designated Router                 = 3.3.3.3,
Backup Designated Router          = 0.0.0.0,
Hello Interval                    = 1,
Router Dead Interval              = 4,
Retransmit Interval               = 5,
Transit Delay                     = 1,
Ifindex                           = 17,
IPv6 'ifindex'                    = 2071,
MTU                               = 1500,
# of attached neighbors           = 0,
Globally reachable prefix #0      = 2071::2/64
```

Output fields when an IP address or interface name is specified are described below:

output definitions

Type	The OSPF interface type, which can be Broadcast, NBMA, Point-to-Point, or Point-to-Multipoint.
Admin Status	The current administrative status of the interface, either **enabled** or **disabled**.
IPv6 Interface Status	The current administrative status of the IPv6 interface, either **up** or **down**.
Oper Status	Indicates 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**.
Area	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.
Priority	The priority of the interface with regards to becoming the designated router. The higher the number, the higher the priority.
Cost	The cost added to routes learned on this interface.
Designated Router	The identification number of the designated router.
Backup Designated Router	The identification number of the backup designated router.
Hello Interval	The number of seconds between hello messages sent out on the interface.
Router Dead Interval	The number of seconds the interface waits for hello messages received from a neighbor before declaring the neighbor as dead.
Retransmit Interval	The number of seconds the interface waits before resending hello messages.
Transit Delay	The estimated number of seconds required to transmit a link state update over this interface.

output definitions (continued)

Ifindex	The unique value assigned to an interface.
IPv6 'ifindex'	The unique value assigned to an IPv6 interface.
MTU	The Maximum Transfer Unit (in bytes) for the interface.
# of attached neighbors	The number of OSPFv3 neighbors in the initialization state.
Globally reachable prefix #0	A globally unique IPv6 address.

Release History

Release 6.1.3; command was introduced.

Related Commands

ipv6 ospf interface	Creates and deletes an OSPFv3 interface.
ipv6 ospf interface dead-interval	Configures the OSPFv3 interface dead interval.
ipv6 ospf interface hello-interval	Configures the OSPFv3 interface hello interval.
ipv6 ospf interface cost	Configures the OSPFv3 interface cost.
ipv6 ospf interface priority	Configures the OSPFv3 interface priority.
ipv6 ospf interface retrans-interval	Configures the OSPFv3 interface retransmit interval.
ipv6 ospf interface transit-delay	Configures the OSPFv3 interface transit delay.
ipv6 ospf interface area	Configures an OSPFv3 interface area.
ipv6 ospf interface status	Enables or disables the administration status on an OSPFv3 interface.

MIB Objects

```
ospfv3IfTable
   ospfv3IfAreaId
   ospfv3IfType
   ospfv3IfAdminStat
   ospfv3IfRtrPriority
   ospfv3IfTransitDelay
   ospfv3IfRetransInterval
   ospfv3IfHelloInterval
   ospfv3IfRtrDeadInterval
   ospfv3IfPollInterval
   ospfv3IfState
   ospfv3IfDesignatedRouter
   ospfv3IfBackupDesignatedRouter
   ospfv3IfEvents
   ospfv3IfStatus
```

29 IS-IS Commands

Intermediate System-Intermediate System (IS-IS) is a shortest path first (SPF) or link-state protocol. IS-IS is an interior gateway protocol (IGP) that distributes routing information between routers in a single autonomous system (AS) for IP as well as OSI environments. This feature allows a single routing protocol to support pure IP and OSI environments, and dual environments. Integrated IS-IS is also deployed extensively in an IP-only environment.

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. IS-IS routers have adjacencies with other routers on point-to-point links. In a multi-access network, routers report their adjacencies to a Designated Intermediate System (DIS), which generates an additional Link State PDU (LSP), commonly known as the pseudo-node LSP. The DIS is responsible for flooding the LAN with LSP and also for synchronizing the entire AS topology. This database is built from the collected link state advertisements of all routers.

IS-IS is a hierarchical protocol where the autonomous system is divided into multiple areas to reduce the size of the Routing table. Routing within an area is referred to as Level-1 routing and that between two or more areas is referred to as Level 2 routing. Each area runs a separate copy of the basic link-state routing algorithm.

Note. IS-IS is currently supported only on the OmniSwitch 6850E Series

---

Alcatel-Lucent's version of IS-IS complies with RFC 1142.

MIB information for the IP commands is as follows:

Filename: AlcatelIND1Isis.mib
Module: ALCATEL-IND1-ISIS-MIB

Filename: IETF_ISIS.MIB
Module: ISIS-MIB

A summary of the available commands is listed here:

Global IS-IS Commands	**ip load isis** **ip isis status** **ip isis area-id** **ip isis level-capability** **ip isis auth-check** **ip isis auth-type** **ip isis csnp-auth** **ip isis hello-auth** **ip isis psnp-auth** **ip isis lsp-lifetime** **ip isis lsp-wait** **ip isis spf-wait** **ip isis summary-address** **ip isis overload** **ip isis overload-on-boot** **ip isis graceful-restart** **ip isis graceful-restart helper** **ip isis strict-adjacency-check** **ip isis level auth-type** **ip isis level hello-auth** **ip isis level csnp-auth** **ip isis level psnp-auth** **ip isis level wide-metrics-only** **show ip isis adjacency** **show ip isis database** **show ip isis hostname** **show ip isis routes** **show ip isis spf** **show ip isis spf-log** **show ip isis statistics** **show ip isis status** **show ip isis summary-address**

Interface Commands	**ip isis interface** **ip isis interface status** **ip isis interface interface-type** **ip isis interface csnp-interval** **ip isis interface hello-auth-type** **ip isis interface level-capability** **ip isis interface lsp-pacing-interval** **ip isis interface passive** **ip isis interface retransmit-interval** **ip isis interface default-type** **ip isis interface level hello-auth-type** **ip isis interface level hello-interval** **ip isis interface level hello-multiplier** **ip isis interface level metric** **ip isis interface level passive** **ip isis interface level priority** **show ip isis interface**
Clear Commands	**clear ip isis adjacency** **clear ip isis lsp-database** **clear ip isis spf-log** **clear ip isis statistics**

ip load isis

Loads the IS-IS software on the router.

ip load isis

Syntax Definitions

N/A

Defaults

By default, IS-IS is not loaded on the switch.

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

- You need to load IS-IS on the switch before executing any IS-IS configuration command.
- To unload IS-IS, remove all the IS-IS configuration from “boot.cfg”.

Examples

```
-> ip load isis
```

Release History

Release 6.2.1; command was introduced.

Related Commands

show ip protocols	Displays switch routing protocol information and status.

MIB Objects

```
alaDrcTmIPIsisStatus
```

ip isis status

Enables or disables the administrative status of IS-IS on the switch.

ip isis status {enable | disable}

Syntax Definitions

enable	Enables IS-IS.
disable	Disables IS-IS.

Defaults

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

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

When IS-IS status is disabled, the configuration settings and related statistics of the protocol remain unaffected.

Examples

```
-> ip isis status enable
-> ip isis status disable
```

Release History

Release 6.2.1; command was introduced.

Related Commands

show ip isis status	Displays the IS-IS status.

MIB Objects

```
isisSysTable
   isisSysAdminState
```

ip isis area-id

Configures the area ID for the switch.

ip isis area-id *area address*

no ip isis area-id *area address*

Syntax Definitions

area address	1–13 byte variable length integer, which specifies the area address.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to remove the area ID.
- The area ID is part of the Network Service Access Point (NSAP) address.
- Other parts of NSAP address (system ID and selector ID) are not configurable. System ID is derived from router ID and selector ID remains always as 00.
- You can configure a maximum of three area addresses.

Examples

```
-> ip isis area-id 49.0001
-> no ip isis area-id 49.0001
```

Release History

Release 6.2.1; command was introduced.

Related Commands

show ip isis status	Displays the IS-IS status.

MIB Objects

```
isisManAreaAddrTable
   isisManAreaAddrExistState
```

ip isis level-capability

Configures the router level of the IS-IS protocol globally.

ip isis level-capability {level-1 | level-2 | level-1/2}

Syntax Definitions

level-1	Specifies that the router can operate at Level-1 only.
level-2	Specifies that the router can operate at Level-2 only.
level-1/2	Specifies that the router can operate at both Level-1 and Level-2.

Defaults

parameter	default
level-1 | **level-2** | **level-1/2**	**level-1/2**

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

- Changing the level capability restarts the IS-IS protocol.
- You can also configure the level capability at per interface level.

Examples

```
-> ip isis level-capability level-1
-> ip isis level-capability level-2
```

Release History

Release 6.2.1; command was introduced.

Related Commands

ip isis interface level-capability	Configures the IS-IS level on the specified interface.
show ip isis status	Displays the IS-IS status.

MIB Objects

```
isisSysTable
   isisSysType
```

ip isis auth-check

Enables or disables authentication check for IS-IS PDUs.

ip isis auth-check {enable | disable}

Syntax Definitions

enable	Enables authentication check for IS-IS PDUs.
disable	Disables authentication check for IS-IS PDUs.

Defaults

By default, authentication check is enabled.

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

- If enabled, IS-IS PDUs that fail to match either of the authentication type and key requirements are rejected.
- If disabled, the authentication PDUs are generated and the IS-IS PDUs are authenticated on receipt. An error message will be generated in case of a mismatch; but PDUs will not be rejected.

Examples

```
-> ip isis auth-check enable
-> ip isis auth-check disable
```

Release History

Release 6.3.1; command was introduced;

Related Commands

ip isis auth-type	Enables authentication and configures the authentication type of IS-IS protocol globally.
ip isis level auth-type	Enables authentication and configures the authentication types for specific IS-IS levels.
show ip isis status	Displays the IS-IS status.

MIB Objects

```
vRtrIsisTable
   vRtrIsisAuthCheck
```

ip isis auth-type

Enables authentication and configures the authentication type of IS-IS protocol globally.

ip isis auth-type {simple {key *key* **| encrypt-key** *encrypt-key***} | md5 {key** *key* | **encrypt-key** *encrypt-key***} | none}**

Syntax Definitions

simple	Simple authentication will be used.
md5	Specifies that MD5 authentication algorithm will be used. Hash-key will be used in MD5 authentication.
key	Key will be plain text ASCII up to 118 characters. Use quotes around string if the key contains multiple words with spaces between them.
encrypt-key	The key in hexadecimal format to provide security consideration on the authentication key. Configuration snapshot always displays authentication key in the encrypted form.
none	No authentication will be used.

Defaults

parameter	default
simple | **md5** | **none**	**none**

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

- Simple authentication uses only a text string as the password in the packet. This helps to protect the routers from a configuration mishap. MD5 authentication is used to protect the system from malicious actions.
- MD5 authentication is used to encrypt the information that is sent over the network. MD5 authentication uses shared secret key. The Key is used to sign the packets with an MD5 checksum to sign the packet, so that the packets cannot be tampered. As the key is not included in the packet, snooping the key is not possible.
- Use the Key parameter to configure the password for Simple or MD5 authentication. Alternatively, use the *encrypt-key* parameter to configure the password by supplying the encrypted form of the password as the encrypt-key. The Configuration snapshot always displays the password in the encrypted form. You should use only this *key* parameter during the CLI configuration.
- If the *encrypt-key* parameter is used to configure the password through the CLI, then its value should be the same as the one that appears in the configuration snapshot. Only valid system generated values are accepted as encrypt-key.
- This command configures the authentication type of ISIS protocol globally. These settings can be overridden at each level.

- By default, the authentication is disabled and no authentication type is configured.

Examples

```
-> ip isis auth-type simple key rachel
-> ip isis auth-type md5 encrypt-key 7a1e441a014b4030
```

Release History

Release 6.2.1; command was introduced.
Release 6.3.1; **key** and **encrypt-key** parameters were added.

Related Commands

ip isis level auth-type	Enables authentication and configures the authentication types for specific IS-IS levels.
show ip isis status	Displays the IS-IS status.

MIB Objects

```
vRtrIsisTable
   vRtrIsisAuthType
   vRtrIsisAuthKey
```

ip isis csnp-auth

Enables or disables the authentication of Complete Sequence Number PDUs (CSNPs).

ip isis csnp-auth

no ip isis csnp-auth

Syntax Definitions

N/A

Defaults

CSNP authentication check is enabled by default.

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

Use the **no** form of this command to prevent the CSNP authentication.

Examples

```
-> ip isis csnp-auth
-> no ip isis csnp-auth
```

Release History

Release 6.2.1; command was introduced.

Related Commands

ip isis level csnp-auth	Configures CSNP authentication for specific IS-IS levels.
show ip isis status	Displays the IS-IS status.

MIB Objects

```
vRtrIsisTable
   vRtrIsisCsnpAuthentication
```

ip isis hello-auth

Enables or disables the authentication of Hello PDUs globally.

ip isis hello-auth

no ip isis hello-auth

Syntax Definitions

N/A

Defaults

Authentication check of Hello PDUs is enabled by default.

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

Use the **no** form of this command to prevent the authentication of Hello packets.

Examples

```
-> ip isis hello-auth
-> no ip isis hello-auth
```

Release History

Release 6.2.1; command was introduced.

Related Commands

ip isis level hello-auth	Enables or disables the authentication of Hello PDUs for specific IS-IS levels.
show ip isis status	Displays the IS-IS status.

MIB Objects

```
vRtrIsisTable
   vRtrIsisHelloAuthentication
```

ip isis psnp-auth

Enables or disables the authentication of Partial Sequence Number PDUs (PSNPs).

ip isis psnp-auth

no ip isis psnp-auth

Syntax Definitions

N/A

Defaults

PSNP authentication check is enabled by default.

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

Use the **no** form of this command to prevent the authentication of PSNP packets.

Examples

```
-> ip isis psnp-auth
-> no ip isis psnp-auth
```

Release History

Release 6.2.1; command was introduced.

Related Commands

ip isis level psnp-auth	Configures the PSNP authentication for specific IS-IS levels.
show ip isis status	Displays the IS-IS status.

MIB Objects

```
vRtrIsisTable
   vRtrIsisPsnpAuthentication
```

ip isis lsp-lifetime

Configures the time interval for which Link State PDUs generated by a router are considered valid by other routers in the same domain.

ip isis lsp-lifetime *seconds*

no ip isis lsp-lifetime

Syntax Definitions

seconds	Validity interval in seconds.The valid range is 350–65535.

Defaults

parameter	default
seconds	1200

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

Use the **no** form of this command to restore the default value.

Examples

```
-> ip isis lsp-lifetime 760
-> no ip isis lsp-lifetime
```

Release History

Release 6.2.1; command was introduced.

Related Commands

ip isis interface lsp-pacing-interval	Configures the time interval between IS-IS LSP PDUs sent from the specified interface.
show ip isis status	Displays the IS-IS status.
show ip isis database	Displays IS-IS LSP database information of the adjacent routers.

MIB Objects

```
vRtrIsisTable
  vRtrIsisLspLifetime
```

ip isis lsp-wait

Configures the intervals between the first, second and subsequently generated LSPs.

ip isis lsp-wait {max-wait | initial-wait | second-wait} *seconds*

no ip isis lsp-wait {max-wait | initial-wait | second-wait}

Syntax Definitions

max-wait	Specifies the maximum interval between two successive LSPs, in seconds. The valid range is 1–120.
initial-wait	Specifies the initial LSP generation delay, in seconds. The valid range is 0–100.
second-wait	Specifies the time interval between the first and second generated LSPs, in seconds. The valid range is 1–100.
seconds	Specifies the time interval.

Defaults

parameter	default
seconds **(max-wait)**	5
seconds **(initial-wait)**	0
seconds **(second-wait)**	1

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to restore the default value.
- Successive LSPs are generated at increasing **second-wait** interval until a maximum value is reached.

Examples

```
-> ip isis lsp-wait max-wait 25
-> no ip isis lsp-wait initial-wait
```

Release History

Release 6.2.1; command was introduced.

Related Commands

ip isis interface lsp-pacing-interval	Configures the time interval between IS-IS LSP PDUs sent from the specified interface.
show ip isis status	Displays the IS-IS status.

MIB Objects

```
vRtrIsisTable
   vRtrIsisLspInitialWait
   vRtrIsisLspSecondWait
   vRtrIsisLspMaxWait
```

ip isis spf-wait

Configures the intervals between the first, second, and subsequent SPF calculations.

ip isis spf-wait {max-wait *seconds* **| initial-wait** *milliseconds***| second-wait** *milliseconds***}**

no ip isis spf-wait {max-wait | initial-wait | second-wait}

Syntax Definitions

max-wait *seconds*	Specifies the maximum interval between two successive SPF calculations, in seconds. The valid range is 1–120 seconds.
initial-wait *milliseconds*	Specifies the initial SPF calculation delay, in milliseconds. The valid range is 10–100000 milliseconds.
second-wait *milliseconds*	Specifies the interval between first and second generated SPFs, in milliseconds. The valid range is 1–100000 milliseconds.

Defaults

parameter	default
max-wait *seconds*	10
initial-wait *milliseconds*	1000
second-wait *milliseconds*	1000

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to restore the default value.
- Successive SPF calculations are generated at exponentially increasing **second-wait** interval until a maximum value is reached.

Examples

```
-> ip isis spf-wait max-wait 25
-> no ip isis spf-wait initial-wait
```

Release History

Release 6.2.1; command was introduced.

Related Commands

show ip isis status	Displays the IS-IS status.

MIB Objects

vRtrIsisTable

- vRtrIsisSpfWait
- vRtrIsisSpfInitialWait
- vRtrIsisSpfSecondWait

ip isis summary-address

Adds or deletes the summary address.

ip isis summary-address {*ip-prefix/mask* **|** *ip-prefix* **[**/*netmask***]} {level-1 | level-2 | level-1/2}**

no ip isis summary-address {*ip-prefix/mask* **|** *ip-prefix* **[**/*netmask***]}**

Syntax Definitions

ip-prefix/mask	Specifies the IP prefix in dotted decimal notation and the mask length.
ip-prefix	Specifies the IP prefix in dotted decimal notation.
/netmask	Specifies the subnet mask in dotted decimal notation.
level-1	Specifies the IS-IS level as Level-1.
level-2	Specifies the IS-IS level as Level-2.
level-1/2	Specifies the IS-IS level as Level-1/2.

Defaults

parameter	default
level-1 | level-2 | level-1/2	**level-1/2**

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to remove an already configured summary address.
- Native IS-IS routes can only be summarized into Level-2 from the Level-1 database.
- It is not possible to summarize IS-IS internal routes at Level-1, although it is possible to summarize external (redistributed) routes at Level-1.
- IS-IS routes are not summarised by default.

Examples

```
-> ip isis summary-address 10.0.0.0/8 level-2
-> no ip isis summary-address 10.0.0.0/8
```

Release History

Release 6.2.1; command was introduced.
Release 6.3.1; **level-1/2** parameter was added, *netmask* parameter is optional.

Related Commands

show ip isis summary-address Displays the IS-IS summary address database.

MIB Objects

```
vRtrIsisSummaryTable
   vRtrIsisSummRowStatus
```

ip isis overload

Enables and configures the IS-IS router to operate in the overload state for a specified time period.

ip isis overload [timeout *seconds***]**

no ip isis overload [timeout]

Syntax Definitions

timeout *seconds*	Specifies the timeout interval, in seconds. The valid range is 60–1800.

Defaults

By default, the IS-IS overload state is disabled.

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to make the router exit the overload state.
- If the time period is not specified, the router remains in the overload state for an infinite period.
- During normal operation, the router may be forced to enter an overload state due to a lack of resources. When in the overload state, the router is used only if the destination route is directly reachable by the router i.e., it will not be used for other transit traffic.
- This command can be used when the router is overloaded or before executing a shutdown command to divert traffic around the router.

Examples

```
-> ip isis overload timeout 70
-> no ip isis overload timeout
```

Release History

Release 6.2.1; command was introduced..

Related Commands

ip isis overload-on-boot	Configures the IS-IS router to be in the overload state during bootup for a specified time period.
show ip isis status	Displays the IS-IS status.

MIB Objects

```
isisSysTable
   isisSysSetOverload
vRtrIsisTable
   vRtrIsisOverloadTimeout
```

ip isis overload-on-boot

Configures the IS-IS router to be in the overload state after bootup for a specified time period.

ip isis overload-on-boot [timeout *seconds***]**

no ip isis overload-on-boot [timeout *seconds***]**

Syntax Definitions

timeout *seconds*	Specifies the timeout interval, in seconds. The valid range is 60–1800.

Defaults

By default, the IS-IS router will not be in the overload state.

parameter	default
timeout *seconds*	60

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to prevent the router from entering the overload state after bootup.
- The router in the overload state is used only if there is no alternate path to reach the destination.
- This command configures the router after bootup in the overload state until the timeout timer expires or a timeout value is specified in the **no** form of this command.
- The **no overload** command does not influence the overload-on-boot function.

Examples

```
-> ip isis overload-on-boot timeout 80
-> no ip isis overload-on-boot timeout
```

Release History

Release 6.2.1; command was introduced.

Related Commands

ip isis overload	Sets the IS-IS router to operate in the overload state.
show ip isis status	Displays the IS-IS status.

MIB Objects

```
vRtrIsisTable
   vRtrIsisOverloadOnBoot
   vRtrIsisOverloadOnBootTimeout
```

ip isis graceful-restart

Configures graceful restart of the router. It allows routing protocols to reconverge faster, minimizing service interruption.

ip isis graceful-restart

no ip isis graceful-restart

Syntax Definitions

N/A

Defaults

Graceful restart is disabled on the router by default.

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to disable graceful restart and remove the graceful restart configuration from the IS-IS router.
- When graceful restart is enabled, the router can either be a helper (which helps a neighbor router to restart) or a restarting router, or both. In the current release, only the helper mode of a router is supported.

Examples

```
-> ip isis graceful-restart
-> no ip isis graceful-restart
```

Release History

Release 6.2.1; command was introduced.

Related Commands

ip isis graceful-restart helper	Configures the helper mode of routers for graceful restart.
show ip isis status	Displays the IS-IS status.

MIB Objects

```
vRtrIsisTable
   vRtrIsisGracefulRestart
```

ip isis graceful-restart helper

Administratively enables and disables the IS-IS router to operate in the helper mode in response to a router performing a graceful restart.

ip isis graceful-restart helper {enable | disable}

Syntax Definitions

enable	Enables the helper mode on the router.
disable	Disables the helper mode on the router.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

- When graceful restart is enabled, the helper mode is enabled by default.
- When graceful restart helper is enabled on a router, it can help other restarting routers.

Examples

```
-> ip isis graceful-restart helper disable
```

Release History

Release 6.2.1; command was introduced.

Related Commands

ip isis graceful-restart	Configures graceful restart on the router.
show ip isis status	Displays the IS-IS status.

MIB Objects

```
vRtrIsisTable
   vRtrIsisGRHelperMode
```

ip isis strict-adjacency-check

Enables or disables the adjacency check configuration on the router.

ip isis strict-adjacency-check {enable | disable}

Syntax Definitions

enable	Enables the adjacency check configuration on the router.
disable	Disables the adjacency check configuration on the router.

Defaults

By default, the adjacency check configuration is disabled.

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

- When the adjacency check configuration is enabled, both routers have to run the same IP version only in the IS-IS protocol to form an adjacency.
- When the adjacency check configuration is disabled, one common IP version running between two routers is enough to form an adjacency in the IS-IS protocol.

Examples

```
-> ip isis strict-adjacency-check enable
```

Release History

Release 6.2.1; command was introduced.

Related Commands

show ip isis status	Displays the IS-IS status.

MIB Objects

```
vRtrIsisTable
   vRtrIsisStrictAdjacencyCheck
```

ip isis level auth-type

Enables authentication and configures the authentication types for specific IS-IS levels.

ip isis level {1 | 2} auth-type {simple {key *key* | **encrypt-key** *encrypt-key***} | md5 {key** *key* **| encrypt-key** *encrypt-key***} | none}**

Syntax Definitions

1	Specifies the IS-IS level as Level-1.
2	Specifies the IS-IS level as Level-2.
simple	Simple authentication will be used.
md5	Specifies that MD5 authentication algorithm will be used. Hash-key will be used in MD5 authentication.
key	Key will be plain text ASCII up to 118 characters. Use quotes around string if the key contains multiple words with spaces between them.
encrypt-key	The key in hexadecimal format to provide security consideration on the authentication key. Configuration snapshot always displays authentication key in the encrypted form.
none	No authentication will be used.

Defaults

parameter	default
simple | **md5** | **none**	**none**

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

- Simple authentication uses only a text string as the password in the packet. This helps to protect the routers from a configuration mishap. MD5 authentication is used to protect the system from malicious actions.
- MD5 authentication is used to encrypt the information that is sent over the network. MD5 authentication uses shared secret key. The Key is used to sign the packets with an MD5 checksum to sign the packet, so that the packets cannot be tampered. As the key is not included in the packet, snooping the key is not possible.
- Use the Key parameter to configure the password for Simple or MD5 authentication. Alternatively, use the *encrypt-key* parameter to configure the password by supplying the encrypted form of the password as the encrypt-key. The Configuration snapshot always displays the password in the encrypted form. You should use only this *key* parameter during the CLI configuration.

- If the *encrypt-key* parameter is used to configure the password through the CLI, then its value should be the same as the one that appears in the configuration snapshot. Only valid system generated values are accepted as encrypt-key.
- This command overrides the global configuration of IS-IS authentication type.
- This command also sets the password or hash-key according to the type of authentication.
- By default, the authentication is disabled and no authentication type is configured.

Examples

```
-> ip isis level 2 auth-type simple key rachel
-> ip isis level 2 auth-type md5 encrypt-key 7a1e441a014b4030
```

Release History

Release 6.2.1; command was introduced.
Release 6.3.1; **key** and **encrypt-key** parameters were added.

Related Commands

ip isis auth-type	Enables authentication and configures the authentication type of IS-IS protocol globally.
show ip isis status	Displays the IS-IS status.

MIB Objects

```
vRtrIsisLevelTable
   vRtrIsisLevelAuthType
   vRtrIsisLevelAuthKey
```

ip isis level hello-auth

Enables or disables the authentication of Hello PDUs for specific IS-IS levels.

ip isis level {1 | 2} hello-auth

no ip isis level {1 | 2} hello-auth

Syntax Definitions

1	Specifies the IS-IS level as Level-1.
2	Specifies the IS-IS level as Level-2.

Defaults

Authentication check of Level Hello PDUs is enabled by default.

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to prevent the authentication of Hello packets at the specified IS-IS level.
- This command overrides the global configuration of IS-IS Hello authentication.

Examples

```
-> ip isis level 1 hello-auth
-> no ip isis level 1 hello-auth
```

Release History

Release 6.2.1; command was introduced.

Related Commands

ip isis hello-auth	Enables or disables the authentication of Hello PDUs globally.
show ip isis status	Displays the IS-IS status.

MIB Objects

```
vRtrIsisLevelTable
   vRtrIsisLevelHelloAuthentication
```

ip isis level csnp-auth

Enables or disables the CSNP authentication for specific IS-IS levels.

ip isis level {1 | 2} csnp-auth

no ip isis level {1 | 2} csnp-auth

Syntax Definitions

1	Specifies the IS-IS level as Level-1.
2	Specifies the IS-IS level as Level-2.

Defaults

CSNP authentication check for specific IS-IS levels is enabled by default.

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to prevent the authentication of CSNPs at the specified IS-IS level.
- This command overrides the global configuration of IS-IS CSNP authentication.

Examples

```
-> ip isis level 1 csnp-auth
-> no ip isis level 1 csnp-auth
```

Release History

Release 6.2.1; command was introduced.

Related Commands

ip isis csnp-auth	Enables or disables the authentication of CSNPs.
show ip isis status	Displays the IS-IS status.

MIB Objects

```
vRtrIsisLevelTable
   vRtrIsisLevelCsnpAuthentication
```

ip isis level psnp-auth

Enables or disables PSNP authentication for specific IS-IS levels.

ip isis level {1 | 2} psnp-auth

no ip isis level {1 | 2} psnp-auth

Syntax Definitions

1	Specifies the IS-IS level as Level-1.
2	Specifies the IS-IS level as Level-2.

Defaults

PSNP authentication check for specific IS-IS levels is enabled by default.

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to prevent the authentication of PSNPs at the specified IS-IS level.
- This command overrides the global configuration of IS-IS PSNP authentication.

Examples

```
-> ip isis level 1 psnp-auth
-> no ip isis level 1 psnp-auth
```

Release History

Release 6.2.1; command was introduced.

Related Commands

ip isis psnp-auth	Enables or disables the authentication of PSNPs.
show ip isis status	Displays the IS-IS status.

MIB Objects

```
vRtrIsisLevelTable
   vRtrIsisLevelPsnpAuthentication
```

ip isis level wide-metrics-only

Enables the wide metrics in LSPs for specific IS-IS levels.

ip isis level {1 | 2} wide-metrics-only

no ip isis level {1 | 2} wide-metrics-only

Syntax Definitions

1	Specifies the IS-IS level as Level-1.
2	Specifies the IS-IS level as Level-2.

Defaults

By default, wide metrics is disabled.

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to restore the narrow metric (1–63).
- Wide metrics are used for improved granularity of metrics.
- Numeric values above 63 indicate wide metrics.

Examples

```
-> ip isis level 1 wide-metrics-only
-> no ip isis level 1 wide-metrics-only
```

Release History

Release 6.2.1; command was introduced.

Related Commands

show ip isis status	Displays the IS-IS status.

MIB Objects

```
vRtrIsisLevelTable
   VrtrIsisLevelWideMetricsOnly
```

show ip isis adjacency

Displays information about IS-IS adjacent routers.

show ip isis adjacency [{system-id *nbr_sys_id* | **interface** *interface_name***}] [detail]**

Syntax Definitions

nbr_sys_id	The system ID of the neighbor router.
interface_name	The name of the IS-IS interface.
detail	Indicates that the output is displayed in a detailed manner.

Defaults

By default adjacency information for all the neighbor routers are displayed.

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

Use *the nbr_sys_id* or *interface_name* parameter with this command to view the adjacency information for a specific neighbor.

Examples

```
-> show ip isis adjacency
================================================================================
ISIS Adjacency
================================================================================
System ID          Type     State     Hold      Interface   Host-name
--------------------------------------------------------------------------------
1720.2116.0051      L2        UP        8         vlan2      HostA
1720.2116.0051      L1        UP        8         vlan2      HostA
1720.2116.0051      L1        UP        8         vlan3      HostA
1720.2116.0051      L2        UP        8         vlan3      HostA
--------------------------------------------------------------------------------
Adjacency : 4
================================================================================
```

output definitions

System ID	The system ID of the adjacent router. The system ID is a fixed size, six octet field in the NSAP. In an IS-IS routing domain, each router is identified by a 6-octet hexadecimal system ID.
Type	The level (**LI, L2,** or **L1/L2**) of the adjacent router.
State	The state of the adjacent router (**Up** or **Down**).
Hold	The Hold time of the adjacent router.
Interface	The interface name of the adjacent router.

output definitions

Host-name	The hostname of the adjacent router.
Adjacencies	The total number of adjacent routers.

```
-> show ip isis adjacency detail
================================================================================
ISIS adjacency
================================================================================
--------------------------------------------------------------------------------
SystemID     : 1720.2116.0051       SNPA       : 00:d0:95:f3:0f:08
Interface    : vlan2                Up Time    : SUN OCT 01 05:18:51 2006
State        : UP                   Priority   : 64
Nbr Sys Type : L2                   L.CircType : L1L2
Hold Time    : 6                    Max Hold   : 9
Adj Level    : L2                   Host-name  : HostA
IPv4 Neighbor      : 2.2.2.3
Restart Support    : Disabled
Restart Status     : Not currently being helped
Restart Suppressed : Disabled
--------------------------------------------------------------------------------
SystemID     : 172.2116.0052        SNPA       : 00:d0:95:f3:0f:08
Interface    : vlan2                Up Time    : SUN OCT 01 05:18:51 2006
State        : UP                   Priority   : 64
Nbr Sys Type : L1                   L.CircType : L1L2
Hold Time    : 6                    Max Hold   : 9Adj Level    : L2IPv4
Neighbor      : 2.2.2.3
Restart Support    : Disabled
Restart Status     : Not currently being helped
Restart Suppressed              :   Disabled
--------------------------------------------------------------------------------
Adjacency : 2
================================================================================
```

output definitions

SystemID	The system ID of the adjacent router. The system ID is a fixed size, six octet field in the NSAP. In an IS-IS routing domain, each router is identified by a 6-octet hexadecimal system ID.
Interface	The interface name of the adjacent router.
State	The state of the adjacent router (**Up** or **Down**).
Adj Level	The adjacency level (**L1** or **L2**) of the router.
Nbr Sys Type	The type of the neighboring router(**L1, L2** or **L1L2**)
Hold Time	The Hold time of the adjacent router.
IPv4 Neighbor	The 32-bit IP address of the neighbor.
Restart Support	Indicates if graceful restart is **enabled** or **disabled**.
Restart Status	Indicates whether the router is currently helping an adjacent router to restart.
Restart Suppressed	Indicates whether the advertisement of LSPs are suppressed (**enabled**) or not (**disabled**) as per the request of adjacent router.
SNPA	The SNPA address of the adjacent router.
Up Time	Indicates the time period in seconds, during which the router was in the adjacency.

output definitions

Priority	The priority of the adjacent router.
Host-name	The hostname of the adjacent router.
L. CircType	Indicates the level circuit type (**L1, L2** or **L1L2**) of the adjacent router.
Max Hold	Indicates the maximum Hold time of the adjacent router.

Release History

Release 6.2.1; command was introduced.
Release 6.3.1; System ID/HostName field removed; System ID, Host-name, and IPv4 neighbor fields added.

Related Commands

clear ip isis adjacency	Clears and resets the IS-IS adjacency database.

MIB Objects

```
isisISAdjTable
   isisISAdjIndex
   isisISAdjState
   isisISAdjNeighSNPAAddress
   isisISAdjNeighSysType
   isisISAdjNeighSysID
   isisISAdjUsage
   isisISAdjNeighPriority
   isisISAdjUpTime
   isisISAdjHoldTimer
vRtrIisisISAdjTable
   vRtrIsisISAdjCircLevel
   vRtrIsisISAdjRestartSupport
   vRtrIsisISAdjRestartSupressed
   vRtrIsisISAdjExpireIn
   vRtrIsisISAdjNeighborIP
    vRtrIsisISAdjRestartStatus
```

show ip isis database

Displays IS-IS LSP database information of the adjacent routers.

show ip isis database [{system_id *system_id* **| lsp_id** *lsp_id***}] [detail] [level {1** | **2}]**

Syntax Definitions

system_id	The system ID of the router.
lsp_id	The LSP ID.
detail	Indicates that the output is displayed in a detailed manner.
level	Indicates the IS-IS level, either **1** or **2**.

Defaults

By default the entire LSP database is displayed.

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

- Use *system-id* or *lsp-id* parameter with this command to view specific LSP database information.
- Use the **level** parameter with this command to view the LSP database information of a particular level.

Examples

```
-> show ip isis database
Legends : P            =  The Partition repair bit is set
OV    = The overload bit is set
ATT   = The Attach bit is set
L1    = Specifies a Level 1 IS type
L2    = Specifies a Level 2 IS type
================================================================
ISIS Database
================================================================
LSP ID                    Sequence  Checksum  Lifetime  Attributes
----------------------------------------------------------------
Displaying level-1 database
----------------------------------------------------------------
1720.2116.0051.00-00      0x44      0xb664    919          L1L2
level-1 LSP count : 1

Displaying level-2 database
----------------------------------------------------------------
1720.2116.0051.00-00      0x45      0xb465    1083         L1L2
level-2 LSP count : 1
================================================================
```

output definitions

LSP ID	The LSP ID. Indicates the system ID and the pseudo-node ID of the originating router.
Sequence	The sequence number of the LSP. The sequence number is a value used to identify old and duplicate LSPs.
Checksum	The checksum value of the LSP.
Lifetime	The number of seconds the LSP remains valid. The LSP lifetime value of zero indicates that this LSP is being removed from the Link State Database of all the routers.
Attributes	The level capability of the router.
LSP Count	The number of LSPs in the Link State Database.

```
show isis database detail
   Legends : P           =     The Partition repair bit is set
             OV    =  The overload bit is set
             ATT   =  The Attach bit is set
             L1    =  Specifies a Level 1 IS type
             L2    =  Specifies a Level 2 IS type
=========================================================================
ISIS Database
=========================================================================
Displaying level-1 database
-------------------------------------------------------------------
LSP ID        : 1720.2116.0051.00-00             Level     : L1
Sequence      : 0x44       Checksum  : 0xb664    Lifetime  : 818
Version       : 1          Pkt Type  : 18        Pkt Ver   : 1
Attributes    : L1L2       Max Area  : 3
SysID Len     : 6          Used Len  : 635       Alloc Len : 1489

TLVs  :
Area Addresses      :
   Area Address     :  (3)  49.0000
Supp protocols      :
   Protocols        :  Ipv4 , Ipv6
IS-Hostname         :
   Hostname         :  HostA
IS Neighbors        :
   Virtual Flag     :  0
   Neighbor         :  1720.2116.0052.00  Metric : 10 (I)
IPv4 I/F Address    :
   IP Address       : 172.21.160.51
   IP Address       : 172.21.160.52
IPv4 Internal Reach :
   IP Prefix        : 16.16.16.0/24 (Dir.: UP )   Metric  : 10 (I)
   IP Prefix        : 17.17.17.0/24 (Dir.: UP )   Metric  : 10 (I)
IPv4 External Reach :
   IP Prefix        : 24.24.24.0/24 (Dir.: UP )   Metric  : 10 (E)
   IP Prefix        : 25.25.25.0/24 (Dir.: UP )   Metric  : 10 (E)

level-1 LSP count : 1

Displaying level-2 database
-------------------------------------------------------------------
```

```
LSP ID        : 1720.2116.0051.00-00            Level     : L2
Sequence      : 0x45       Checksum  : 0xb465   Lifetime  : 981
Version       : 1          Pkt Type  : 20       Pkt Ver   : 1
Attributes    : L1L2       Max Area  : 3
SysID Len     : 6          Used Len  : 635      Alloc Len : 1489

TLVs  :
Area Addresses      :
   Area Address     :  (3) 49.0000
Supp protocols      :
   Protocols        :  Ipv4  Ipv6
IS-Hostname         :
   Hostname         :  HostA
IS Neighbors        :
   Virtual Flag     :  0
   Neighbor         :  1720.2116.0052.00  Metric : 10 (I)
IPv4 I/F Address    :
   IP Address       : 172.21.160.51
   IP Address       : 172.21.160.52
IPv4 Internal Reach :
   IP Prefix        : 16.16.16.0/24 (Dir.: UP )   Metric  : 10 (I)
   IP Prefix        : 17.17.17.0/24 (Dir.: UP )   Metric  : 10 (I)
IPv4 External Reach :
   IP Prefix        : 24.24.24.0/24 (Dir.: UP )   Metric  : 10 (E)
   IP Prefix       : 25.25.25.0/24 (Dir.: UP )   Metric  : 10 (E)

level-2 LSP count : 1

================================================================
```

output definitions

LSP ID	The LSP ID. Indicates the system ID and the pseudo-node ID of the originating router.
Sequence	The sequence number of the LSP. The Sequence number is a value used to identify old and duplicate LSPs.
Checksum	The checksum value of the LSP.
Lifetime	The number of seconds the LSP remains valid. The LSP lifetime value of zero indicates that this LSP is being removed from the Link State Database of all the routers.
Version	The version of the IS-IS protocol that has generated the LSP.
Pkt Type	The IS-IS PDU type number derived from the PDU header, which can be **18** or **20**. The number 18 represents L1 LSP PDU type and 20 represents L2 LSP PDU type.
Pkt Ver	The version of the IS-IS protocol that has generated the packet.
Attributes	The level capability of the router.
Max Area	The Maximum number of areas supported by the originating router of the LSP.
SysID Len	The length of the system-id as used by the originating router.
Used Len	The length used by the LSP.
Alloc Len	The length allocated for the LSP to be stored.
Area Address	The area ID of the router.
Supp protocols	The network layer protocols that are supported.
IS-Host Name	The host name of the router.
System ID	The system ID of the adjacent router. The system ID is a fixed size, six octet field in the NSAP. In an IS-IS routing domain, each router is identified by a 6-octet hexadecimal system ID.
IS Neighbors	The list of reachable IS-IS neighbors.
IPv4 Internal Reach	The list of IS-IS internal routes.
IP Prefix	The IP address and subnet mask of the destination.
Metrics	The metric value to reach the destination.
IPv4 External Reach	The list of external IS-IS routes.
level-1 LSP Count	The number of Level-1 LSPs.
level-2 LSP Count	The number of Level-2 LSPs.

Release History

Release 6.2.1; command was introduced..

Related Commands

show ip isis hostname	Displays the database of IS-IS host name and its corresponding system ID.
clear ip isis lsp-database	Clears and resets the IS-IS LSP database information.

MIB Objects

```
vRtrIsisLSPTable
   vRtrIsisLSPId
   vRtrIsisLSPSeq
   vRtrIsisLSPChecksum
   vRtrIsisLSPLifetimeRemain
   vRtrIsisLSPAttributes
   vRtrisisLSPVersion
   vRtrIsisLSPPktType
   vRtrIsisLSPSysIdLen
   vRtrIsisLSPAllocLen
   vRtrIsisLSPMaxArea
   vRtrIsisLSPBuff
   vRtrisisLSPUsedLen
```

show ip isis hostname

Displays the database of IS-IS host name and its corresponding system ID.

show ip isis hostname

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show ip isis hostname
Hosts
================================================================================
System Id                      Hostname
--------------------------------------------------------------------------------
1800.0000.0002                 core_west
1800.0000.0005                 core_east
1800.0000.0008                 asbr_west
1800.0000.0009                 asbr_east
1800.0000.0010                 abr_sjc
1800.0000.0011                 abr_lax
1800.0000.0012                 abr_nyc
1800.0000.0013                 abr_dfw
1800.0000.0015                 dist_oak
1800.0000.0018                 dist_nj
1800.0000.0020                 acc_nj
1800.0000.0021                 acc_ri
1800.0000.0027                 dist_arl
1800.0000.0028                 dist_msq
1800.0000.0029                 acc_arl
```

output definitions

System Id	The system ID of the router. The system ID is a fixed size, six octet field in the NSAP. In an IS-IS routing domain, each router is identified by a 6-Octet hexadecimal system ID.
Hostname	The host name of the router.

Release History

Release 6.2.1; command was introduced.

Related Commands

show ip isis adjacency	Displays information about IS-IS adjacent routers.
show ip isis database	Displays IS-IS LSP database information of the adjacent routers
ip isis area-id	Configures the area ID for the router.

MIB Objects

```
vRtrIsisHostnameTable
   vRtrIsisSysID
   vRtrIsisHostname
```

show ip isis routes

Displays the IS-IS route information from the routing table.

show ip isis routes

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show isis routes

================================================================================
ISIS Routes
================================================================================
Prefix              Metric        Lvl/Type   SPF-num  Nexthop    System ID
--------------------------------------------------------------------------------
1.1.1.0/24          10            1/Int       7       0.0.0.0    1720.2116.0051
2.2.2.0/24          10            1/Int       1       0.0.0.0    1720.2116.0051
3.3.3.0/24          10            1/Int       1       0.0.0.0    1720.2116.0051
4.4.4.0/24          10            1/Int       1       0.0.0.0    1720.2116.0051
5.5.5.0/24          10            1/Int       1       0.0.0.0    1720.2116.0051
6.6.6.0/24          10            1/Int       1       0.0.0.0    1720.2116.0051
--------------------------------------------------------------------------------
Routes : 8
================================================================================
```

output definitions

Prefix	The IP prefix and mask of the destination routes.
Metric	The cost to reach the destination route.
Lvl/Type	The level and route type of the routes.
SPF-num	The version of the SPF calculation used to select the route.
Nexthop	The Next Hop address to reach the destination.
System ID	The system ID of the adjacent router. The system ID is a fixed size, six octet field in the NSAP. In an IS-IS routing domain, each router is identified by a 6-octet hexadecimal system ID.

Release History

Release 6.2.1; command was introduced.

Related Commands

N/A

MIB Objects

```
vRtrIsisRouteTable
   vRtrIsisRouteLevel
   vRtrIsisRouteSpfVersion
   vRtrIsisRouteType
   vRtrisisRouteDest
   vRtrIsisRouteNexthopIP
   vRtrIsisRouteNexthopSysID
   vRtrIsisRouteMetric
   vRtrIsisRouteMask
```

show ip isis spf

Displays the IS-IS SPF calculation information.

show ip isis spf [detail]

Syntax Definitions

detail	Indicates that the output is displayed in a detailed manner.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show ip isis spf
=========================================================================
ISIS Path Table
=========================================================================
Node                          Interface           Nexthop
-------------------------------------------------------------------------
1720.2116.0051.00             vlan2              1720.2116.0051
1720.2116.0051.00             vlan3              1720.2116.0051
1720.2116.0051.00             vlan4              1720.2116.0051
1720.2116.0051.00             vlan5              1720.2116.0051
1720.2116.0051.00             vlan2              1720.2116.0051
1720.2116.0051.00             vlan3              1720.2116.0051
1720.2116.0051.00             vlan4              1720.2116.0051
-------------------------------------------------------------------
SPF count: 7
=========================================================================
```

output definitions

Node	The system ID of the routers.
Interface	The Interface name of the router.
Nexthop	The system ID of the Next Hop router.

```
-> show ip isis spf detail

=========================================================================
ISIS Path Table
=========================================================================
Node       : 1720.2116.0051.00      Metric   : 10
Interface  : vlan2                  SNPA     : 00:d0:95:f3:0f:08
```

```
Nexthop    : 1720.2116.0051


Node       : 1720.2116.0051.00      Metric   : 10
Interface  : vlan3                  SNPA     : 00:d0:95:f3:0f:08
Nexthop    : 1720.2116.0051


Node       : 1720.2116.0051.00      Metric   : 10
Interface  : vlan4                  SNPA     : 00:d0:95:f3:0f:08
Nexthop    : 1720.2116.0051


Node       : 1720.2116.0051.00      Metric   : 10
Interface  : vlan5                  SNPA     : 00:d0:95:f3:0f:08
Nexthop    : 1720.2116.0051
--------------------------------------------------------------------------
SPF count: 4
==========================================================================
```

output definitions

Node	The system ID of the routers.
Metric	The metric value used for SPF calculations.
Interface	The interface name of the router.
SNPA	The SNPA address of the router.
Nexthop	The system ID of the Next Hop router.
SPF count	The number of SPF calculations done by the router.

Release History

Release 6.2.1; command was introduced.

Related Commands

show ip isis spf-log	Displays the IS-IS SPF log.
show ip isis status	Displays the IS-IS status.

MIB Objects

```
vRtrIsisPathTable
   vRtrIsisPathID
   vRtrIsisPathIfIndex
   vRtrIsisPathNHopSysID
   vRtrIsisPathMetric
   vRtrIsisPathSNPA
```

show ip isis spf-log

Displays the IS-IS SPF log.

show ip isis spf-log [detail]

Syntax Definitions

detail	Indicates that the output is displayed in a detailed manner.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

This command displays the last 20 IS-IS SPF events.

Examples

```
-> show ip isis spf-log
ISIS SPFLog
================================================================================
When       Duration       L1-Nodes      L2-Nodes      Event-Count
--------------------------------------------------------------------------------
01/30/2005 11:01:54 <0.01s 1              1               3
--------------------------------------------------------------------------------
Log Entries : 1
```

output definitions

When	The date on which the SPF calculation was completed.
Duration	The time duration of the event.
L1-Nodes	The number of Level-1 nodes.
L2-Nodes	The number of Level-2 nodes.
Event-Count	The number of SPF calculations.
Log Entries	The total number of log entries.

```
-> show ip isis spf-log detail

================================================================================
ISIS SPFLog
================================================================================
SpfTimeStamp          :  SUN OCT 01 05:15:29 2006
spfRunTime            :  0
Spf Involved L1 Nodes :  69
Spf Involved L2 Nodes :  71
Spf Event-count       :  169
Last TriggeredLspId   :  0020.0200.2001.00-4a
```

```
Spf Trigger Reason    :  newAdjacency(0) ,lspExpired(8) ,lspChanged(10)
SpfTimeStamp          :  SUN OCT 01 05:15:46 2006
spfRunTime            :  0
Spf Involved L1 Nodes :  72
Spf Involved L2 Nodes :  72
Spf Event-count       :  227
Last TriggeredLspId   :  0020.0200.2001.00-4a
Spf Trigger Reason    :  newAdjacency(0) ,lspExpired(8) ,lspChanged(10)
--------------------------------------------------------------------------------
Log Entries : 2
================================================================================
```

output definitions

SpfTimeStamp	The timestamp when the SPF run started on the system.
spfRunTime	The time (in hundredths of a second) required to complete the SPF run.
Spf Involved L1 Nodes	The number of Level-1 nodes involved in the SPF calculation.
Spf Involved L1 Nodes	The number of Level-2 nodes involved in the SPF calculation.
Spf Event-count	The number of SPF events that triggered the SPF calculation.
Last TriggeredLspId	The LSP ID of the last LSP processed before the SPF run.
Spf trigger Reason	Indicates the reasons (**newAdjacency**, **lspExpired**, or **lspChanged**) for SPF calculations.
Log Entries	The number of SPF logs.

Release History

Release 6.2.1; command was introduced.

Related Commands

show ip isis spf	Displays the IS-IS SPF calculation information.
clear ip isis spf-log	Clears and resets the IS-IS SPF log information.

MIB Objects

```
vRtrIsisSpfLogTable
   vRtrIsisSpfRunTime
   vRtrIsisSpfL1Nodes
   VRtrIsisSpfL2Nodes
   vRtrIsisSpfEventCount
   vRtrIsisSpfLastTriggerLSPId
   vRtrIsisSpfTriggerReason
```

show ip isis statistics

Displays the IS-IS statistics information.

show ip isis statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show ip isis statistics
=============================================================================
ISIS Statistics
=============================================================================
ISIS Instance             : 1                            SPF Runs         : 44
Purge Intiated           : 0                            LSP Regens       : 54
CSPF Statistics
Requests                  : 0                            Request Drops    : 0
Paths Found               : 0                            Paths Not Found  : 0
-----------------------------------------------------------------------------
PDU Type  Received  Processed  Dropped Sent       Retransmitted
-----------------------------------------------------------------------------
LSP       185         184       1       54         0
IIH       8382        8382      0       2796       0
CSNP      3352        352       0       0          0
PSNP      0           0         0       4          0

Unknown   0           0         0       0          0
```

output definitions

ISIS Instance	The number of IS-IS instances.
SPF Runs	The number of SPF calculations that have been performed.
Purge Intiated	The number of purges that the system initiated. A purge is initiated if the router decides that a link-state PDU must be removed from the database.
LSP Regens	The number of LSPs that have been regenerated. An LSP is regenerated when it nears the end of its lifetime and has not changed.
Requests	The number of CSNP requests received.

output definitions (continued)

Request Drops	The number of CSNP requests that are dropped.
Paths Found	The number of paths found.
Paths Not Found	The number of paths not found.
PDU Type	The type of PDU.
Received	The number of PDUs received since IS-IS started or since the statistics were set to zero.
Processed	The number of PDUs that are processed (number of PDUs received less the number dropped).
Dropped	The number of PDUs that are dropped.
Sent	The number of PDUs transmitted since IS-IS started or since the statistics were set to zero.
Retransmitted	The number of PDUs that are retransmitted.

Release History

Release 6.2.1; command was introduced.

Related Commands

clear ip isis statistics	Clears and resets the IS-IS statistics information.

MIB Objects

vRtrIsisStatsTable
- vRtrIsisSpfRuns
- vRtrIsisLSPRegenerations
- vRtrIsisInitiatedPurges
- vRtrIsisLSPRecd
- vRtrIsisLSPDrop
- vRtrIsisLSPSent
- vRtrIsisLSPRetrans
- vRtrIsisIIHRecd
- vRtrIsisIIHDrop
- vRtrIsisIIHSent
- vRtrIsisIIHRetrans
- vRtrIsisCSNPRecd
- vRtrIsisCSNPDrop
- vRtrIsisCSNPSent
- vRtrIsisCSNPRetrans
- vRtrIsisPSNPRecd
- vRtrIsisPSNPDrop
- vRtrIsisPSNPSent
- vRtrIsisPSNPRetrans
- vRtrIsisUnknownRecd
- vRtrIsisUnknownDrop
- vRtrIsisUnknownSent
- vRtrIsisUnknownRetrans
- vRtrIsisCSPFRequests
- vRtrIsisCSPFDroppedRequests
- vRtrIsisCSPFPathsFound
- vRtrIsisCSPFPathsNotFound

show ip isis status

Displays the IS-IS status.

show ip isis status

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show isis status
============================================================
ISIS Status
============================================================
System Id : 0050.0500.5001
Admin State              : UP
Last Enabled : WED OCT 24 10:05:55 2007
Level Capability         : L1L2
Authentication Check     : True
Authentication Type      : None
Graceful Restart         : Disabled
GR helper-mode           : Disabled
LSP Lifetime             : 1200
LSP Wait                 : Max :5 sec, Initial :0 sec, Second :1 sec
Adjacency Check          : Loose
L1 Auth Type             : None
L2 Auth Type             : None
L1 Wide Metrics-only     : Disabled
L2 Wide Metrics-only     : Disabled
L1 LSDB Overload         : Disabled
L2 LSDB Overload         : Disabled
L1 LSPs                  : 177
L2 LSPs                  : 177
Last SPF                 : FRI OCT 26 05:04:09 2007
SPF Wait                 : Max :10000 ms, Initial :1000 ms, Second :1000 ms
Hello-Auth Check         : Enabled
Csnp-Auth Check          : Enabled
Psnp-Auth Check          : Enabled
L1 Hello-Auth Check      : Enabled
L1 Csnp-Auth Check       : Enabled
L1 Psnp-Auth Check       : Enabled
```

```
L2 Hello-Auth Check      : Enabled
L2 Csnp-Auth Check       : Enabled
L2 Psnp-Auth Check       : Enabled
Area Address             : 49.0000
==========================================================
```

output definitions

System Id	The system ID of the router. The system ID is a fixed size, six octet field in the NSAP. In an IS-IS routing domain, each router is identified by a 6-octet hexadecimal system ID.
Admin State	The state of the router (**Up** or **Down**).
Last Enabled	The date and time when the router is enabled.
Level Capability	The level capability of the router **(L1, L2,** or **L1L2**).
Authentication Check	Indicates the status of the authentication (**true** or **false**).
Authentication Type	The type of authentication (**password** or **md5**).
Graceful Restart	Indicates if graceful restart is **Enabled** or **Disabled**.
GR helper-mode	Indicates if the helper mode of graceful restart is **Enabled** or **Disabled**.
LSP Lifetime	The Lifetime of the LSP (in seconds).
LSP Wait	The Wait time of the LSP (in seconds).
Adjacency Check	The adjacency check configuration on the router
L1 Auth Type	The authentication type (**password** or **md5**) for Level-1 adjacency.
L2 Auth Type	The authentication type (**password** or **md5**) for Level-2 adjacency.
L1 Wide Metrics-only	Indicates whether wide metrics is **Enabled** or **Disabled** for Level-1 adjacency.
L2 Wide Metrics-only	Indicates whether wide metrics is **Enabled** or **Disabled** for Level-2 adjacency.
L1 LSDB Overload	Indicates whether LSDB Overload is **Enabled** or **Disabled** for Level-1 adjacency.
L2 LSDB Overload	Indicates whether LSDB Overload is **Enabled** or **Disabled** for Level-2 adjacency.
L1 LSPs	The number of LSPs for Level-1 adjacency.
L2 LSPs	The number of LSPs for Level-2 adjacency.
Last SPF	The date and duration of the last SPF calculation.
SPF Wait	The Wait time for the SPF calculation.
Hello-Auth Check	Indicates the status of global Hello authentication check (**Enabled** or **Disabled**).
Csnp-Auth Check	Indicates the status of global CSNP authentication check (**Enabled** or **Disabled**).
Psnp-Auth Check	Indicates the status of global PSNP authentication check (**Enabled** or **Disabled**).
L1 Hello-Auth Check	Indicates the status of L1 Hello authentication check (**Enabled** or **Disabled**).
L1 Csnp-Auth Check	Indicates the status of L1 CSNP authentication check (**Enabled** or **Disabled**).

output definitions (continued)

L1 Psnp-Auth Check	Indicates the status of L1 PSNP authentication check (**Enabled** or **Disabled**).
L2 Hello-Auth Check	Indicates the status of L2 Hello authentication check (**Enabled** or **Disabled**).
L2 Csnp-Auth Check	Indicates the status of L2 CSNP authentication check (**Enabled** or **Disabled**).
L2 Psnp-Auth Check	Indicates the status of L2 PSNP authentication check (**Enabled** or **Disabled**).
Area Address	The area address of the router.

Release History

Release 6.2.1; command was introduced.
Release 6.3.1; Adjacency Check field was added.

Related Commands

ip isis status	Enables or disables the administration status of IS-IS on the router.
ip isis level-capability	Configures the router level of the IS-IS protocol globally.
ip isis auth-type	Configures authentication type of IS-IS protocol globally.
ip isis csnp-auth	Enables or disables the authentication of CSNPs.
ip isis hello-auth	Enables or disables the authentication of Hello PDUs globally.
ip isis psnp-auth	Enables or disables the authentication of PSNPs.
ip isis graceful-restart	Configures graceful restart on the router.
ip isis overload	Sets the IS-IS router to operate in the overload state for a specified time period.
ip isis overload-on-boot	Configures the IS-IS router to be in the overload state after bootup for a specified time period.
ip isis lsp-wait	Configures the time interval between successively generated LSPs.
ip isis spf-wait	Configures the time interval between successive Shortest Path First (SPF) calculations.
ip isis level auth-type	Enables the authentication and configures the authentication types for specific IS-IS levels.
ip isis level hello-auth	Enables or disables the authentication of Hello PDUs for specific IS-IS levels.
ip isis level csnp-auth	Enables or disables the authentication of CSNPs for specific IS-IS levels.
ip isis level psnp-auth	Enables or disables the authentication of PSNP PDUs for specific IS-IS levels.
ip isis level wide-metrics-only	Configures wide metrics in LSPs for specific IS-IS levels.
ip isis area-id	Configures the area ID for the switch.
ip isis auth-check	Enables or disables authentication check for IS-IS PDUs.

ip isis graceful-restart helper	Administratively enables and disables the IS-IS router to operate in the helper mode in response to a router performing a graceful restart.
ip isis lsp-lifetime	Configures the time interval for which Link State PDUs generated by a router are considered valid by other routers in the same domain.
ip isis strict-adjacency-check	Enables or disables the adjacency check configuration on the router.

MIB Objects

```
isisSysTable
   isisSysType
   isisSysID
   isisSysSetOverload
   isisSysAdminState
vRtrIsisTable
   vRtrIsisLastEnabledTime
   vRtrIsisAuthKey
   vRtrIsisAuthType
   vRtrIsisLspLifetime
   vRtrIsisOverloadTimeout
   vRtrIsisLastSpfRun
   vRtrIsisGracefulRestart
   vRtrIsisOverloadOnBootv
   vRtrIsisOverloadOnBootimeout
   vRtrIsisSpfWait
   vRtrIsisSpfInitialWait
   vRtrIsisSpfSecondWait
   vRtrIsisLspMaxWait
   vRtrIsisLspInitialWait
   vRtrIsisLspSecondWait
   vRtrIsisCsnpAuthentication
   vRtrIsisHelloAuthentication
   vRtrIsisPsnpAuthentication
   vRtrIsisGRHelperMode
   vRtrIsisSpfWait
vRtrIsisLevelTable
   vRtrIsisLevelAuthKey
   vRtrIsisLevelAuthType
   vRtrIsisLevelExtPreference
   vRtrIsisLevelPreference
   vRtrIsisLevelWideMetricsOnly
   vRtrIsisLevelCsnpAuthentication
   vRtrIsisLevelPsnpAuthentication
   vRtrIsisLevelHelloAuthentication
   vRtrIsisLevelWideMertic
   vRtrIsisLevelNumLSPs
```

show ip isis summary-address

Displays the IS-IS summary address database.

show ip isis summary-address [*ip-addr* **[***/mask***]]**

Syntax Definitions

ip-addr	The 32-bit IP address.
/mask	The netmask value. The valid range is 1–32.

Defaults

By default summary address information for all the IP addresses is displayed.

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

Use the *ip-addr* parameter with this command to view the summary address information for a specific IP address.

Examples

```
-> show ip isis summary-address
================================================================================
ISIS Summary Address
=====================================================
Address                     Level
--------------------------------------------------------------------------------
1.0.0.0/8                   L1
2.1.0.0/24                  L1L2
3.1.2.3/32                  L2
--------------------------------------------------------------------------------

Summary Address : 3
```

output definitions

Address	The summary address for a range of IPv4 addresses.
Level	The capability level of the router.
Summary Address	The number of summarized addresses.

Release History

Release 6.2.1; command was introduced.

Related Commands

ip isis summary-address	Adds or deletes the summary address.

MIB Objects

```
vRtrIsissummaryTable
   vRtrIsisSummPefix
   vRtrIsisSummMask
   vRtrIsisSummLevel
```

ip isis interface

Creates an IS-IS interface.

ip isis interface *interface_name*

no ip isis interface *interface_name*

Syntax Definitions

interface_name	The name of the IS-IS interface.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to remove the IS-IS interface.
- The interface name cannot contain spaces.

Examples

```
-> ip isis interface vlan-101
-> no ip isis interface vlan-101
```

Release History

Release 6.2.1; command was introduced.

Related Commands

show ip isis interface	Displays the IS-IS interface information.

MIB Objects

```
vRtrIsisIfTable
   vRtrIsisIfRowStatus
```

ip isis interface status

Enables or disables IS-IS on an interface.

ip isis interface *interface_name* **status {enable | disable}**

Syntax Definitions

interface_name	Name of the interface.
enable	Administratively enables IS-IS on the interface.
disable	Administratively disables IS-IS on the interface.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

When the status is manually disabled, the configuration settings and related statistics of the protocol remain unaffected.

Examples

```
-> ip isis interface vlan-101 status enable
-> ip isis interface vlan-101 status disable
```

Release History

Release 6.2.1; command was introduced.

Related Commands

show ip isis interface	Displays the IS-IS interface information.

MIB Objects

```
isisCircTable
   isisCircAdminState
```

ip isis interface interface-type

Configures the IS-IS interface as broadcast or point-to-point.

ip isis interface *interface_name* **interface-type {broadcast | point-to-point}**

Syntax Definitions

interface_name	The name of the interface.
broadcast	Sets the interface as a broadcast IS-IS interface.
point-to-point	Sets the interface as a point-to-point IS-IS interface.

Defaults

parameter	default
broadcast | point-to-point	**broadcast**

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

N/A.

Examples

```
-> ip isis interface vlan-101 interface-type broadcast
-> ip isis interface vlan-101 interface-type point-to-point
```

Release History

Release 6.2.1; command was introduced.

Related Commands

ip isis interface default-type	Sets the interface type to default
show ip isis interface	Displays the IS-IS interface information.

MIB Objects

```
isisCircTable
   isisCircType
```

ip isis interface csnp-interval

Configures the time interval to send CSNPs from the specified interface.

ip isis interface *interface_name* **csnp-interval** *seconds*

no ip isis interface *interface_name* **csnp-interval**

Syntax Definitions

interface_name	The name of the interface.
seconds	The time interval (1–65535) in seconds between successive CSNP PDUs sent on this interface.

Defaults

parameter	default
seconds (broadcast)	10
seconds (point-to-point)	5

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

Use the **no** form of this command to restore the settings to the default value.

Examples

```
-> ip isis interface vlan-101 csnp-interval 50
-> no ip isis interface vlan-101 csnp-interval
```

Release History

Release 6.2.1; command was introduced.

Related Commands

show ip isis interface	Displays the IS-IS interface information.

MIB Objects

```
vRtrisisIftable
   vRtrIsisIfCsnpInterval
```

ip isis interface hello-auth-type

Configures the authentication of Hello PDUs on a specific interface.

ip isis interface *interface_name* **hello-auth-type {simple {key** *key* **| encrypt-key** *encrypt-key***} | md5 {key** *key* **| encrypt-key** *encrypt-key***} | none}**

Syntax Definitions

interface_name	The name of the interface.
simple	Simple authentication will be used.
md5	Specifies that MD5 authentication algorithm will be used. Hash-key will be used in MD5 authentication.
key	Key will be plain text ASCII up to 118 characters. Use quotes around string if the key contains multiple words with spaces between them.
encrypt-key	The key in hexadecimal format to provide security consideration on the authentication key. Configuration snapshot always displays authentication key in the encrypted form.
none	No authentication will be used.

Defaults

parameter	default
simple | **md5** | **none**	**none**

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

- Simple authentication uses only a text string as the password in the packet. This helps to protect the routers from a configuration mishap. MD5 authentication is used to protect the system from malicious actions.
- MD5 authentication is used to encrypt the information that is sent over the network. MD5 authentication uses shared secret key. The Key is used to sign the packets with an MD5 checksum to sign the packet, so that the packets cannot be tampered. As the key is not included in the packet, snooping the key is not possible.
- Use the Key parameter to configure the password for Simple or MD5 authentication. Alternatively, use the *encrypt-key* parameter to configure the password by supplying the encrypted form of the password as the encrypt-key. The Configuration snapshot always displays the password in the encrypted form. You should use only this *key* parameter during the CLI configuration.
- If the *encrypt-key* parameter is used to configure the password through the CLI, then its value should be the same as the one that appears in the configuration snapshot. Only valid system generated values are accepted as encrypt-key.

- By default, the authentication is disabled and no authentication type is configured.

Examples

```
-> ip isis interface vlan-101 hello-auth-type md5 encrypt-key 7a1e441a014b4030
-> ip isis interface vlan-101 hello-auth-type none
```

Release History

Release 6.2.1; command was introduced.
Release 6.3.1; **key** and **encrypt-key** parameters were added.

Related Commands

ip isis interface level hello-auth-type	Configures the authentication of Hello PDUs for the specified IS-IS level of an interface.
show ip isis interface	Displays the IS-IS interface information.

MIB Objects

```
vRtrIsisIfTable
   vRtrIsisIfHelloAuthType
   vRtrIsisIfHelloAuthKey
```

ip isis interface level-capability

Configures the IS-IS level on the specified interface.

ip isis interface *interface_name* **level-capability [level-1 | level-2 | level-1/2]**

Syntax Definitions

interface_name	The name of the interface.
level-1	Specifies that the interface can operate at Level-1 only.
level-2	Specifies that the interface can operate at Level-2 only.
level-1/2	Specifies that the interface can operate at both Level-1 and Level-2.

Defaults

parameter	default
level-1 | **level-2** | **level-1/2**	**level-1/2**

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

- Changing the level capability restarts the IS-IS protocol on the interface.
- If the level capability is configured globally and on a specific interface, the combination of the two settings will decide the potential adjacency.

Examples

```
-> ip isis interface vlan-101 level-capability level-1
```

Release History

Release 6.2.1; command was introduced.

Related Commands

ip isis level-capability	Configures the router level of the IS-IS protocol globally.
show ip isis interface	Displays the IS-IS interface information.

MIB Objects

```
isisCircTable
   isisCircLevel
```

ip isis interface lsp-pacing-interval

Configures the time interval between IS-IS LSP PDUs sent from the specified interface.

ip isis interface *interface_name* **lsp-pacing-interval** *milliseconds*

no ip isis interface *interface_name* **lsp-pacing-interval**

Syntax Definitions

interface_name	The name of the interface.
milliseconds	The time interval in milliseconds (from 0 to 65535) between IS-IS LSPs.

Defaults

parameter	default
milliseconds	*100*

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to restore the default settings.
- No LSPs are sent from the specified interface if the time interval is set to 0.

Examples

```
-> ip isis interface vlan-101 lsp-pacing-interval 120
-> no ip isis interface vlan-101 lsp-pacing-interval
```

Release History

Release 6.2.1; command was introduced.

Related Commands

ip isis lsp-lifetime	Configures the time interval for which LSPs generated by a router is considered valid by other routers in the same domain.
ip isis lsp-wait	Configures the time interval between successively generated LSPs.
show ip isis interface	Displays the IS-IS interface information.

MIB Objects

```
vRtrIsisIfTable
   vRtrIsisIfLspPacingInterval
```

ip isis interface passive

Configures the interface as passive.

ip isis interface *interface_name* **passive**

no ip isis interface *interface_name* **passive**

Syntax Definitions

interface_name	The name of the interface.

Defaults

By default, the interface passive configuration is disabled.

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to remove the passive attribute.
- The passive interface will not permit ingressing and egressing IS-IS PDUs.

Examples

```
-> ip isis interface lan-1 passive
-> no ip isis interface lan-1 passive
```

Release History

Release 6.2.1; command was introduced.

Related Commands

ip isis interface level passive	Configures the interface as passive at the specified IS-IS level.
show ip isis interface	Displays the IS-IS interface information.

MIB Objects

```
isisCircTable
   isisCircPassiveCircuit
```

ip isis interface retransmit-interval

Configures the minimum time interval between LSP retransmissions on a point-to-point interface.

ip isis interface *interface_name* **retransmit-interval** *seconds*

no ip isis interface *interface_name* **retransmit-interval**

Syntax Definitions

interface_name	The name of the interface.
seconds	The minimum time interval (1–65535) in seconds between LSP transmissions on a point-to-point interface.

Defaults

parameter	default
seconds	5

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

Use the **no** form of this command to restore the default settings.

Examples

```
-> ip isis interface lan-3 retransmit-interval 130
-> no ip isis interface lan-4 retransmit-interval
```

Release History

Release 6.2.1; command was introduced.

Related Commands

show ip isis interface	Displays the IS-IS interface information.

MIB Objects

```
vRtrIsisIfTbale
   vRtrIsisIfRetransmitInterval
```

ip isis interface default-type

Sets the interface type to default.

ip isis interface *interface_name* **default-type**

Syntax Definitions

interface_name	The IP interface name.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

This command is used to indicate whether the circuit type is default or has been modified.

Examples

```
-> ip isis interface lan-3 default-type
```

Release History

Release 6.2.1; command was introduced.

Related Commands

ip isis interface interface-type	Configures the IS-IS interface as broadcast or point-to-point.

MIB Objects

```
vRtrIsisIfTable
   vRtrIsisIfTypeDefault
```

ip isis interface level hello-auth-type

Configures the authentication of Hello PDUs for the specified IS-IS level of an interface.

ip isis interface *interface_name* **level [1 | 2] hello-auth-type {simple {key** *key* | **encrypt-key** *encrypt-key***} | md5 {key** *key* **| encrypt-key** *encrypt-key***} | none}**

Syntax Definitions

interface_name	The name of the interface.
1	Specifies the IS-IS level as Level-1.
2	Specifies the IS-IS level as Level-2.
simple	Simple authentication will be used.
md5	Specifies that MD5 authentication algorithm will be used. Hash-key will be used in MD5 authentication.
key	Key will be plain text ASCII up to 118 characters. Use quotes around string if the key contains multiple words with spaces between them.
encrypt-key	The key in hexadecimal format to provide security consideration on the authentication key. Configuration snapshot always displays authentication key in the encrypted form.
none	No authentication will be used.

Defaults

parameter	default
simple | **md5** | **none**	**none**

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

- Simple authentication uses only a text string as the password in the packet. This helps to protect the routers from a configuration mishap. MD5 authentication is used to protect the system from malicious actions.
- MD5 authentication is used to encrypt the information that is sent over the network. MD5 authentication uses shared secret key. The Key is used to sign the packets with an MD5 checksum to sign the packet, so that the packets cannot be tampered. As the key is not included in the packet, snooping the key is not possible.
- Use the Key parameter to configure the password for Simple or MD5 authentication. Alternatively, use the *encrypt-key* parameter to configure the password by supplying the encrypted form of the password as the encrypt-key. The Configuration snapshot always displays the password in the encrypted form. You should use only this *key* parameter during the CLI configuration.

- If the *encrypt-key* parameter is used to configure the password through the CLI, then its value should be the same as the one that appears in the configuration snapshot. Only valid system generated values are accepted as encrypt-key.
- This command also configures the authentication type and the corresponding key. These settings override the configuration done on the specific interface.
- By default, the authentication is disabled and no authentication type is configured.

Examples

```
-> ip isis interface wan-50 level 1 hello-auth-type md5 key xyz123
-> ip isis interface man-80 level 2 hello-auth-type none
```

Release History

Release 6.2.1; command was introduced.

Related Commands

ip isis interface hello-auth-type	Configures the authentication of Hello PDUs on a specific interface.
show ip isis interface	Displays the IS-IS interface information.

MIB Objects

```
vRtrIsisIfLevelTable
   vRtrIsisIfLevelHelloAuthType
   vRtrIsisIfLevelHelloAuthKey
```

ip isis interface level hello-interval

Configures the time interval between the successive Hello PDUs for the specified IS-IS level of an interface.

ip isis interface *interface_name* **level [1 | 2] hello-interval** *seconds*

no ip isis interface *interface_name* **level [1 | 2] hello-interval**

Syntax Definitions

interface_name	The name of the interface.
seconds	The Hello interval, in seconds. The valid range is 1–20000.

Defaults

parameter	default
seconds (designated routers)	3
seconds (non-designated routers)	9

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

Use the **no** form of this command to restore the default settings.

Examples

```
-> ip isis interface man-1 level 1 hello-interval 50
-> no isis interface wan-876 level 2 hello-interval
```

Release History

Release 6.2.1; command was introduced.

Related Commands

show ip isis interface	Displays the IS-IS interface information.

MIB Objects

```
vRtrIsisIfLevelTable
   vRtrIsisIfLevelHelloTimer
```

ip isis interface level hello-multiplier

Configures the number of missing Hello PDUs from a neighbor, after which the adjacency is declared as down.

ip isis interface *interface_name* **level [1 | 2] hello-multiplier** *number*

no ip isis interface *interface_name* **level [1 | 2] hello-multiplier**

Syntax Definitions

interface_name	The name of the interface.
number	The multiplier (2–100) of the Hello interval.

Defaults

parameter	default
number	3

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

Use the **no** form of this command to restore the default settings.

Examples

```
-> ip isis interface lan-1 level 1 hello-multiplier 10
-> no ip isis interface lan-1 level 2 hello-multiplier
```

Release History

Release 6.2.1; command was introduced.

Related Commands

show ip isis interface	Displays the IS-IS interface information.

MIB Objects

```
isisCircLevelTable
   isisCircLevelHelloMultiplier
```

ip isis interface level metric

Configures the metric value of the specified IS-IS level of the interface.

ip isis interface *interface_name* **level [1 | 2] metric** *number*

no ip isis interface *interface_name* **level [1 | 2] metric**

Syntax Definitions

interface_name	The name of the interface.
1	Specifies the IS-IS level as Level-1.
2	Specifies the IS-IS level as Level-2.
number	The metric value (1–16777215) assigned for the specified level of the interface.

Defaults

parameter	default
number	10

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to restore the default value.
- To calculate the lowest cost to reach a destination, each configured level on each interface must have a cost.

Examples

```
-> ip isis interface interface-1 level 1 metric 25
-> no ip isis interface interface-2 level 2 metric
```

Release History

Release 6.2.1; command was introduced.

Related Commands

show ip isis interface	Displays the IS-IS interface information.

MIB Objects

```
vRtrIsisIfLevelTable
   vRtrisisIfLevelAdminMetric
```

ip isis interface level passive

Configures the interface as passive at the specified IS-IS level.

ip isis interface *interface_name* **level [1 | 2] passive**

no ip isis interface *interface_name* **level [1 | 2] passive**

Syntax Definitions

interface_name	The name of the interface.
1	Specifies the IS-IS level as Level-1.
2	Specifies the IS-IS level as Level-2.

Defaults

By default, the interface level passive configuration is disabled.

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to remove the passive attribute.
- The passive interface will not permit ingressing and egressing IS-IS PDUs.

Examples

```
-> ip isis interface lan-5 level 1 passive
-> no ip isis interface wan-10 level 1 passive
```

Release History

Release 6.2.1; command was introduced.

Related Commands

ip isis interface passive	Configures the interface as passive.
show ip isis interface	Displays the IS-IS interface information.

MIB Objects

```
vRtrIsisIfLevelTable
   vRtrIsisIfLevelPassive
```

ip isis interface level priority

Configures the IS-IS router interface priority for the designated router election on a multi-access network.

ip isis interface *interface_name* **level [1 | 2] priority** *number*

no ip isis interface *interface_name* **level [1 | 2] priority**

Syntax Definitions

interface_name	The name of the given IP interface.
1	Specifies the IS-IS level as Level-1.
2	Specifies the IS-IS level as Level-2.
number	The priority value of this interface at this level. The valid range is 0–127.

Defaults

parameter	default
number	64

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to restore the default value.
- The router with the highest priority is the preferred designated router.
- The designated router sends LSPs to this network and also to the routers that are attached to it.

Examples

```
-> ip isis interface vlan-isis level 1 priority 4
-> ip isis interface vlan-isis level 2 priority 4
-> no ip isis interface vlan-isis level 1 priority
```

Release History

Release 6.2.1; command was introduced.

Related Commands

show ip isis interface	Displays the IS-IS interface information.

MIB Objects

```
vRtrIsisIfLevelTable
   vRtrIsisIfLevelISPriority
```

show ip isis interface

Displays the IS-IS interface information.

show ip isis interface [*interface_name***] [detail]**

Syntax Definitions

interface_name	The name of the interface.
detail	Indicates that the output is displayed in a detailed manner.

Defaults

By default the interface information for all the interfaces is displayed.

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

Use the *interface_name* parameter with this command to view information for a specific interface.

Examples

```
-> show ip isis interface
=============================================================================
ISIS Interfaces
=============================================================================
Interface    Level      CircID   Oper-state   Admin-state  L1/L2-Metric
-----------------------------------------------------------------------------
system         L1L2      1          Up         Up           10/10
if2/1          L2        8          Up         Up           - /10
if2/2          L1        5          Up         Up           10/-
if2/3          L1        6          Up         Up           10/-
if2/4          L1        7          Up         Up           10/-
if2/5          L2        2          Up         Up           -/10
lag-1          L2        3          Up         Up           -/10
if2/8          L2        4          Up         Up           -/10
-----------------------------------------------------------------------------
Interfaces : 8
```

output definitions

Interface	The name of the IS-IS interface.
Level	The level capability of the interface.
CircID	The circuit ID of the interface.
Oper-state	The operational state of the interface (**up** or **down**).
Admin-state	The administrative state of the interface (**up** or **down**).
L1/L2 -Metric	The metric value of the router for the corresponding capability level.
Interfaces	The total number of interfaces.

```
-> show ip isis interface detail
================================================================================
ISIS Interface
================================================================================
--------------------------------------------------------------------------------
Interface          : system         Level Capability  : L1L2
Oper State         : Up             Admin State       : Up
Auth Type          : None
Circuit Id         : 1              RetransmitInt     : 5
Type               : Broadcast      LSP Pacing Int    : 100
Mesh Group         : Inactive       CSNP Int          : 10
Level              : 1              Adjacencies       : 0
Desg IS            : abr_nyc
Auth Type          : None           Metric            : 10
Hello Timer        : 9              Hello Mult        : 3
Priority           : 64             Passive           : No
Level              : 2              Adjacencies      : 0
Desg IS            : abr_nyc
Auth Type          : None            Metric           : 10
Hello Timer        : 9               Hello Mult       : 3
Priority           : 64              Passive          : No
--------------------------------------------------------------------------------
Interface          :  if2/1          Level Capability : L2
Oper State         : Up              Admin State : Up
Auth Type          : None
Circuit Id         : 8               RetransmitInt    : 5
Type               : Pt-to-Pt        LSP Pacing Int   : 100
Mesh Group         : Inactive        CSNP Int         : 10
Level              : Pt-to-Pt
Desg  IS           : abr_nyc
Auth Type          : None            Metric           : 10
Hello Timer        : 9               Hello Mult       : 3
Priority           : 64              Passive          : No
```

output definitions

Interface	The name of the IS-IS interface.
Level Capability	The level capability of the interface.
Oper State	The operational state of the interface (**up** or **down**).
Admin State	The administrative state of the interface (**up** or **down**).
Auth Type	Indicates the authentication type (**simple**, **MD5**, or **none**) of the interface.
Circuit Id	The circuit ID of the interface.
RetransmitInt	Specifies the minimal interval of time, in seconds between retransmission of an LSP on the point-to-point interface.
Type	The type of interface: **Broadcast** or **Pt-to-Pt** (point to point).
LSP Pacing Int	The LSP Pacing interval.
Mesh Group	The status of the mesh group (**Active** or **Inactive**).
CSNP Int	The CSNP interval.
Level	Indicates the IS-IS level of the neighbor (**L1,L2**, or **L1L2**).
Adjacencies	The number of adjacencies formed.

output definitions (continued)

Desg IS	The ID of the LAN Designated Intermediate System on this circuit at this level.
Auth Type	Indicates the authentication type (**simple**, **MD5**, or **none**) for the specified level.
Metric	The metric value of this circuit for a specific level.
Hello Timer	Indicates the Hello timer value.
Hello Mult	Indicates the Hello multiplier value.
Priority	The priority value of the interface.
Passive	Indicates whether the interface is configured as a passive interface (**Yes** or **No**).

Release History

Release 6.2.1; command was introduced.

Related Commands

ip isis interface	Creates an IS-IS interface.

MIB Objects

```
 isisCircTable
   isisCircLocalID
   isisCircAdminState
   isisCircType
   isisCircLevel
   isisCircPassiveCircui
   isisCircMeshGroup
isisCircLevelTable
   isisCircLevelISPriority
   isisCircLevelCircID
   isisCircLevelDesIS
   isisCircLevelHelloMultiplier
   isisCircLevelHelloTimer
   isisCircLevelCSNPInterval
vRtrIsisIfTable
   vRtrIsisIfAdminState
   vRtrIsisIfOperState
   vRtrIsisIfCsnpInterval
   vRtrIsisIfHelloAuthKey
   vRtrIsisIfHelloAuthType
   vRtrIsisIfLspPacingInterval
   vRtrIsisIfRetransmitInterval
vRtrIsisIfLevelTable
   vRtrIsisIfLevelHelloAuthKey
   vRtrIsisIfLevelHelloAuthType
   vRtrIsisIfLevelPassive
   vRtrIsisIfLevelNumAdjacencies
   vRtrIsisIfLevelISPriority
   vRtrIsisIfLevelHelloTimer
```

```
vRtrIsisLevelOperMetric
vRtrIsisIfLevelAdminMetric
```

clear ip isis adjacency

Clears and resets the IS-IS adjacency database information.

clear ip isis adjacency [system-id *nbr-sys-id***]**

Syntax Definitions

nbr-sys-id	The system ID of the neighbor router.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

If the *nbr-sys-id* parameter is specified, only the entries specific to that system ID are removed from the database.

Examples

```
-> clear ip isis adjacency system-id 1122.3344.5566
```

Release History

Release 6.2.1; command was introduced.

Related Commands

show ip isis adjacency	Displays information about IS-IS adjacent routers.

MIB Objects

```
isisISAdjTable
   isisISAdjIndex
   isisISAdjState
   isisISAdjNeighSNPAAddress
   isisISAdjNeighSysType
   isisISAdjNeighSysID
   isisISAdjUsage
   isisISAdjHoldTimer
   isisISAdjNeighPriority
   isisISAdjUpTime
vRtrIsisISAdjTable
   vRtrIsisISAdjExpiresIn
   vRtrIsisISAdjCircLevel
   vRtrIsisISAdjRestartSupport
   vRtrIsisISAdjRestartStatus
```

```
vRtrIsisISAdjRestartSupressed
```

clear ip isis lsp-database

Clears and resets the IS-IS LSP database information.

clear ip isis lsp-database [system-id *sys-id***]**

Syntax Definitions

sys-id	The system ID of the router.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

If the *sys-id* parameter is specified, only the entries specific to that system ID are removed from the database.

Examples

```
-> clear ip isis lsp-database system-id 000a.1234.2345
```

Release History

Release 6.2.1; command was introduced..

Related Commands

show ip isis database	Displays IS-IS LSP database information of the adjacent routers.

MIB Objects

```
vRtrIsisLSPTable
   vRtrIsisLSPId
   vRtrIsisLSPSeq
   vRtrIsisLSPChecksum
   vRtrIsisLSPLifetimeRemain
   vRtrIsisLSPVersion
   vRtrIsisLSPPktType
   vRtrIsisLSPPktVersion
   vRtrIsisLSPMaxArea
   vRtrIsisLSPSysIdLen
   vRtrIsisLSPAttributes
   vRtrIsisLSPUsedLen
   vRtrIsisLSPAllocLen
   vRtrIsisLSPBuff
   vRtrIsisLSPZeroRLT
```

clear ip isis spf-log

Clears and resets the IS-IS SPF log information.

clear ip isis spf-log

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> clear ip isis spf-log
```

Release History

Release 6.2.1; command was introduced.

Related Commands

show ip isis spf-log	Displays the IS-IS SPF log.

MIB Objects

```
vRtrIsisSpfLogTable
   vRtrIsisSpfRunTime
   vRtrIsisSpfL1Nodes
   VRtrIsisSpfL2Nodes
   vRtrIsisSpfEventCount
   vRtrIsisSpfLastTriggerLSPId
   vRtrIsisSpfTriggerReason
```

clear ip isis statistics

Clears and resets the IS-IS statistics information.

clear ip isis statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> clear ip isis statistics
```

Release History

Release 6.2.1; command was introduced.

Related Commands

show ip isis statistics	Displays the IS-IS statistics information.

MIB Objects

vRtrIsisStatsTable
- vRtrIsisSpfRuns
- vRtrIsisLSPRegenerations
- vRtrIsisInitiatedPurges
- vRtrIsisLSPRecd
- vRtrIsisLSPDrop
- vRtrIsisLSPSent
- vRtrIsisLSPRetrans
- vRtrIsisIIHRecd
- vRtrIsisIIHDrop
- vRtrIsisIIHSent
- vRtrIsisIIHRetrans
- vRtrIsisCSNPRecd
- vRtrIsisCSNPDrop
- vRtrIsisCSNPSent
- vRtrIsisCSNPRetrans
- vRtrIsisPSNPRecd
- vRtrIsisPSNPDrop
- vRtrIsisPSNPSent
- vRtrIsisPSNPRetrans
- vRtrIsisUnknownRecd
- vRtrIsisUnknownDrop
- vRtrIsisUnknownSent
- vRtrIsisUnknownRetrans
- vRtrIsisCSPFRequests
- vRtrIsisCSPFDroppedRequests
- vRtrIsisCSPFPathsFound
- vRtrIsisCSPFPathsNotFound

30 BGP Commands

This chapter describes the CLI commands used to configure the BGP (Border Gateway Protocol) and Multiprotocol extensions to BGP. 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.

Multiprotocol Extensions to BGP-4 supports the exchange of IPv6 unicast prefixes, as well as the establishment of BGP peering sessions with BGP speakers identified by their IPv6 addresses.

The Alcatel-Lucent implementation of BGP-4 and Multiprotocol Extensions to BGP-4 complies with the following RFCs: 4271, 2439, 3392, 2385, 1997, 4456, 3065, 4273, 4760, 2545

Note. In the following document, the BGP terms “peer” and “neighbor” are used interchangeably to mean any BGP speaker 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

The following table summarizes the available commands:

Global BGP Commands	**ip load bgp** **ip bgp status** **ip bgp unicast** **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** **show ip bgp** **show ip bgp statistics** **show ip bgp dampening** **show ip bgp dampening-stats** **show ip bgp path** **show ip bgp routes**
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 in-prefix6list** **ip bgp neighbor out-prefix6list** **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 prefix6-list** **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 prefix6-list** **show ip bgp policy route-map**
BGP Graceful Restart Commands	**ip bgp graceful-restart** **ip bgp graceful-restart restart-interval**
IPv6 Global BGP Commands	**ipv6 bgp unicast** **ip bgp neighbor activate-ipv6** **ip bgp neighbor ipv6-nexthop** **show ipv6 bgp path** **show ipv6 bgp routes**
IPv6 BGP Network Configuration Commands	**ipv6 bgp network** **ipv6 bgp network community** **ipv6 bgp network local-preference** **ipv6 bgp network metric** **ipv6 bgp network status** **show ipv6 bgp network**

IPv6 BGP Neighbor (Peer) Configuration Commands	**ipv6 bgp neighbor** **ipv6 bgp neighbor clear soft** **ipv6 bgp neighbor soft-reconfiguration** **ipv6 bgp neighbor in-prefix6list** **ipv6 bgp neighbor out-prefix6list** **ipv6 bgp neighbor activate-ipv6** **ipv6 bgp neighbor ipv6-nexthop** **ipv6 bgp neighbor status** **ipv6 bgp neighbor remote-as** **ipv6 bgp neighbor timers** **ipv6 bgp neighbor maximum-prefix** **ipv6 bgp neighbor next-hop-self** **ipv6 bgp neighbor conn-retry-interval** **ipv6 bgp neighbor default-originate** **ipv6 bgp neighbor update-source** **ipv6 bgp neighbor ipv4-nexthop** **show ipv6 bgp neighbors** **show ipv6 bgp neighbors statistics** **show ipv6 bgp neighbors timers** **show ipv6 bgp neighbors policy**

ip load bgp

Loads the BGP protocol software into running memory on the router. 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- This command requires that the BGP software be resident in flash memory in the active directory.
- Enter this command in the router's configuration file (boot.cfg) to ensure BGP software is running after a reboot.
- The command does not administratively enable BGP on the router; BGP will be disabled after issuing this command. You must issue the **ip bgp status** to start the BGP protocol.

Examples

```
-> ip load bgp
```

Release History

Release 6.1; command was introduced.

Related Commands

ip bgp autonomous-system	Configures the Autonomous system number for this BGP router.
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 6400, 6850E, 6855, 9000E

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.

Examples

```
-> ip bgp status enable
-> ip bgp status disable
```

Release History

Release 6.1; command was introduced.

Related Commands

ip load bgp	Loads the BGP software.

MIB Objects

```
alaBgpGlobal
   alaBgpProtoStatus
```

ip bgp unicast

Enables or disables unicast IPv4 advertisements for the BGP routing process.

ip bgp unicast

no ip bgp unicast

Syntax Definitions

N/A

Defaults

By default, BGP IPv4 advertisements are enabled.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to turn off IPv4 unicast advertisements.
- BGP should be disabled before enabling or disabling IPv4 unicast advertisements.
- IPv4 unicast advertisements may be turned off on homogenous IPv6 networks that are not aware of IPv4 routing. In such cases, the command, **ip router router-id**, must be used to explicitly configure the 32-bit unique router identifier.

Examples

```
-> ip bgp unicast
-> no ip bgp unicast
```

Release History

Release 6.1.5; command was introduced.

Related Commands

ipv6 bgp unicast	Enables or disables unicast IPv6 updates for the BGP routing process.
show ip bgp	Displays the current global settings for the local BGP speaker.
ip router router-id	Configures the router ID for the router.

MIB Objects

```
alaBgpGlobal
   alaBgpMultiProtocolIpv4
```

ip bgp autonomous-system

Configures the Autonomous System (AS) number for this router. This number identifies this BGP speaker (this router) 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- A router can belong to only one AS. Do not specify more than one AS value for each router.
- The BGP protocol must be disabled (using the **ip bgp status** command) before using this command.

Examples

```
-> ip bgp autonomous-system 64724
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to disable this feature after it has been enabled.
- 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.

Examples

```
-> ip bgp bestpath as-path ignore
-> no ip bgp bestpath as-path ignore
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

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.

Examples

```
-> ip bgp cluster-id 1.2.3.4
```

Release History

Release 6.1; 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 router. The valid range is 0–4294967295.

Defaults

parameter	default
value	100

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to restore the default value.
- 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 router so it can compare its own local preference to those received in advertised paths. If other routers 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.

Examples

```
-> ip bgp default local-preference 200
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to disable Fast External Failover.
- 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.

Examples

```
-> ip bgp fast-external-failover
-> no ip bgp fast-external-failover
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to disable MED comparison for external peers.
- 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.

Examples

```
-> ip bgp always-compare-med
-> no ip bgp always-compare-med
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to disable missing MEDs as worst.
- 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.
- The BGP protocol must be disabled (using the **ip bgp status** command) before using this command.

Examples

```
-> ip bgp bestpath med missing-as-worst
-> no ip bgp bestpath med missing-as-worst
```

Release History

Release 6.1; 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 (router) 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to disable the speaker as a route reflector.
- In addition to defining this router 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.

Examples

```
-> ip bgp client-to-client reflection
-> no ip bgp client-to-client reflection
```

Release History

Release 6.1; command was introduced.

Related Commands

ip bgp status	Administratively disables BGP in this router.
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

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to reset the feature to the default value.
- A lower value may increase the likelihood of route flapping as route status is updated more frequently.

Examples

```
-> ip bgp as-origin-interval 15
-> no ip bgp as-origin-interval
```

Release History

Release 6.1; 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 synchronization of BGP prefixes with AS-internal routing information. Enabling this command will force the BGP speaker to advertise prefixes only if the prefixes are reachable through AS-internal routing protocols (IGPs like RIP and OSPF).

ip bgp synchronization

no ip bgp synchronization

Syntax Definitions

N/A

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to disable IGP synchronization.
- 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.

Examples

```
-> ip bgp synchronization
-> no ip bgp synchronization
```

Release History

Release 6.1; 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 router). 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to restore the default value.
- 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.

Examples

```
-> ip bgp confederation identifier 3
```

Release History

Release 6.1; command was introduced.

Related Commands

ip bgp autonomous-system	Sets the AS number for this router.
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 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to disable support for multiple equal cost paths.
- The BGP protocol must be disabled (using the **ip bgp status** command) before using this command.

Examples

```
-> ip bgp maximum-paths
-> no ip bgp maximum-paths
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

The BGP protocol must be disabled (using the **ip bgp status** command) before using this command.

Examples

```
-> ip bgp log-neighbor-changes
-> no ip bgp log-neighbor-changes
```

Release History

Release 6.1; command was introduced.

Related Commands

ip bgp status	Disables BGP within the router.

MIB Objects

```
alaBgpGlobal
   alaBgpPeerChanges
```

ip bgp dampening

Enables or disables BGP route dampening or the suppression of unstable routes. Route dampening helps to 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to disable dampening.
- BGP dampening is disabled by default. When enabled, route dampening suppresses routes that are unstable, or “flapping,” and disrupting the network.
- BGP dampening of IPv6 route flaps is currently not supported.
- 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.

Examples

```
-> ip bgp dampening
-> ip bgp dampening half-life 20 reuse 800 suppress 60 max-suppress-time 40
-> no ip bgp dampening
```

Release History

Release 6.1; command was introduced.

Related Commands

ip bgp dampening clear	Clears the dampening history data for all routes on the router, 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 router, 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 6400, 6850E, 6855, 9000E

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.
- BGP dampening of IPv6 route flaps is currently not supported.

Examples

```
-> ip bgp dampening clear
```

Release History

Release 6.1; command was introduced.

Related Commands

ip bgp dampening	Enables or disables route dampening.

MIB Objects

```
alaBgpGlobal
   alaBgpDampeningClear
```

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.

Note that only one of the following optional keywords is specified with each use of the base command. Keywords are not combined together in a single command.

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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete an aggregate route.
- 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.

Examples

```
-> ip bgp aggregate-address 172.22.2.115 255.255.255.0
-> no ip bgp aggregate-address 172.22.2.115 255.255.255.0
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

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.

Examples

```
-> ip bgp aggregate-address 172.22.2.115 255.255.255.0 status enable
-> ip bgp aggregate-address 172.22.2.115 255.255.255.0 status disable
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to disable the **as-set** option.
- 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.

Examples

```
-> 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 6.1; 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, for example, 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 6400, 6850E, 6855, 9000E

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
```

Examples

```
-> 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 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to set the local preference back to the default value.
- 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).

Examples

```
-> 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 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to reset the aggregate metric back to its default value.
- 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.

Examples

```
-> 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 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to disable this feature.
- 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.

Examples

```
-> 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 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete a local network.
- 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.

Examples

```
-> 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 6.1; 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 6400, 6850E, 6855, 9000E

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.

Examples

```
-> ip bgp network 172.22.2.115 255.255.255.0 status enable
```

Release History

Release 6.1; 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, for example, 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 6400, 6850E, 6855, 9000E

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
```

Examples

```
-> ip bgp network 172.22.2.115 255.255.255.0 community export
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to return the local preference of the specified network to its default setting.
- 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).

Examples

```
-> ip bgp network 10.10.10.10 255.255.255.0 local-preference 600
-> no ip bgp network 10.10.10.10 255.255.255.0 local-preference 600
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to return the metric for this network to its default value.
- 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.

Examples

```
-> ip bgp network 10.10.10.10 255.255.255.0 metric 100
-> no ip bgp network 10.10.10.10 255.255.255.0 metric 100
```

Release History

Release 6.1; 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
   alaBgpNetworkMetric
```

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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete a BGP peer.
- 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.

Examples

```
-> ip bgp neighbor 10.10.10.10
-> no ip bgp neighbor 10.10.10.10
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

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.

Examples

```
-> ip bgp neighbor 10.10.10.10 status enable
-> ip bgp neighbor 10.10.10.10 status disable
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

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.

Examples

```
-> ip bgp neighbor 10.10.10.10 255.255.255.0 advertisement-interval 60
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

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.

Examples

```
-> ip bgp neighbor 10.10.10.10 clear
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove this peer as a client to the local route reflector.
- 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.

Examples

```
-> ip bgp neighbor 10.10.10.10 route-reflector-client
-> no ip bgp neighbor 10.10.10.10 route-reflector-client
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to disable this feature.
- 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.

Examples

```
-> ip bgp neighbor 10.10.10.10 default-originate
-> no ip bgp neighbor 10.10.10.10 default-originate
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

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.
- 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.

Examples

```
-> ip bgp neighbor 10.10.10.10 timers 80 240
-> ip bgp neighbor 10.10.10.10 timers
```

Release History

Release 6.1; 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

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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.

Examples

```
-> ip bgp neighbor 10.10.10.10 connect-interval 60
-> ip bgp neighbor 10.10.10.10 connect-interval
```

Release History

Release 6.1; 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.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to disable automatic peer restart.
- 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).
- 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.

Examples

```
-> ip bgp neighbor 10.10.10.10 auto-restart
-> no ip bgp neighbor 10.10.10.10 auto-restart
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

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.
- The BGP peer is restarted after issuing this command.

Examples

```
-> ip bgp neighbor 10.10.10.10 maximum-prefix 1000
-> ip bgp neighbor 10.10.10.10 maximum-prefix 1000 warning only
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Entering the keyword **none** in place of a key removes the password and disables authentication.
- 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.
- The BGP peer is restarted after issuing this command.

Examples

```
-> ip bgp neighbor 10.10.10.10 md5 key openpeer5
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to disable multi-hop connections.
- 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).
- The BGP peer is restarted after issuing this command.

Examples

```
-> ip bgp neighbor 10.10.10.10 ebgp-multihop 250
-> no ip bgp neighbor 10.10.10.10 ebgp-multihop 50
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

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.

Examples

```
-> ip bgp neighbor 10.10.10.10 description “peer for building 3”
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to disable next hop processing behavior.
- 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.
- The BGP peer is restarted after issuing this command.

Examples

```
-> ip bgp neighbor 10.10.10.10 next-hop-self
-> no ip bgp neighbor 10.10.10.10 next-hop-self
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to disable passive peer behavior.
- 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.
- The BGP peer is restarted after issuing this command.

Examples

```
-> ip bgp neighbor 10.10.10.10 passive
-> no ip bgp neighbor 10.10.10.10 passive
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

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 router and it may be in an external AS, but it must still be configured on this router before the local BGP speaker can establish a connection to the peer. The local BGP speaker does not auto-discover peers in other routers; it initially learns about peers through the peer commands.
- The BGP peer is restarted after issuing this command.

Examples

```
-> ip bgp neighbor 10.10.10.10 remote-as 100
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to disable stripping of private AS numbers.
- 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.
- The BGP peer is restarted after issuing this command.

Examples

```
-> ip bgp neighbor 10.10.10.10 remove-private-as
-> no ip bgp neighbor 10.10.10.10 remove-private-as
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to disable this feature.
- 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 in-prefix6list** command.
- The BGP peer is restarted after issuing this command.

Examples

```
-> ip bgp neighbor 10.10.10.10 soft-reconfiguration
-> no ip bgp neighbor 10.10.10.10 soft-reconfiguration
```

Release History

Release 6.1; command was introduced.

Related Commands

ip bgp neighbor clear	Restarts this BGP peer.
ip bgp neighbor in-prefix6list	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 6400, 6850E, 6855, 9000E

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**.

Examples

```
-> ip bgp neighbor 10.10.10.10 stats-clear
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to disable this feature.
- 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 BGP peer is restarted after issuing this command.

Examples

```
-> ip bgp confederation neighbor 10.10.10.10
-> no ip bgp confederation neighbor 10.10.10.10
```

Release History

Release 6.1; command was introduced.

Related Commands

ip bgp confederation identifier	Sets a confederation identification value for the local BGP speaker (this router).

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_name***]**

Syntax Definitions

ip_address	The 32-bit IP address for this peer.
interface_name	The name of the interface.

Defaults

parameter	default
interface_address	0.0.0.0

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 router. The router identification for a peer, especially an external peer, may not exist in the local router, but that distant peer can still be contacted via this router. 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.

Examples

```
-> ip bgp neighbor 10.10.10.10 update-source 172.22.2.117
-> ip bgp neighbor 10.10.10.10 update-source vlan-22
-> ip bgp neighbor 10.10.10.10 update-source
```

Release History

Release 6.1; command was introduced.

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 6400, 6850E, 6855, 9000E

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**.

Examples

```
-> ip bgp neighbor 10.10.10.10 in-aspathlist InboundASpath
-> ip bgp neighbor 10.10.10.10 in-aspathlist none
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

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**."

Examples

```
-> ip bgp neighbor 10.10.10.10 in-communitylist InboundCommlist
-> ip bgp neighbor 10.10.10.10 in-communitylist none
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

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.**"

Examples

```
-> ip bgp neighbor 10.10.10.10 in-prefixlist InboundPrefix
-> ip bgp neighbor 10.10.10.10 in-prefixlist none
```

Release History

Release 6.1; command was introduced.

Related Commands

ip bgp policy prefix-list	Creates or deletes a prefix match list.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerPrefixListIn
```

ip bgp neighbor in-prefix6list

Configures an inbound BGP prefix6-list policy for an IPv4 BGP peer.

ip bgp neighbor *peer_address* **in-prefix6list** *pfx_list_name*

Syntax Definitions

peer_address	The 32-bit IPv4 address of the BGP peer.
pfx_list_name	An output prefix list name (1 - 70 characters).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The prefix list name (**uniqLocal** in the example below) is created using the **ip bgp policy prefix6-list** command. Any outbound routes from the BGP peer must match this prefix filter before being advertised or passed to the outbound policy.
- BGP neighbor must be configured.

Examples

```
-> ip bgp neighbor 10.0.0.1 in-prefix6list uniqLocal
```

Release History

Release 6.3.4; command was introduced.

Related Commands

ip bgp policy prefix6-list	Creates or deletes a BGP prefix6-list policy for filtering IPv6 prefixes.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerPrefix6ListIn
```

ip bgp neighbor out-prefix6list

Configures an outgoing BGP prefix6-list policy for an IPv4 BGP peer.

ip bgp neighbor *peer_address* **out-prefix6list** *pfx_list_name*

Syntax Definitions

peer_address	The 32-bit IPv4 address of the BGP peer.
pfx_list_name	An Output prefix list name (1 - 70 characters).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The prefix list name (**uniqLocal** in the example below) is created using the **ip bgp policy prefix6-list** command. Any outbound routes from the BGP peer must match this prefix filter before being advertised or passed to outbound policy.
- BGP neighbor must be configured.

Examples

```
-> ip bgp neighbor 10.0.0.1 out-prefix6list uniqLocal
```

Release History

Release 6.3.4; command was introduced.

Related Commands

ip bgp policy prefix6-list	Creates or deletes a BGP prefix6-list policy for filtering IPv6 prefixes.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerPrefix6ListOut
```

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 6400, 6850E, 6855, 9000E

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**".

Examples

```
-> ip bgp neighbor 10.10.10.10 out-aspathlist OutboundASpath
-> ip bgp neighbor 10.10.10.10 out-aspathlist none
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

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**".

Examples

```
-> ip bgp neighbor 10.10.10.10 out-communitylist OutboundCommlist
-> ip bgp neighbor 10.10.10.10 out-communitylist none
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

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**".

Examples

```
-> ip bgp neighbor 10.10.10.10 out-prefixlist OutboundPrefix
-> ip bgp neighbor 10.10.10.10 out-prefixlist none
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no f**orm of this command to deassign an inbound map.
- The policy route map name (**peeringPointAMap** in the example below) is created using the **ip bgp policy prefix6-list** command. Any inbound routes from the BGP peer must match this route map filter before being accepted or passed to inbound policy.
- It is also possible to deassign a route map by entering **none** in place of a route map name.

Examples

```
-> ip bgp neighbor 10.10.10.10 route-map InboundRoute in
-> ip bgp neighbor 10.10.10.10 route-map OutboundRoute out
-> ip bgp neighbor 10.10.10.10 route-map none in
-> no ip bgp neighbor 10.10.10.10 route-map in
```

Release History

Release 6.1; command was introduced.

Related Commands

ip bgp policy prefix6-list	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 6400, 6850E, 6855, 9000E

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.

Examples

```
-> ip bgp neighbor 10.10.10.10 clear soft in
-> ip bgp neighbor 10.10.10.10 clear soft out
```

Release History

Release 6.1; 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, for example, InboundAspath, ranging from 0 to 70 characters, or a value of none. The AS path name is case sensitive.
regular_expression	Regular expression, for example, "^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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove an AS path list.
- To create an AS path list, use the **ip bgp policy aspath-list** command.
- A regular expression consists of a character string presented in the form of a pattern, for example, ^100 200$. Valid regular expression characters (metacharacters) are shown in the table below. See also "Configuring BGP" in your OmniSwitch AOS Release 6 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.
|	Separates AS numbers in an alternation sequence.

Symbol	Description
)	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 in-prefix6list** 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 (that is, 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 6.1; command was introduced.

Related Commands

ip bgp neighbor in-aspathlist	Assigns an inbound AS path list filter to a BGP peer.
ip bgp neighbor in-prefix6list	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, for example, InboundAspath, ranging from 0 to 70 characters, or a value of none. The AS path name is case sensitive.
regular_expression	Regular expression, for example, “^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 6400, 6850E, 6855, 9000E

Usage Guidelines

- A regular expression consists of a character string presented in the form of a pattern, for example, ^100 200$. Refer to **ip bgp policy aspath-list** on page 30-97 for a table of valid regular expression characters (metacharacters). See also “Configuring BGP” in your OmniSwitch AOS Release 6 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 in-prefix6list** 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 (that is, 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.

Examples

```
-> ip bgp policy aspath-list InboundAspath “^100 200$” action permit
-> ip bgp policy aspath-list OutboundAspath “^300 400$” action deny
```

Release History

Release 6.1; command was introduced.

Related Commands

ip bgp neighbor in-aspathlist	Assigns an inbound AS path list filter to a BGP peer.
ip bgp neighbor in-prefix6list	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, for example, InboundAspath, ranging from 0 to 70 characters, or a value of none. The AS path name is case sensitive.
regular_expression	A regular expression, for example, "^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, for example, 1, assigned to the policy action. Valid priority range is from 1 - 255.

Defaults

parameter	default
value	1

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- A regular expression consists of a character string presented in the form of a pattern, for example, ^100 200$. Refer to **ip bgp policy aspath-list** on page 30-97 for a table of valid regular expression characters (metacharacters). See also "Configuring BGP" in your OmniSwitch AOS Release 6 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 in-prefix6list** 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 (that is, 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.

Examples

```
-> ip bgp policy aspath-list InboundAspath "^100 200$" priority 1
```

```
-> ip bgp policy aspath-list OutboundAspath “^300 400$” priority 5
```

Release History

Release 6.1; command was introduced.

Related Commands

ip bgp neighbor in-aspathlist	Assigns an inbound AS path list filter to a BGP peer.
ip bgp neighbor in-prefix6list	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, for example, 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a community-list.
- 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.

Examples

```
-> 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 6.1; 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, for example, 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 6400, 6850E, 6855, 9000E

Usage Guidelines

By default, this command allows routes that match the criteria specified in the community list to pass.

Examples

```
-> ip bgp policy community-list commListAIn 600:1 action permit
-> ip bgp policy community-list commListAIn 600:1 action deny
```

Release History

Release 6.1; 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, for example, 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 6400, 6850E, 6855, 9000E

Usage Guidelines

By default, this command only allows routes to pass if the community string exactly matches the community attribute of the route.

Examples

```
-> ip bgp policy community-list commListC 600:1 match-type exact
```

Release History

Release 6.1; 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, for example, 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 6400, 6850E, 6855, 9000E

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.

Examples

```
-> ip bgp policy community-list commListB 500:1 priority 3
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

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.

Examples

```
-> ip bgp policy prefix-list prefixListA 12.0.0.0 255.0.0.0
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

Configures the action to be taken for a prefix list when a match is found.

Examples

```
-> ip bgp policy prefix-list prefixListA 12.0.0.0 255.0.0.0 action deny
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

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.

Examples

```
-> ip bgp policy prefix-list prefixListA 14.0.0.0 255.0.0.0 ge 8 le 16
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

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.

Examples

```
-> ip bgp policy prefix-list prefixListA 14.0.0.0 255.0.0.0 ge 8 le 16
```

Release History

Release 6.1; 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 prefix6-list

Configures a BGP prefix6-list policy for filtering IPv6 prefixes. This policy can be applied to filter unique local IPv6 addresses.

ip bgp policy prefix6-list *pfx_list_name prefix6/pfx_length* **[action{permit|deny}] [status{enable|disable}] [ge[**{*masklength*}**]] [le[**{*masklength*}**]]**

no ip bgp policy prefix6-list *pfx_list_name prefix6/pfx_length* **[action{permit|deny}] [status{enable|disable}] [ge[**{*masklength*}**]] [le[**{*masklength*}**]]**

Syntax Definitions

pfx_list_name	Prefix list name.
prefix6	Prefix list IPv6 address for the prefix list.
pfx_length	Prefix length. Prefix length should be in the range of 0 to 128.
permit | **deny**	Action to be taken which can be either permit or deny.
enable | **disable**	Row Status can be either enabled or disabled.
masklength	Minimum length of the prefix to be matched. It should be in the range of 0 - 32.
masklength	Maximum length of the prefix to be matched. It should be in the range of 0 - 32.

Defaults

NA

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to disable this feature.
- BGP must be configured on the system.
- The **ge** (lower limit) value must be greater than or equal to the prefix length and less than or equal to the **le** (upper limit) value.

Examples

```
-> ip bgp policy prefix6-list uniqLocal FC00::/48
-> ip bgp policy prefix6-list uniqLocal FC00::/48 action permit
-> ip bgp policy prefix6-list uniqLocal FC00::/48 status enable
-> no ip bgp policy prefix6-list uniqLocal FC00::/48
```

Release History

Release 6.3.4; command was introduced.

Related Commands

show ip bgp policy prefix6-list	Displays configured prefix6-list policies on the system.
show ipv6 bgp neighbors policy	Displays incoming and outgoing prefix6 list policy indentifiers configured for BGP IPv6 peer.

MIB Objects

```
alaBgpPrefix6MatchListTable
   alaBgpPrefix6MatchListId
   alaBgpPrefix6MatchListAddr
   alaBgpPrefix6MatchListAddrLength
   alaBgpPrefix6MatchListAction
   alaBgpPrefix6MatchListRowStatus
   alaBgpPrefix6MatchListGE
   alaBgpPrefix6MatchListLE
```

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 6400, 6850E, 6855, 9000E

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.

Examples

```
-> ip bgp policy route-map routemap1 1
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

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.

Examples

```
-> ip bgp policy route-map routemap1 1 action deny
```

Release History

Release 6.1; command was introduced.

Related Commands

ip bgp policy prefix6-list	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 6400, 6850E, 6855, 9000E

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.

Examples

```
-> ip bgp policy route-map routemap1 1 aspath-list aspathlist1
-> ip bgp policy route-map routemap1 1 aspath-list none
```

Release History

Release 6.1; command was introduced.

Related Commands

ip bgp policy prefix6-list	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**”**. Note that multiple AS path entries must be enclosed in quotes (for example, “500 600 700”).

Defaults

parameter	default
path	none

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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**”**.

Examples

```
-> ip bgp policy route-map routemap1 1 asprepend “700 800 900”
```

Release History

Release 6.1; command was introduced.

Related Commands

ip bgp policy prefix6-list	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 6400, 6850E, 6855, 9000E

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**.

Examples

```
-> 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 6.1; command was introduced.

Related Commands

ip bgp policy prefix6-list	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 6400, 6850E, 6855, 9000E

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**”.

Examples

```
-> ip bgp policy route-map routemap1 1 community-list listB
```

Release History

Release 6.1; command was introduced.

Related Commands

ip bgp policy prefix6-list	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 6400, 6850E, 6855, 9000E

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.

Examples

```
-> 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 6.1; command was introduced.

Related Commands

ip bgp policy prefix6-list	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 6400, 6850E, 6855, 9000E

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.

Examples

```
-> ip bgp policy route-map routemap1 1 lpref 555
-> ip bgp policy route-map routemap1 1 lpref 555 lpref-mode inc
```

Release History

Release 6.1; command was introduced.

Related Commands

ip bgp policy prefix6-list	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 6400, 6850E, 6855, 9000E

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.

Examples

```
-> 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 6.1; command was introduced.

Related Commands

ip bgp policy prefix6-list	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 6400, 6850E, 6855, 9000E

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**".

Examples

```
-> ip bgp policy route-map routemap1 1 match-community 400:1 500 700:1
```

Release History

Release 6.1; command was introduced.

Related Commands

ip bgp policy prefix6-list	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 6400, 6850E, 6855, 9000E

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.

Examples

```
-> 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 6.1; command was introduced.

Related Commands

ip bgp policy prefix6-list	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 6400, 6850E, 6855, 9000E

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.

Examples

```
-> 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 6.1; command was introduced.

Related Commands

ip bgp policy route-map match-mask	Configures a matching prefix primitive in the route map.
ip bgp policy prefix6-list	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 6400, 6850E, 6855, 9000E

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 30-97.
- 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 AOS Release 6 Advanced Routing Configuration Guide* for more information on the use of regular expressions in BGP commands.

Examples

```
-> ip bgp policy route-map routemap1 1 match-regexp "500 .* 400$"
```

Release History

Release 6.1; command was introduced.

Related Commands

ip bgp policy prefix6-list	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 6400, 6850E, 6855, 9000E

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.

Examples

```
-> ip bgp policy route-map routemap1 1 med 555
-> ip bgp policy route-map routemap1 1 med 555 med-mode inc
```

Release History

Release 6.1; 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 prefix6-list	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 6400, 6850E, 6855, 9000E

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.

Examples

```
-> 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 6.1; 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 prefix6-list	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 6400, 6850E, 6855, 9000E

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**”.

Examples

```
-> ip bgp policy route-map routemap1 1 origin egp
```

Release History

Release 6.1; command was introduced.

Related Commands

ip bgp policy route-map origin	Configures action to take on origin attribute when a match is found.
ip bgp policy prefix6-list	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 6400, 6850E, 6855, 9000E

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.

Examples

```
-> ip bgp policy route-map routemap1 1 prefix-list listC
```

Release History

Release 6.1; 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 prefix6-list	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 6400, 6850E, 6855, 9000E

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.

Examples

```
-> ip bgp policy route-map routemap1 1 weight 500
```

Release History

Release 6.1; command was introduced.

Related Commands

ip bgp policy prefix6-list	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 6400, 6850E, 6855, 9000E

Usage Guidelines

Configures the value to strip from the community attribute of the routes matched by this route map instance (sequence number).

Examples

```
-> ip bgp policy route-map routemap1 1 commmunity_strip communitylist
```

Release History

Release 6.1; command was introduced.

Related Commands

ip bgp policy prefix6-list	Configures an AS path matching regular expression primitive in the route map.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapCommunityStrip
```

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 6400, 6850E, 6855, 9000E

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.

Examples

```
-> 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 Fail Over               = disabled,
Log Neighbor Changes                 = disabled,
Multi path                            = disabled,
Graceful Restart                      = enabled,
Graceful Restart Status               = Not Restarting,
Configured Graceful Restart Interval = 90s,
IPv4 Unicast                          = enabled,
IPv6 Unicast                          = 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.

output definitions (continued)

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.
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.
Graceful Restart	Indicates whether graceful restart is enabled or disabled.

output definitions (continued)

Graceful Restart Status	Indicates the graceful restart state. This feature is not supported in Multiprotocol BGP.
Configured Graceful Restart Interval	Indicates the timer for achieving a graceful restart.
IPv4 Unicast	Indicates whether IPv4 unicast is enabled or disabled.
IPv6 Unicast	Indicates whether IPv6 unicast is enabled or disabled.

Release History

Release 6.1; command was introduced.
Release 6.1.5; fields added.

Related Commands

ipv6 bgp unicast	Enables or disables unicast IPv4 updates for the BGP routing process.
ipv6 bgp unicast	Enables or disables unicast IPv6 updates for the BGP routing process
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 6400, 6850E, 6855, 9000E

Usage Guidelines

This command show various BGP statistics for the router, such as number of neighbors, active prefixes, number of paths, and so on.

Examples

```
-> 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 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

This command shows the setting for dampening on the router, assuming it is enabled.

Examples

```
-> 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 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

This command displays various statistics on routes that have flapped, and are thus subject to the settings of the dampening feature.

Examples

```
-> 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 router.
Mask	The mask for the local BGP speaker that is responsible for route dampening in this router.
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 6.1; 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 6400, 6850E, 6855, 9000E

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.

Examples

```
-> show ip bgp path
Legends: Sta     = Path state
         >       = best, F = feasible, S = Stale
         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      i100
 >  192.40.6.0      255.255.255.248 192.40.4.29     192.40.4.29      i100
 >  192.40.6.8      255.255.255.248 192.40.4.29     192.40.4.29      i100
 U  110.100.10.0    255.255.255.0   2001:100:3:4::1 110.100.10.20    ?    100
 U  110.100.11.0    255.255.255.0   2001:100:3:4::1 110.100.10.20    ?    100
 U  110.100.12.0    255.255.255.0   2001:100:3:4::1 110.100.10.20    ?    100
 U  110.100.13.0     255.255.255.0  2001:100:3:4::1 110.100.10.20    ?    100
 U  110.100.14.0     255.255.255.0  2001:100:3:4::1 110.100.10.20    ?    100
```

output definitions

Sta	Status flag. “>” Best Path: Indicates this is the best route to the destination. “F" Feasible: The alternate path available when the best path goes down. “S” Stale: Indicates the peer that advertised this route's next hop is in the process of graceful restart. “P” Policy Changing: Indicates that a policy being applied may change the route. “U” Unsynchronized: Making a path unfeasible forcefully when a nexthop is not reachable or if the local bgp network is deleted." “D” Dampened: Indicates that this route is being dampened to prevent flapping. “N” None: No path available.
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 or IPv6 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 an 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.

output definitions (continued)

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.
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 router does not support. For example, multi-protocol attributes are currently not supported by the router, but it is possible for these attributes to appear in a BGP route.

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

This command displays all the routes in the routing table with details.

Examples

```
-> 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 6.1; command was introduced.

Related Commands

show ip bgp path	Displays BGP paths.

MIB Objects

```
alaBgpRouteTable
   alaBgpRouteEntry
```

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 6400, 6850E, 6855, 9000E

Usage Guidelines

This command displays a specific aggregate address, or all aggregate addresses on the router.

Examples

```
-> show ip bgp aggregate-address
Network         Mask            Summarize As-Set   Admin state Oper state
--------------+---------------+---------+--------+-----------+----------
20.20.20.20 255.255.255.255 disabled  disabled disabled    not_active
10.10.10.10 255.255.255.255 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 message 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 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

This command displays all the configured networks, or a single network.

Examples

```
-> show ip bgp network
Network         Mask            Admin state Oper state
---------------+---------------+-----------+----------
20.20.20.20 255.255.255.255 disabled    not_active
20.20.20.21 255.255.255.255 disabled    not_active


-> show ip bgp network 20.20.20.20 255.255.255.255
Network address          = 20.20.20.20,
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 6.1; command was introduced.

Related Commands

ip bgp network	Configures a local BGP network.

MIB Objects

```
alabgpMIBNetworkGroup
   alaBgpNetworkEntry
```

show ip bgp neighbors

Displays the configured IPv4 BGP peers.

show ip bgp neighbors [*ip_address*]

Syntax Definitions

ip_address	A 32-bit IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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.

Examples

```
-> show ip bgp neighbors
Legends:Nbr = Neighbor
         As = Autonomous System
Nbr address     As    Admin state Oper state   BgpId           Up/Down
---------------+-----+-----------+------------+---------------+-----------
10.10.10.10 3     enabled     estab        192.40.4.29     00h:14m:48s
10.10.10.11 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
Graceful Restart State            = None,
Advertised Restart Interval       = 0s,
Forwarding State during restart   = NotPreserved,
Activate IPv6 unicast             = enabled,
Configured IPv6 NextHop Address   = ::,
Neighbor Ipv6 unicast             = advertised
```

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" (that is, 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.

output definitions (continued)

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.
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 router 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 router is IPv4 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 router is not IPv4 multicasts capable so all peers will be disabled for this capability.
Neighbor type	Indicates whether this peer is internal or external to the router.
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.
Graceful Restart State	Indicates the graceful restart state. This feature is not supported in Multiprotocol BGP.
Advertised Restart Interval	Indicates the restart interval in seconds.

output definitions (continued)

Forwarding State during restart	Indicates whether the peer has preserved the forwarding state during the graceful restart.
Activate IPv6 unicast	Indicates if the IPv6 unicast updates are enabled or not. Options include **enabled** or **disabled**.
Configured IPv6 NextHop Address	Specifies the IPv6 nexthop address. This is specified using the **ipv6 bgp neighbor ipv6-nexthop** command.
Neighbor Ipv6 unicast	Indicates whether Multiprotocol IPv6 Unicast capability is enabled or disabled between the peers.

Release History

Release 6.1; command was introduced.
Release 6.1.5; fields added.

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 the incoming and outgoing prefix6 list policy identifiers configured for the specified BGP IPv4 peer.

show ip bgp neighbors policy *ipv4_address*

Syntax Definitions

ipv4_address	A 32-bit IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

This command displays all of the configured policies for the router, or the polices configured for a specific BGP IPv4 peer.

Examples

```
-> 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 output prefix6-list name   = uniqeLocal
  Neighbor input prefix6-list name    = uniqeLocal
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
  Neighbor output prefix6-list name   = UniqueLocal
  Neighbor input prefix6-list name    = UniqueLocal
```

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 in-prefix6list** 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.
Neighbor output prefix6-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 prefix6-list name	The inbound prefix list policy for the peer. This can be assigned by using the **ip bgp neighbor out-prefixlist** command.

Release History

Release 6.1; command was introduced.
Release 6.3.4; **soft reconfiguration**, **output perfix6-list**, **input prefix6-list** parameters added.

Related Commands

show ip bgp neighbors	Displays BGP peer main status.

MIB Objects

```
alabgpPeerTable
   alaBgpPeer6Addr
   alaBgpPeerPrefix6ListIn
   alaBgpPeerPrefix6ListOut
```

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 6400, 6850E, 6855, 9000E

Usage Guidelines

This command displays the timer values for all peer associated with this speaker, or for a specific peer.

Examples

```
-> 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)
---------------+-----+-----+-------+-----+-----+------+-----
20.20.20.20     3     90    90      30    120   30     30
20.20.20.21     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 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

This command displays message statistics for all peers associated with this speaker, or with a specific peer.

Examples

```
-> 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
---------------+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----
20.20.20.20     3     110   123   5     0     0     1     8     2     2
20.20.20.21     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 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 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 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- This command displays a list of all of the AS path policies for the router, 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 30-97.
- When using regular expressions in the CLI, the regular expression must be enclosed by quotation marks.

Examples

```
-> 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 enable or disable.
Priority	The AS path list priority. This is 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 6.1; 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 6400, 6850E, 6855, 9000E

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.

Examples

```
-> 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 (continued)

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 6.1; 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 6400, 6850E, 6855, 9000E

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.

Examples

```
-> 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 6.1; 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 prefix6-list

Displays the configured prefix6-list policies on the system.

show ip bgp policy prefix6-list [pfx_list_name**[{**prefix6/prefix_length**}]]**

Syntax Definitions

pfx_list_name	A prefix list name.
prefix6	A prefix list IPv6 address.
prefix_length	The number of bits that are significant in the IPv6 address (mask). The valid range is 3-128.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 IPv6 address and IPv6 mask.

Examples

```
-> show ip bgp policy prefix6-list

Prefix6 List name      Prefix6 address/Prefix length
--------------------+------------------------------
pl1                    fc00::/7

-> show ip bgp policy prefix6-list pl1

Prefix6 List name = pl1
Prefix          = fc00::
Prefix Length   = 7
   Admin state        = disabled,
   Match MaskLength   >= (GE) = 0,
   Match MaskLength  <= (LE) = 0,
   Action             = deny
```

output definitions

Prefix6 List name	The name of the prefix6-list. This is defined using the **ip bgp policy prefix6-list** command.
Prefix6 Address	The IPv6 address of the prefix6-list. This is defined using the **ip bgp policy prefix6-list** command.
Prefix Length	The mask of the prefix6-list. This is defined using the **ip bgp policy prefix6-list** command.

output definitions (continued)

Admin state	The administrative state of the prefix list, either enabled or disabled.
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 6.3.4; command was introduced.

Related Commands

ip bgp policy prefix6-list	Creates or deletes a BGP prefix6-list policy for filtering IPv6 prefix.

MIB Objects

```
alaBgpPrefix6MatchListTable
   alaBgpPrefix6MatchListId
   alaBgpPrefix6MatchListAddr
   alaBgpPrefix6MatchListAddrLength
   alaBgpPrefix6MatchListRowStatus
   alaBgpPrefix6MatchListGE
   alaBgpPrefix6MatchListLE
   alaBgpPrefix6MatchListAction
```

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 6400, 6850E, 6855, 9000E

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.

Examples

```
-> 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 prefix6-list** command.
RouteMap instance	The instance of the route map policy. This is determined using the **ip bgp policy prefix6-list** 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 6.1; command was introduced.

Related Commands

ip bgp policy prefix6-list	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

ip bgp graceful-restart

Configures support for the graceful restart feature on a BGP router.

ip bgp graceful-restart

no ip bgp graceful-restart

Syntax Definitions

N/A

Defaults

Graceful restart is enabled by default.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to disable support for the graceful restart feature on a BGP router. It has only unplanned graceful restart.
- The minimum hardware configuration for this command is a redundant CMM configuration. This command is not supported on a chassis with a single CMM or on an in a standalone switch.
- On an OmniSwitch stackable switch graceful restart is supported only on active ports (that is, interfaces) that are on the secondary or idle modules in a stack during a takeover. It is not supported on ports on a primary element in a stack.
- Note that graceful restart does not support IPv6 prefixes at this time.

Examples

```
-> ip bgp graceful restart
-> no ip bgp graceful restart
```

Release History

Release 6.1.3; command was introduced.

Related Commands

show ip bgp	Displays the current global settings for the local BGP speaker.

MIB Objects

```
alaBgpGlobal
   alaBgpGracefulRestart
   alaBgpRestartInterval
```

ip bgp graceful-restart restart-interval

Configures the grace period for achieving a graceful BGP restart.

ip bgp graceful-restart restart-interval [*seconds***]**

Syntax Definitions

seconds	The hitless restart timeout interval, in seconds. The valid range is 1–3600.

Defaults

parameter	default
seconds	90

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The minimum hardware configuration for this command is a redundant CMM configuration. This command is not supported on a chassis-based switch with a single CMM or on a standalone switch.
- On a stackable switch, a graceful restart is supported only on active ports (that is, interfaces) that are on the secondary or idle modules in a stack during a takeover. It is not supported on ports on a primary element in a stack.
- Note that graceful restart does not support IPv6 prefixes at this time.

Examples

```
-> ip bgp graceful-restart restart-interval 600
```

Release History

Release 6.1.3; command was introduced.

Related Commands

show ip bgp	Displays the current global settings for the local BGP speaker.

MIB Objects

```
alaBgpGlobal
   alaBgpGracefulRestart
   alaBgpRestartInterval
```

ipv6 bgp unicast

Enables or disables unicast IPv6 advertisements for the BGP routing process.

ipv6 bgp unicast

no ipv6 bgp unicast

Syntax Definitions

N/A

Defaults

By default, IPv6 BGP advertisements are disabled.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to turn off IPv6 unicast advertisements.
- BGP should be disabled before enabling or disabling IPv6 unicast advertisements.

Examples

```
-> ipv6 bgp unicast
-> no ipv6 bgp unicast
```

Release History

Release 6.1.5; command was introduced.

Related Commands

ipv6 bgp unicast	Enables or disables unicast IPv4 updates for the BGP routing process.
show ip bgp	Displays the current global settings for the local BGP speaker.

MIB Objects

```
alaBgpGlobal
   alaBgpMultiProtocolIpv6
```

ip bgp neighbor activate-ipv6

Enables or disables the exchange of IPv6 unicast routes between BGP peer routers identified by their IPv4 addresses.

ip bgp neighbor *ip_address* **activate-ipv6**

no ip bgp neighbor i*p_address* **activate-ipv6**

Syntax Definitions

ip_address	The 32-bit IPv4 address of the neighbor.

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the **no** form of this command to disable the exchange of IPv6 unicast routes between BGP peer routers identified by their IPv4 addresses.

Examples

```
-> ip bgp neighbor 1.0.0.1 activate-ipv6
-> no ip bgp neighbor 1.0.0.1 activate-ipv6
```

Release History

Release 6.1.5; command was introduced.

Related Commands

show ip bgp neighbors	Displays BGP peer main status.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerIpv6Unicast
```

ip bgp neighbor ipv6-nexthop

Configures the IPv6 next hop addresses for the IPv6 prefixes advertised between BGP peers. These BGP peers are identified by their IPv4 addresses.

ip bgp neighbor *ip_address* **ipv6-nexthop** *ipv6_address*

Syntax Definitions

ip_address	The 32-bit IPv4 address of the neighbor.
ipv6_address	A 128-bit global IPv6 address to be used as the next hop for IPv6 routes being advertised to this BGP speaker.

Defaults

By default, the IPv6 next hop value is set to all zeros.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- To reset the IPv6 next hop value, enter an all-zero address.
- For internal BGP (IBGP) peers, the IPv6 next hop is used only if the peer **next-hop-self** option is configured.
- For external BGP (EBGP) peers, the IPv6 next hop is used for all the advertised IPv6 routes.

Examples

```
-> ip bgp neighbor 1.0.0.1 ipv6-nexthop 2001:100:3:4::1
-> ip bgp neighbor 1.0.0.1 ipv6-nexthop ::
```

Release History

Release 6.1.5; command was introduced.

Related Commands

show ipv6 bgp neighbors	Displays the configured IPv6 BGP peers.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerIpv6NextHop
```

show ipv6 bgp path

Displays the known IPv6 BGP paths for all the routes or a specific route.

show ipv6 bgp path [ipv6-addr *ipv6_address/prefix_length***]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address.
/prefix_length	The number of bits that are significant in the IPv6 address (mask) (3..128).

Defaults

By default, IPv6 BGP paths for all the routes will be displayed.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the *ipv6_address/prefix_length* parameter to display the IPv6 BGP paths for a specified route.

Examples

```
-> show ipv6 bgp path
Legends: Sta     = Path state
         >       = best, F = feasible, S = stale
         U       = un-synchronized
         Nbr     = Neighbor
         (O)     = Path Origin (? = incomplete, i = igp, e = egp)
         degPref = degree of preference
Sta  Prefix                       Nbr Address                        (O) degPref
---+-----------------------------+----------------------------------+---+-------
 >  2020:100:200:1::/64          2001:100:3:4::1                     i   100
 >  2020:100:200:2::/64          2001:100:3:4::1                     i   100
 >  2020:100:200:3::/64          2001:100:3:4::1                     i   100
 >  2020:100:200:4::/64          2001:100:3:4::1                     i   100
 >  2020:100:200:5::/64          2001:100:3:4::1                     i   100
 >  2525:2525:1::/48             100.3.4.1                           i   100
 >  2525:2525:2::/48             100.3.4.1                           i   100
 >  2525:2525:3::/48             100.3.4.1                           i   100
 >  2525:2525:4::/48             100.3.4.1                           i   100
 >  2525:2525:5::/48             100.3.4.1                           i   100
```

output definitions

Sta	Status flag. “>” Best Path: Indicates this is the best route to the destination. “F" Feasible: The alternate path available when the best path goes down. “S” Stale: Indicates the peer that advertised this route's next hop is in the process of graceful restart. “P” Policy Changing: Indicates that a policy being applied may change the route. “U” Unsynchronized: Making a path unfeasible forcefully when a nexthop is not reachable or if the local bgp network is deleted." “D” Dampened: Indicates that this route is being dampened to prevent flapping. “N” None: No path available.
Prefix	The destination address of the IPv6 route in the hexadecimal format.
Nbr Address	The IP or IPv6 address of the BGP peer that advertises this 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 ipv6 bgp path ipv6-addr 2020:100:200:1::/64
BGP Path parameters
Path address   = 2020:100:200:1::
Path Length    = 64
Path protocol  = ibgp
Path neighbor  = peer(2001:100:3:4::1)
  Path nextHop            = 2001:100:3:4::1,
  Path origin             = igp,
  Path local preference   = 100,
  Path state              = active,
  Path weight             = 0,
  Path preference degree  = 100,
  Path autonomous systems = [nAs=0] : <none>,
  Path MED                = <none>,
  Path atomic             = no,
  Path AS aggregator      = <none>,
  Path IPaddr aggregator  = <none>,
  Path community          = <none>,
  Path Originator Id      = <none>,
  Path Cluster List       = <none>,
  Path unknown attribute  = <none>
```

output definitions

Path address	The IPv6 address for route path.
Path Length	The prefix length of the IPv6 path.

output definitions (continued)

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 neighbor	The IPv6 address of the BGP peer.
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	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 an 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.
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 Originator Id	The Router Id of the BGP4 speaker that performed route reflection

output definitions (continued)

Path Cluster List	Sequence of Cluster Id values representing the reflection path that the route has passed, if this is a reflected route in the local AS.
Path unknown attribute	Indicates BGP attributes found in UPDATE messages which the router does not support. For example, multi-protocol attributes are not supported by the router in this release, but it is possible for these attributes to appear in a BGP route.

Release History

Release 6.1.5; command was introduced.

Related Commands

show ipv6 bgp routes	Displays the known IPv6 BGP routes.

MIB Objects

alaBgpPath6Table
- alaBgpPath6Addr
- alaBgpPath6MaskLen
- alaBgpPath6PeerBgpId
- alaBgpPath6SrcProto
- alaBgpPath6Weight
- alaBgpPath6Pref
- alaBgpPath6State
- alaBgpPath6Origin
- alaBgpPath6NextHop
- alaBgpPath6As
- alaBgpPath6LocalPref
- alaBgpPath6Med
- alaBgpPath6Atomic
- alaBgpPath6AggregatorAs
- alaBgpPath6AggregatorAddr
- alaBgpPath6Community
- alaBgpPath6OriginatorId
- alaBgpPath6ClusterList
- alaBgpPath6PeerName
- alaBgpPath6UnknownAttr

show ipv6 bgp routes

Displays the known IPv6 BGP routes.

show ipv6 bgp routes

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show ipv6 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
 Prefix                          ECL ICC ICL LCL AGG AGC AGL AGW AGH GDL DMP ACT
--------------------------------+---+---+---+---+---+---+---+---+---+---+---+----
 2020:100:200:1::/64             No  No  No  No  No  No  No  No  No  No  No  Yes
 2020:100:200:2::/64             No  No  No  No  No  No  No  No  No  No  No  Yes
 2020:100:200:3::/64             No  No  No  No  No  No  No  No  No  No  No  Yes
 2020:100:200:4::/64             No  No  No  No  No  No  No  No  No  No  No  Yes
 2020:100:200:5::/64             No  No  No  No  No  No  No  No  No  No  No  Yes
 2525:2525:1::/48                No  No  No  No  No  No  No  No  No  No  No  Yes
 2525:2525:2::/48                No  No  No  No  No  No  No  No  No  No  No  Yes
 2525:2525:3::/48                No  No  No  No  No  No  No  No  No  No  No  Yes
 2525:2525:4::/48                No  No  No  No  No  No  No  No  No  No  No  Yes
 2525:2525:5::/48                No  No  No  No  No  No  No  No  No  No  No  Yes
```

output definitions

Prefix	The destination address of the IPv6 route in the hexadecimal format.
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 6.1.5; command was introduced.

Related Commands

show ipv6 bgp path	Displays the known IPv6 BGP paths for all the routes or a specific route.

MIB Objects

```
alaBgpRoute6Table
   alaBgpRoute6Addr
   alaBgpRoute6MaskLen
   alaBgpRoute6State
   alaBgpRoute6IsHidden
   alaBgpRoute6IsAggregate
   alaBgpRoute6IsAggregateContributor
   alaBgpRoute6IsAggregateList
   alaBgpRoute6IsAggregateWait
   alaBgpRoute6IsOnEbgpChgList
   alaBgpRoute6IsOnIbgpClientChgList
   alaBgpRoute6IsOnIbgpChgList
   alaBgpRoute6IsOnLocalChgList
   alaBgpRoute6IsOnDeleteList
   alaBgpRoute6IsDampened
```

ipv6 bgp network

Advertises a locally reachable IPv6 address as an IPv6 BGP network to other BGP peers.

ipv6 bgp network *ipv6_address/prefix_length*

no ipv6 bgp network *ipv6_address/prefix_length*

Syntax Definitions

ipv6_address	The 128-bit IPv6 address.
/prefix_length	The number of bits that are significant in the IPv6 address (mask) (3..128).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the **no** form of this command to turn off the advertisement of locally reachable IPv6 networks.

Examples

```
-> ipv6 bgp network 2001::1/64
-> no ipv6 bgp network 2001::1/64
```

Release History

Release 6.1.5; command was introduced.

Related Commands

ipv6 bgp network status	Enables or disables a BGP network.
show ipv6 bgp network	Displays the status of all the IPv6 BGP networks or a specific IPv6 BGP network

MIB Objects

```
alaBgpNetwork6Table
   alaBgpNetwork6Addr
   alaBgpNetwork6MaskLen
```

ipv6 bgp network community

Defines a community for a route created by the **ipv6 bgp network** command. Communities are a way of grouping BGP peers that do not share an IPv6 subnet or an AS.

ipv6 bgp network *ipv6_address/prefix_length* **[community {none** | *num* | *num:num***}]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address.
/prefix_length	The number of bits that are significant in the IPv6 address (mask) (3..128).
none	Removes a prefix from a community.
num	The community attribute number.
num:num	Community attribute in the AA : NN format. AA indicates the autonomous system and NN indicates the community number.

Defaults

By default, a route is not assigned to a community.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

The IPv6 BGP route created with the **ipv6 bgp network** command should exist before the **community** attribute is defined.

Examples

```
-> ipv6 bgp network 2004::2/64 community 23:20
```

Release History

Release 6.1.5; command was introduced.

Related Commands

ipv6 bgp network	Advertises a locally reachable IPv6 address as an IPv6 BGP network to other BGP peers.
show ipv6 bgp network	Displays the status of all the IPv6 BGP networks or a specific IPv6 BGP network

MIB Objects

```
alaBgpNetwork6Table
   alaBgpNetwork6Addr
   alaBgpNetwork6MaskLen
   alaBgpNetwork6Community
```

ipv6 bgp network local-preference

Defines the local preference value for a route generated by the **ipv6 bgp network** command. This value will override the default local preference value; it is used when announcing this network to internal peers.

ipv6 bgp network *ipv6_address/prefix_length* **[local-preference** *num***]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address.
/prefix_length	The number of bits that are significant in the IPv6 address (mask) (3..128).
num	The local preference attribute value. The valid range is 0–4294967295.

Defaults

parameter	default
num	0

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

The IPv6 BGP route created with the **ipv6 bgp network** command should exist before the **local-preference** attribute is defined.

Examples

```
-> ipv6 bgp network 2004::1/24 local-preference 6
```

Release History

Release 6.1.5; command was introduced.

Related Commands

ipv6 bgp network	Advertises a locally reachable IPv6 address as an IPv6 BGP network to other BGP peers
show ipv6 bgp network	Displays the status of all the IPv6 BGP networks or a specific IPv6 BGP network

MIB Objects

```
alaBgpNetwork6Table
   alaBgpNetwork6Addr
   alaBgpNetwork6MaskLen
   alaBgpNetwork6LocalPref
```

ipv6 bgp network metric

Configures the Multi-Exit Discriminator (MED) attribute value for an network generated by the **ipv6 bgp network** command. This value is sent from routers of one AS to another to indicate the path that the remote AS can use to send data to the local AS.

ipv6 bgp network *ipv6_address/prefix_length* **[metric** *num***]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address.
/prefix_length	The number of bits that are significant in the IPv6 address (mask) (3..128).
num	The MED attribute value. The valid range is 0–4294967295.

Defaults

parameter	default
num	0

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

The IPv6 BGP route created with the **ipv6 bgp network** command should exist before the **metric** attribute is defined for the same route.

Examples

```
-> ipv6 bgp network 2001::1/64 metric 20
```

Release History

Release 6.1.5; command was introduced.

Related Commands

ipv6 bgp network	Advertises a locally reachable IPv6 address as a IPv6 BGP network to other BGP peers.
show ipv6 bgp network	Displays the status of all the IPv6 BGP networks or a specific IPv6 BGP network

MIB Objects

```
alaBgpNetwork6Table
   alaBgpNetwork6Addr
   alaBgpNetwork6MaskLen
   alaBgpNetwork6Metric
```

ipv6 bgp network status

Enables or disables a BGP network. The BGP status must be manually enabled after configuring all the BGP neighbor and network parameters.

ipv6 bgp network *ipv6_address/prefix_length* **[status {enable | disable}]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address.
/prefix_length	The number of bits that are significant in the IPv6 address (mask) (3..128).
enable	Enables the BGP network.
disable	Disables the BGP network.

Defaults

By default, the BGP network is disabled.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

The IPv6 BGP route created with the **ipv6 bgp network** command should exist before the **status** attribute is defined.

Examples

```
-> ipv6 bgp network 2001::1/64 status enable
```

Release History

Release 6.1.5; command was introduced.

Related Commands

show ipv6 bgp network	Displays the status of all the IPv6 BGP networks or a specific IPv6 BGP network.

MIB Objects

```
alaBgpNetwork6Table
   alaBgpNetwork6Addr
   alaBgpNetwork6MaskLen
   alaBgpNetwork6RowStatus
```

show ipv6 bgp network

Displays the status of all the IPv6 BGP networks or a specific IPv6 BGP network.

show ipv6 bgp network [*ipv6_address/prefix_length***]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address.
/prefix_length	The number of bits that are significant in the IPv6 address (mask) (3..128).

Defaults

By default, all IPv6 BGP networks and their status will be displayed.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the *ipv6_address/prefix_length* parameter to display the status of a specific IPv6 BGP nework.

Examples

```
show ipv6 bgp network
 Network                            Admin state Oper state
-----------------------------------+-----------+----------
2525:500:600::/64                   enabled     active


show ipv6 bgp network 2525:500:600::/64
Network address          = 2525:500:600::/64,
Network admin state      = enabled,
Network oper state       = active,
Network metric           = 0,
Network local preference = 0,
Network community string = <none>
```

output definitions

Network or **Network address**	The IPv6 address configured for this local BGP network. This value is configured through the **ipv6 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 **ipv6 bgp network status** command.
Oper state or **Network oper state**	Indicates whether this BGP local network is operationally active or inactive.

output definitions (continued)

Network metric	The multi-exit discriminator (MED) value configured for this local BGP network. This value is configured through the **ipv6 bgp network metric** command.
Network local preference	The local preference value for this local BGP network. This value is configured through the **ipv6 bgp network local-preference** command.
Network community string	The community string value for this local BGP network. This value is configured through the **ipv6 bgp network community** command.

Release History

Release 6.1.5; command was introduced.

Related Commands

ipv6 bgp network	.Advertises a locally reachable IPv6 address as an IPv6 BGP network to other BGP peers.

MIB Objects

```
alaBgpNetwork6Table
   alaBgpNetwork6Addr
   alaBgpNetwork6MaskLen
   alaBgpNetwork6State
   alaBgpNetwork6Metric
   alaBgpNetwork6LocalPref
   alaBgpNetwork6Community
   alaBgpNetwork6RowStatus
```

ipv6 bgp neighbor

Creates or deletes a BGP peer relationship using IPv6 addresses.

ipv6 bgp neighbor *ipv6_address*

no ipv6 bgp neighbor *ipv6_address*

Syntax Definitions

ipv6_address	The 128-bit IPv6 address of the new BGP peer.

Defaults

By default, no BGP peers are configured in the BGP network.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete a BGP peer.
- To establish a BGP session, the BGP peer should be reachable.
- You must manually enable a BGP peer after creating it. A BGP peer is enabled using the **ipv6 bgp neighbor status** command.
- Once created, a BGP peer must be assigned an autonomous system number using the **ipv6 bgp neighbor remote-as** command.
- Use **update-source** keyword to configure the IPv6 interface when link-local address is used as neighbor address.

Examples

```
-> ipv6 bgp neighbor 2001::1
-> no ipv6 bgp neighbor 2001::1
```

Release History

Release 6.1.5; command was introduced.

Related Commands

ipv6 bgp neighbor status	Enables or disables the BGP peer status.
ipv6 bgp neighbor remote-as	Assigns an AS number to the BGP peer.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
```

ipv6 bgp neighbor clear soft

Invokes an inbound or outbound policy reconfiguration for an IPv6 BGP peer.

ipv6 bgp neighbor *peer6_address* **clear soft {in | out}**

Syntax Definitions

peer6_address	The 128-bit IPv6 address of the BGP peer.
in	Restarts inbound policy evaluation of the peer.
out	Restarts outbound policy evaluation of the peer.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- This command reconfigures (or reapplies) all inbound or outbound policies to existing routes without restarting the IPv6 peer session.
- This command is useful if policies have been changed.
- BGP neighbour must be configured.

Examples

```
-> ipv6 bgp neighbor 2001::1 clear soft in
-> ipv6 bgp neighbor 2001::1 clear soft out
```

Release History

Release 6.3.4; command was introduced.

Related Commands

ipv6 bgp neighbor soft-reconfiguration	Enables or disables IPv6 BGP peer soft reconfiguration.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeer6ddr
   alaBgpPeer6ReconfigureInBound
   alaBgpPeer6ReconfigureOutound
```

ipv6 bgp neighbor soft-reconfiguration

Enables or disables IPv6 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.

ipv6 bgp neighbor *peer6_address* **soft-reconfiguration**

no ipv6 bgp neighbor *peer6_address* **soft-reconfiguration**

Syntax Definitions

peer6_address	The 128-bit IPv6 address of the BGP peer.

Default

This command is enabled by default.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to disable this feature.
- 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.
- BGP neighbor must be configured.
- BGP peer is restarted after issuing this command.

Examples

```
-> ipv6 bgp neighbor 2021::10 soft-reconfiguration
-> no ipv6 bgp neighbor 2021::10 soft-reconfiguration
```

Release History

Release 6.3.4; command was introduced

Related Commands

ipv6 bgp neighbor clear soft	Invokes an inbound or outbound policy reconfiguration for an IPv6 BGP peer.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeer6Addr
   alaBgpPeer6SoftReconfig
```

ipv6 bgp neighbor in-prefix6list

Configures an inbound BGP prefix6-list policy for an IPv6 BGP peer.

ipv6 bgp neighbor *peer6_address* **in-prefix6list** *pfx_list_name*

Syntax Definitions

peer6_address	The 128-bit IPv6 address of the BGP peer.
pfx_list_name	An Output prefix list name (1 - 70 characters).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The prefix list name (**uniqLocal** in the example below) is created using the **ip bgp policy prefix6-list** command. Any outbound routes from the BGP peer must match this prefix filter before being advertised or passed to outbound policy.
- BGP neighbor must be configured.

Examples

```
-> ipv6 bgp neighbor 2021::10 in-prefix6list uniqLocal
```

Release History

Release 6.3.4; command was introduced.

Related Commands

ip bgp policy prefix6-list	Creates or deletes a BGP prefix6-list policy for filtering IPv6 prefixes.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeer6Addr
   alaBgpPeer6Prefix6ListIn
```

ipv6 bgp neighbor out-prefix6list

Configures an outgoing BGP prefix6-list policy for an IPv6 BGP peer.

ipv6 bgp neighbor *peer6_address* **out-prefix6list** *pfx_list_name*

Syntax Definitions

peer6_address	The 128-bit IPv6 address of the BGP peer.
pfx_list_name	An Output prefix list name (1 - 70 characters). .

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The prefix list name (**uniqLocal** in the example below) is created using the **ip bgp policy prefix6-list** command. Any outbound routes from the BGP peer must match this prefix filter before being advertised or passed to outbound policy.
- BGP neighbor must be configured.

Examples

```
-> ipv6 bgp neighbor 2021::10 out-prefix6list uniqLocal
```

Release History

Release 6.3.4; command was introduced.

Related Commands

ip bgp policy prefix6-list	Creates or deletes a BGP prefix6-list policy for filtering IPv6 prefixes.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeer6Addr
   alaBgpPeer6Prefix6ListOut
```

ipv6 bgp neighbor activate-ipv6

Enables the exchange of IPv6 unicast routes between BGP peer routers identified by their IPv6 addresses.

ipv6 bgp neighbor *ipv6_address* **[activate-ipv6]**

no ipv6 bgp neighbor i*pv6_address* **[activate-ipv6]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address.

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the **no** form of this command to disable the exchange of IPv6 unicast routes between BGP peer routers identified by their IPv6 addresses.

Examples

```
-> ipv6 bgp neighbor 1.0.0.1 activate-ipv6
-> no ipv6 bgp neighbor 1.0.0.1 activate-ipv6
```

Release History

Release 6.1.5; command was introduced.

Related Commands

show ipv6 bgp neighbors	Displays the configured IPv6 BGP peers.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeer6ActivateIpv6
```

ipv6 bgp neighbor ipv6-nexthop

Configures the IPv6 next hop addresses for IPv6 prefixes advertised between BGP peers. These BGP peers are identified by their IPv6 addresses.

ipv6 bgp neighbor *ipv6_address* **[ipv6-nexthop** *ipv6_address***]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address of the next hop router.

Defaults

By default, the IPv6 next hop address is set to all zeros.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- To reset the IPv6 next hop value, enter an all-zero address.
- For internal BGP (IBGP) peers, the IPv6 next hop is used only if the peer **next-hop-self** option is configured.
- For external BGP (EBGP) peers, the IPv6 next hop is used for all the advertised IPv6 routes.
- For BGP peers configured with their link-local addresses, the configured IPv6 next hop is used while advertising IPv6 prefixes.

Examples

```
-> ipv6 bgp neighbor 2001::1 ipv6-nexthop fe80::/24
-> no ipv6 bgp neighbor 2001::1 ipv6-nexthop fe80::/24
```

Release History

Release 6.1.5; command was introduced.

Related Commands

show ipv6 bgp neighbors	Displays the configured IPv6 BGP peers.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeerIpv6NextHop
```

ipv6 bgp neighbor status

Enables or disables the BGP peer status. These peers are identified by their IPv6 addresses.

ipv6 bgp neighbor *ipv6_address* **[status {enable | disable}]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address of the new BGP peer.
enable	Enables the BGP peer.
disable	Disables the BGP peer.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- You should first create a BGP peer and assign it an IPv6 address using the **ipv6 bgp neighbor** command before enabling the peer.
- You should configure all the BGP peer related commands before enabling a BGP peer. Once you have enabled the peer, it will begin sending BGP connection and route advertisement messages.

Examples

```
-> ipv6 bgp neighbor 2001::1 status enable
-> ipv6 bgp neighbor 2001::1 status disable
```

Release History

Release 6.1.5; command was introduced.

Related Commands

show ipv6 bgp neighbors	Displays the configured IPv6 BGP peers.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeer6RowStatus
```

ipv6 bgp neighbor remote-as

Assigns an AS number to the BGP peer.

ipv6 bgp neighbor *ipv6_address* **[remote-as** *num***]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address of the BGP peer.
num	Autonomous system number in the range 1–65535.

Defaults

parameter	default
num	1

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- A BGP peer created with the **ipv6 bgp neighbor** command cannot be enabled until it is assigned an autonomous system number. If the AS number assigned to the peer matches the AS number of 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 considered external to the local BGP speaker's AS.
- The BGP peer is restarted after issuing this command.

Examples

```
-> ipv6 bgp neighbor 2001::1 remote-as 100
```

Release History

Release 6.1.5; command was introduced.

Related Commands

ip bgp autonomous-system	Sets the AS for the local BGP speaker.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeer6AS
```

ipv6 bgp neighbor timers

Configures the KEEPALIVE message interval and hold time interval (in seconds) with regards to the specified BGP peer.

ipv6 bgp neighbor *ipv6_address* **[timers** *num num***]**

Syntax Definitions

ipv6_address	A 128-bit IPv6 address for the BGP peer.
num	The KEEPALIVE message interval in seconds.
num	The hold time interval in seconds.

Defaults

parameter	default
num (keepalive)	30 seconds
num (holdtime)	90 seconds

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- KEEPALIVE messages do not contain route updates or indicate a change in the status of the BGP peer; they indicate to the receiving BGP peer that the connection is still live and the peer is reachable.
- By default, the KEEPALIVE interval of 30 seconds is one-third the default hold time interval of 90 seconds. The KEEPALIVE interval can never be more than one-third the value of the hold time interval. When the hold time interval is reached without receiving KEEPALIVE or other updates messages, the peer is considered dead.
- Setting the KEEPALIVE value to zero means no KEEPALIVE messages will be sent.
- 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.
- The hold timer is used during the connection setup process and for on-going connection maintenance with BGP peers. If the peer does not receive a KEEPALIVE, UPDATE, or NOTIFICATION message within this time period, then the BGP connection will be closed.
- Both the KEEPALIVE and hold time interval should be set at the same time.
- Using this command without the variables resets the variables to their default value.

Examples

```
-> ipv6 bgp neighbor 2001::1 timers 80 240
```

Release History

Release 6.1.5; command was introduced.

Related Commands

ipv6 bgp neighbor conn-retry-interval	The interval, in seconds, between BGP retries to set up a connection with another peer via the transport protocol.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeer6HoldTime
   alaBgpPeer6KeepAlive
```

ipv6 bgp neighbor maximum-prefix

Configures the maximum number of prefixes, or paths, the local router can receive from a BGP peer in UPDATE messages.

ipv6 bgp neighbor *ipv6_address* **[maximum-prefix** *num* **[warning-only]]**

no ipv6 bgp neighbor *ipv6_address* **[maximum-prefix** *num* **[warning-only]]**

Syntax Definitions

ipv6_address	A 128-bit IPv6 address for the BGP peer.
num	The number of prefixes. The valid range is 0–4294967295.

Defaults

parameter	default
num	5000

By default, **warning-only** is enabled.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- When the number of prefixes sent by the BGP peer reaches the maximum limit, the peer is restarted.
- You can use BGP logging to receive a warning when the number of prefixes received from the 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.
- The BGP peer is restarted after issuing this command.

Examples

```
-> ipv6 bgp neighbor 2001::2 maximum-prefix 1000 warning-only
-> no ipv6 bgp neighbor 2001::2 maximum-prefix 1000
```

Release History

Release 6.1.5; command was introduced.

Related Commands

show ipv6 bgp neighbors	Displays the configured IPv6 BGP peers.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeer6MaxPrefix
   alaBgpPeer6MaxPrefixWarnOnly
```

ipv6 bgp neighbor next-hop-self

Configures router to advertise its peering address as the next hop address for the specified neighbor.

ipv6 bgp neighbor *ipv6_address* **[next-hop-self]**

no ipv6 bgp neighbor *ipv6_address* **[next-hop-self]**

Syntax Definitions

ipv6_address	A 128-bit IPv6 address for the BGP peer.

Defaults

By default, the **next-hop-self** parameter of BGP updates is disabled.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to disable the **next-hop-self** parameter.
- In meshed networks, the 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 the 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.
- The BGP peer is restarted after issuing this command.

Examples

```
-> ipv6 bgp neighbor 2001::2 next-hop-self
-> no ipv6 bgp neighbor 2001::2 next-hop-self
```

Release History

Release 6.1.5; command was introduced.

Related Commands

show ipv6 bgp neighbors	Displays the configured IPv6 BGP peers.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeer6NextHopSelf
```

ipv6 bgp neighbor conn-retry-interval

The interval, in seconds, between BGP retries to set up a connection with another peer via the transport protocol. In the connect state, BGP tries to set up a connection with a remote peer. If the connection fails, then the connection retry interval starts. Once this interval elapses, BGP retries setting up the connection.

ipv6 bgp neighbor *ipv6_address* **[conn-retry-interval** *num***]**

Syntax Definitions

ipv6_address	A 128-bit IPv6 address for the BGP neighbor.
num	The time interval (in seconds) between retries. The valid range is 0–65535.

Defaults

parameter	default
num	120

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The connection retry time interval starts when a connection to a peer is lost.
- Using this command without the *num* variable resets the variable to its default value.

Examples

```
-> ipv6 bgp neighbor 2001::2 conn-retry-interval 60
```

Release History

Release 6.1.5; command was introduced.

Related Commands

show ipv6 bgp neighbors	Displays the configured IPv6 BGP peers.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeer6ConnRetryInterval
```

ipv6 bgp neighbor default-originate

Enables or disables the BGP local speaker to advertise a default route to the peer.

ipv6 bgp neighbor *ipv6_address* **[default-originate]**

no ipv6 bgp neighbor *ipv6_address* **[default-originate]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address for the neighbor.

Defaults

This **default-originate** parameter is disabled by default.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to disable the BGP peer default origination.
- When this command is enabled, the local BGP speaker advertises the default route to the peer. Such a default route overrides any learned default (propagation) and outbound policy. The default route `::/0` does not need to exist on the local router.
- If the peer is capable of exchanging IP as well as IPv6 prefixes, the default route for both IP and IPv6 is advertised.

Examples

```
-> ipv6 bgp neighbor 2001::1 default-originate
-> no ipv6 bgp neighbor 2001::1 default-originate
```

Release History

Release 6.1.5; command was introduced.

Related Commands

show ipv6 bgp neighbors	Displays the configured IPv6 BGP peers.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeer6DefaultOriginate
```

ipv6 bgp neighbor update-source

Configures the local IPv6 interface from which a BGP peer will be connected. This local IPv6 interface can be configured for internal and external BGP peers.

ipv6 bgp neighbor *ipv6_address* **[update-source** *interface_name***]**

no ipv6 bgp neighbor *ipv6_address* **[update-source** *interface_name***]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address for the BGP peer.
interface_name	The name of the local IPv6 interface that provides the TCP connection for this BGP peer.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The BGP peer is restarted after issuing this command.
- If a BGP peer is configured with its link-local address, use the **update-source** parameter to specify the name of the IPv6 interface from which this peer is reachable. This is required to establish a BGP peering session.

Examples

```
-> ipv6 bgp neighbor 2004::1 update-source bgp_ipv6
-> no ipv6 bgp neighbor 2004::1 update-source bgp_ipv6
```

Release History

Release 6.1.5; command was introduced.

Related Commands

show ipv6 bgp neighbors	Displays the configured IPv6 BGP peers.
ipv6 interface	Configures an IPv6 interface on a VLAN or IPv6 tunnel.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeer6LocalIntfName
```

ipv6 bgp neighbor ipv4-nexthop

Configures the IPv4 next hop addresses for IPv4 prefixes advertised between BGP peers. These BGP peers are identified by their IPv6 addresses.

ipv6 bgp neighbor *ipv6_address* **[ipv4-nexthop** *ip_address***]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address for the BGP peer.
ip_address	The 32-bit IP address of the next hop.

Defaults

By default, the IPv4 next hop value is set to all zeros.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

To reset the IPv4 next hop value, enter an all-zero address.

Examples

```
-> ipv6 bgp neighbor 2004::1 ipv4-nexthop 172.22.2.115
-> ipv6 bgp neighbor 2004::1 ipv4-nexthop 0.0.0.0
```

Release History

Release 6.1.5; command was introduced.

Related Commands

show ipv6 bgp neighbors .Displays the configured IPv6 BGP peers.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeer6Ipv4NextHop
```

show ipv6 bgp neighbors

Displays the configured IPv6 BGP peers.

show ipv6 bgp neighbors [*ipv6_address***]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address of the BGP neighbor.

Defaults

By default, all the configured IPv6 BGP peers will be displayed.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the *ipv6_address* parameter to display the details of a specified IPv6 BGP peer.

Examples

```
-> show ipv6 bgp neighbors
Legends: Nbr = Neighbor
         As  = Autonomous System
Nbr address                As   Admin state  Oper state   BGP Id      Up/Down
--------------------------+-----+-----------+------------+------------+---------
2001:100:3:4::1            30   enabled     established  11.4.0.1     01h:42m:08s
fe80::200:57ff:fe28:7e89   10   enabled     established  11.5.0.1     01h:40m:58s


-> show ipv6 bgp neighbors 2001:100:3:4::1
Neighbor address                  = 2001:100:3:4::1,
Neighbor autonomous system        = 30,
Neighbor Admin state              = enabled,
Neighbor Oper state               = established,
Neighbor passive status           = disabled,
Neighbor name                     = peer(2001:100:3:4::1),
Neighbor local address            = 2001:100:3:4::10,
Neighbor EBGP multiHop            = disabled,
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            = 10,
```

```
Neighbor MD5 key                  = <none>,
Neighbor local port               = 49154,
Neighbor TCP window size          = 32768,
Graceful Restart State            = None,
Advertised Restart Interval       = 0s,
Forwarding State during restart   = NotPreserved,
Activate IPv6 unicast             = enabled,
Configured IPv4 NextHop Address   = 0.0.0.0,
Configured IPv6 NextHop Address   = ::,
Neighbor Ipv6 unicast             = advertised
```

output definitions

Nbr address or **Neighbor address**	The IPv6 address for this BGP peer. Assign this address through the **ipv6 bgp neighbor** command.
As or **Neighbor autonomous system**	The autonomous system to which this peer belongs. A peer's AS number is assigned through the **ipv6 bgp neighbor remote-as** command.
Admin state or **Neighbor Admin state**	Indicates whether this peer has been enabled or disabled through the **ipv6 bgp neighbor status** command.
Oper state or **Neighbor Oper state**	The current BGP state for this peer. Possible states are **idle**, **connect**, **active**, **opensent**, **openconfirm**, and **established**.
BGP Id	The unique BGP identifier of the peer.
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.
Neighbor passive status	Indicates whether the local BGP speaker is "passive" (that is, waiting for this peer to initiate a session).
Neighbor name	The name assigned to this peer.
Neighbor local address	The interface assigned to this peer. This value is configured through the **ipv6 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.
Neighbor next hop self	Indicates whether this peer is using next hop processing. This value is configured through the **ipv6 bgp neighbor next-hop-self** command.
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 router supports route refresh all BGP peers are automatically enabled for this capability.
Neighbor Ipv4 unicast	Indicates whether this peer is multiprotocol IPv4 unicast capable.
Neighbor Ipv4 multicast	Indicates whether this peer is multiprotocol IPv4 multicast capable.
Neighbor type	Indicates whether this peer is internal or external to the AS.
Neighbor auto-restart	Indicates whether peer auto-restart is enabled or disabled.

output definitions (continued)

Neighbor route-reflector-client	Indicates whether this peer is a client to the local route reflector, if configured.
Neighbor confederation status	Indicates whether this peer is a member of a BGP confederation.
Neighbor remove private AS	Indicates whether the stripping of private AS numbers (64512 to 65535) from AS paths is enabled or disabled.
Neighbor default originate	Indicates whether peer default origination is enabled or disabled. When enabled, the local BGP speaker advertises the default route to the peer. This value is configured through the **ipv6 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 **ipv6 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 **ipv6 bgp neighbor update-source** command.
# of prefixes received	Displays the total number of prefixes received by this neighbor.
Neighbor MD5 key	When present, shows an encrypted version of the MD5 password. When not present, and MD5 password has not been configured.
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.
Graceful Restart State	Indicates the graceful restart state. This feature does not support IPv6 prefixes.
Advertised Restart Interval	Indicates the restart interval in seconds.
Forwarding State during restart	Indicates whether the peer has preserved the forwarding state during the graceful restart.
Activate IPv6 unicast	Indicates whether or not IPv6 unicast advertisements are enabled. Options include **enabled** or **disabled**.
Configured IPv4 NextHop Address	Specifies the IPv4 nexthop address. This is specified using the **ipv6 bgp neighbor ipv4-nexthop** command.
Configured IPv6 NextHop Address	Specifies the IPv6 nexthop address. This is specified using the **ipv6 bgp neighbor ipv6-nexthop** command.
Neighbor Ipv6 unicast	Indicates whether or not IPv6 unicast capability is advertised between the peers. Options include enabled or disabled.

Release History

Release 6.1.5; command was introduced.

Related Commands

ipv6 bgp neighbor	Creates or deletes a BGP peer relationship using IPv6 addresses
ipv6 bgp neighbor status	Enables or disables the BGP peer status.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeer6AS
   alaBgpPeer6Passive
   alaBgpPeer6Name
   alaBgpPeer6MultiHop
   alaBgpPeer6MaxPrefix
   alaBgpPeer6MaxPrefixWarnOnly
   alaBgpPeer6NextHopSelf
   alaBgpPeer6SoftReconfig
   alaBgpPeer6InSoftReset
   alaBgpPeer6Ipv4Unicast
   alaBgpPeer6Ipv4Multicast
   alaBgpPeer6RcvdRtRefreshMsgs
   alaBgpPeer6SentRtRefreshMsgs
   alaBgpPeer6RouteMapOut
   alaBgpPeer6RouteMapIn
   alaBgpPeer6LocalAddr
   alaBgpPeer6LastDownReason
   alaBgpPeer6LastDownTime
   alaBgpPeer6LastReadTime
   alaBgpPeer6RcvdNotifyMsgs
   alaBgpPeer6SentNotifyMsgs
   alaBgpPeer6LastSentNotifyReason
   alaBgpPeer6LastRecvNotifyReason
   alaBgpPeer6RcvdPrefixes
   alaBgpPeer6DownTransitions
   alaBgpPeer6Type
   alaBgpPeer6AutoReStart
   alaBgpPeer6ClientStatus
   alaBgpPeer6ConfedStatus
   alaBgpPeer6RemovePrivateAs
   alaBgpPeer6ClearCounter
   alaBgpPeer6TTL
   alaBgpPeer6AspathListOut
   alaBgpPeer6AspathListIn
   alaBgpPeer6PrefixListOut
   alaBgpPeer6PrefixListIn
   alaBgpPeer6CommunityListOut
   alaBgpPeer6CommunityListIn
   alaBgpPeer6Restart
   alaBgpPeer6DefaultOriginate
   alaBgpPeer6ReconfigureInBound
   alaBgpPeer6ReconfigureOutBound
   alaBgpPeer6MD5Key
   alaBgpPeer6MD5KeyEncrypt
   alaBgpPeer6RowStatus
   alaBgpPeer6UpTransitions
   alaBgpPeer6LastWriteTime
   alaBgpPeer6AdminStatus
```

```
alaBgpPeer6State
alaBgpPeer6LocalPort
alaBgpPeer6TcpWindowSize
alaBgpPeer6ActivateIpv6
```

show ipv6 bgp neighbors statistics

Displays the neighbor statistics of the configured IPv6 BGP peers.

show ipv6 bgp neighbors statistics [*ipv6_address***]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address.

Defaults

By default, the neighbor statistics for all the IPv6 BGP peers will be displayed.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the *ipv6_address* parameter to display the neighbor statistics of a specified IPv6 BGP peer.

Examples

```
-> show ipv6 bgp neighbors statistics
Legends: Nbr   = Neighbor
         As    = Autonomous System
         RMSGS = # of received messages
         SMSGS = # of sent messages
         RUPDS = # of Update messages received
         SUPDS = # of Update messages sent
         RNOFY = # of Notify messages received
         SNOFY = # of Notify messages sent
         RPFXS = # of prefixes received
         UPTNS = # of UP transitions
         DNTNS = # of DOWN transitions

Nbr address             As    RMSGS SMSGS RUPDS SUPDS RNOFY SNOFY RPFXS UPTNS DNTNS
------------------------+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----
2001:100:3:4::1         30    225   260   2     3     0     0     10    1     1
```

output definitions

Nbr address	The IPv6 address for this peer. This value is configured using the **ipv6 bgp neighbor** command.
As	The autonomous system to which this peer belongs. This value is configured using the **ipv6 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	Number of unique route prefixes received by this peer.
UPTNS	Number of times this peer has come up, operationally.
DNTNS	Number of times this peer has gone down, operationally.

```
-> show ipv6 bgp neighbors statistics 2001:100:3:4::1
Neighbor address                  = 2001:100:3:4::1,
# of UP transitions               = 1,
Time of last UP transition        = 01h:50m:36s,
# of DOWN transitions             = 1,
Time of last DOWN transition      = 00h:00m:00s,
Last DOWN reason                  = none,
# of msgs rcvd                    = 226,
# of Update msgs rcvd             = 2,
# of prefixes rcvd                = 10,
# of Route Refresh msgs rcvd      = 0,
# of Notification msgs rcvd       = 0,
Last rcvd Notification reason     = none [none]
Time last msg was rcvd            = 00h:00m:04s,
# of msgs sent                    = 260,
# of Update msgs sent             = 3,
# of Route Refresh msgs sent      = 0
# of Notification msgs sent       = 0,
Last sent Notification reason     = none [none]
Time last msg was sent            = 00h:00m:18s,
```

output definitions

Neighbor address	The IPv6 address for this peer. This value is configured using the **ipv6 bgp neighbor** command.
# **of UP transitions**	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 by 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**	Number of unique route prefixes received by this peer.
# of Route Refresh msgs rcvd	Number of route refresh requests this peer has received. Route refresh requests all routes learned be a peer.
# **of Notification msgs rcvd**	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 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	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	Number of route refresh requests this peer has sent. Route refresh requests request all routes learned be a peer.
# of Notification msgs sent	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 6.1.5; command was introduced.

Related Commands

show ipv6 bgp neighbors	Displays the configured IPv6 BGP peers.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeer6RcvdMsgs
   alaBgpPeer6SentMsgs
   alaBgpPeer6RcvdUpdMsgs
   alaBgpPeer6SentUpdMsgs
   alaBgpPeer6LastTransitionTime
   alaBgpPeer6LastUpTime
   alaBgpPeer6BgpId
   alaBgpPeer6LocalIntfName
   alaBgpPeer6RestartTime
   alaBgpPeer6RestartState
   alaBgpPeer6RestartFwdState
   alaBgpPeer6Ipv6Unicast
   alaBgpPeer6HoldTime
   alaBgpPeer6KeepAlive
   alaBgpPeer6ConnRetryInterval
   alaBgpPeer6HoldTimeConfigured
   alaBgpPeer6KeepAliveConfigured
   alaBgpPeer6Ipv4NextHop
   alaBgpPeer6Ipv6NextHop
```

show ipv6 bgp neighbors timers

Displays the timers for configured IPv6 BGP peers.

show ipv6 bgp neighbors timers [*ipv6_address***]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address.

Defaults

By default, the timer values for all the IPv6 BGP peers will be displayed.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the *ipv6_address* parameter to display the timer value for a specified IPv6 BGP peer.

Examples

```
-> show ipv6 bgp neighbors timers
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)
-----------------------------------+-----+-----+-------+-----+-----+------+-----
2001:100:3:4::1                     30    90    90      30    120   30     30
```

output definitions

Nbr address	The IPv6 address for this BGP peer. Assign this address using the **ipv6 bgp neighbor** command.
As	The autonomous system to which this peer belongs. A peer's AS number is assigned using the **ipv6 bgp neighbor remote-as** command.
Hold	The actual negotiated hold time value.
Hold (C)	The hold time value. This value is configured using the **ipv6 bgp neighbor timers** command.
RtAdv	The route advertisement interval, in seconds, for updates between external BGP peers.
Retry	The interval, in seconds, between retries by this peer to set up a connection via TCP with another peer. This value is configured using the **ipv6 bgp neighbor timers** command.

output definitions (continued)

Kalive	The actual negotiated value, 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 using the **ipv6 bgp neighbor timers** command.

Release History

Release 6.1.5; command was introduced.

Related Commands

show ip bgp statistics	Displays BGP global statistics.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeer6ConnRetryInterval
   alaBgpPeer6MinRouteAdvertisementInterval
   alaBgpPeer6HoldTime
```

show ipv6 bgp neighbors policy

Displays the incoming and outgoing prefix6 list policy identifiers configured for BGP IPv6 peer.

show ipv6 bgp neighbors policy *ipv6_address*

Syntax Definitions

ipv6_address	The 128-bit IPv6 address.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

This command displays all of the configured policies for the router, or the polices configured for a specific BGP IPv6 peer.

Examples

```
-> show ipv6 bgp neighbors policy
Neighbor address  =  2001::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
  Neighbor output prefix6-list name   = <none>,
  Neighbor input prefix6-list name    = <none>
```

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 in-prefix6list** 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.

output definitions (continued)

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.
Neighbor output prefix6-list name	The outbound prefix6-list policy for the peer. This can be assigned by using the **ipv6 bgp neighbor out-prefix6list** command.
Neighbor input prefix6-list name	The inbound prefix6-list policy for the peer. This can be assigned by using the **ipv6 bgp neighbor in-prefix6list** command.

Release History

Release 6.3.4; command was introduced.

Related Commands

show ipv6 bgp neighbors	Displays configured IPv6 BGP peers

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Prefix6ListIn
   alaBgpPeer6Prefix6ListOut
```

31 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.

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** **ip slb reset statistics** **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 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 the administrative status for 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	**disable**

Platforms Supported

OmniSwitch 6400, 6850E, 9000E

Usage Guidelines

Disabling the administrative status for the SLB feature does not delete the SLB configuration from the switch. The next time the feature is enabled, the existing configuration will go active.

Examples

```
-> ip slb admin enable
-> ip slb admin disable
```

Release History

Release 6.1; 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 reset statistics

Resets SLB statistics for all clusters configured on the switch.

ip slb reset statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 9000E

Usage Guidelines

Note that the **qos apply** command resets both QoS statistics *and* SLB cluster statistics. The **ip slb reset statistics** command only resets SLB statistics.

Examples

```
-> ip slb reset statistics
```

Release History

Release 6.1.5; 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.

MIB Objects

```
slbFeature
   slbResetStatistics
```

ip slb cluster

Configures a Server Load Balancing (SLB) cluster on a switch.

ip slb cluster *name* **{vip** *ip_address* **| condition** *string***} [l3 | l2]**

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.
string	The name of an existing QoS policy condition that identifies the Server Load Balancing cluster.
l3	Specifies Layer 3 Server Load Balancing mode. The source and destination MAC and TTL of each packet is modified before the packet is bridged or routed to the server.
l2	Specifies Layer 2 Server Load Balancing mode. Packets are not modified before they are bridged to the server. This parameter is only available when using the **condition** parameter.

Defaults

parameter	default
l3 | l2	**l3**

Platforms Supported

OmniSwitch 6400, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to delete a Server Load Balancing cluster.
- The VIP address of the SLB cluster *must* be an address that is in the same subnet as the servers.
- Specifying the **l3** parameter when configuring a VIP cluster is not required. VIP clusters only use the Layer-3 mode to route traffic to the servers. Layer-2 mode is not supported with this type of cluster.
- The QoS policy condition must exist before it is assigned to an SLB cluster. Use the **policy condition** command to create the QoS policy condition. See the “QoS Policy Commands” chapter for more information.
- SLB clusters are not active if the Server Load Balancing feature is disabled for the switch. Use the **ip slb admin** command to enable this feature. Note, however, that it is possible to configure clusters and add or remove servers from a cluster even when SLB is disabled for the switch.

- A maximum of 16 Server Load Balancing clusters may be configured on an OmniSwitch 6850E switch. Each cluster may contain up to 16 servers for a total of 256 servers per switch.

Examples

```
-> ip slb cluster corporate_servers vip 1.2.3.4
-> ip slb cluster "mail servers" vip 1.2.3.6
-> ip slb cluster cluster_1 condition intranet_cond l2
-> ip slb cluster cluster_2 condition slb_cond l3
-> no ip slb cluster hr_servers
```

Release History

Release 6.1; command was introduced.
Release 6.1.3; **condition**, **l2**, **l3**, and **arp** parameters added.
Release 6.1.5; l2 and l3 parameters not used with the vip parameter.

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
   slbClusterName
   slbClusterVIP
   slbClusterRowStatus
   slbClusterPackets
   slbClusterCondition
   slbClusterType
```

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 an existing Server Load Balancing cluster.
enable	Administratively enables a Server Load Balancing cluster on a switch.
disable	Administratively disables a Server Load Balancing cluster on a switch.

Defaults

By default, a cluster is administratively enabled when the cluster is created.

Platforms Supported

OmniSwitch 6400, 6850E, 9000E

Usage Guidelines

The SLB cluster name specified with this command must already exist in the switch configuration.

Examples

```
-> ip slb cluster hr_servers admin status enable
-> ip slb cluster "mail servers" admin status disable
```

Release History

Release 6.1; 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	Configures Server Load Balancing clusters.
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 6400, 6850E, 9000E

Usage Guidelines

If you do not set the ping period to zero, then the ping period *must* be greater than or equal to the ping timeout value divided by 1000. Use the **ip slb cluster ping timeout** command to modify the ping timeout value.

Examples

```
-> ip slb cluster hr_servers ping period 120
-> ip slb cluster "mail servers" ping period 0
```

Release History

Release 6.1; 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

Configures the ping timeout value 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 6400, 6850E, 9000E

Usage Guidelines

Use the **ip slb cluster ping period** command to modify the ping period value.

Examples

```
-> ip slb cluster "mail servers" ping timeout 1000
-> ip slb cluster hr_servers ping timeout 6000
```

Release History

Release 6.1; 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

Configures 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 6400, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> ip slb cluster "mail servers" ping retries 5
-> ip slb cluster hr_servers ping retries 10
```

Release History

Release 6.1; 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 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 6400, 6850E, 9000E

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 6.1; 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 of a physical server in an SLB cluster.

ip slb server ip *ip_address* **cluster** *cluster_name* **[admin status {enable | disable}] [weight** *weight***]**

no ip slb server ip *ip_address* **cluster** *cluster_name*

Syntax Definitions

ip_address	The IP address of the physical server.
cluster_name	The name of an existing Server Load Balancing cluster.
enable	Enables a server.
disable	Disables a server.
weight	Specifies the weight of the server. The valid range of weight value is 0 - 32

Defaults

parameter	default
enable | disable	**enable**
weight	**1**

Platforms Supported

OmniSwitch 6400, 6850E, 9000E

Usage Guidelines

- Use the **no** form of the command to remove a physical server from a Server Load Balancing cluster.
- Up to 16 clusters per switch are allowed. Each cluster may contain up to 16 servers to provide a maximum of 256 physical servers per switch.
- Use the weight parameter to assign the server preference value. Each server or server cluster can be assigned a weight to set their preference value for distribution of incoming network traffic.The weights assigned are relative. For example, if Servers A and B have respective weights of 10 and 20 within a cluster, Server A would get half the traffic of Server B.
- Assigning a weight of 0 (zero) to a server will prevent this server from being assigned any new connections.This server will be a backup server.
- A higher weight value indicates that the server can accept more network traffic.

Examples

```
-> ip slb cluster corporate_servers vip 15.2.2.50
-> ip slb server ip 15.2.2.2 cluster corporate_servers weight 7
-> no ip slb server ip 15.2.2.3 cluster corporate_servers
```

Release History

Release 6.1; command was introduced.
Release 6.4.2; **weight** parameter added.

Related Commands

ip slb admin	Enables or disables Server Load Balancing on a switch.
ip slb cluster	Configures Server Load Balancing clusters.
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 statistics and configuration information for a single physical server in a Server Load Balancing cluster.

MIB Objects

```
slbServerTable
   slbServerAdminStatus
   slbServerAdminWeight
   slbServerClusterName
   slbServerRowStatus
   slbServerWeight
```

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 6400, 6850E, 9000E

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 6.1; 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 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 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 6400, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to delete an SLB probe.
- It is possible to configure up to 20 probes per switch.

Examples

```
-> ip slb probe mail_server_probe smtp
-> no ip slb probe mail_server_probe
```

Release History

Release 6.1; command was introduced.

Related Commands

show ip slb probes	Displays the configuration of SLB probes.

MIB Objects

```
slbProbeTable
   slbProbeName
   slbProbeMethod
```

ip slb probe timeout

Configures the amount of time 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 1–3600000.

Defaults

parameter	default
seconds	3000

Platforms Supported

OmniSwitch 6400, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> ip slb probe mail_server smtp timeout 12000
```

Release History

Release 6.1; command was introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
show ip slb probes	Displays the configuration of SLB probes.

MIB Objects

```
slbProbeTable
   slbProbeName
   slbProbeMethod
   slbProbeTimeout
```

ip slb probe period

Configures the length of time between each SLB probe to check the health of the 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 length of time for the SLB probe period (0–3600 seconds).

Defaults

parameter	default
seconds	60

Platforms Supported

OmniSwitch 6400, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> ip slb probe web_server http period 120
```

Release History

Release 6.1; command was introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
show ip slb probes	Displays the configuration of SLB probes.

MIB Objects

```
slbProbeTable
   slbProbeName
   slbProbeMethod
   slbProbePeriod
```

ip slb probe port

Configures the TCP/UDP port on which the Server Load Balancing (SLB) probe is sent.

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 (0–65535).

Defaults

parameter	default
port_number	0

Platforms Supported

OmniSwitch 6400, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> ip slb probe mis_server udp port 200
```

Release History

Release 6.1; command was introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
show ip slb probes	Displays 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 that are performed 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 (0–255).

Defaults

parameter	default
retries	3

Platforms Supported

OmniSwitch 6400, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> ip slb probe mail_server smtp retries 5
```

Release History

Release 6.1; command was introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
show ip slb probes	Displays the configuration of SLB probes.

MIB Objects

```
slbProbeTable
   slbProbeName
   slbProbeMethod
   slbProbeRetries
```

ip slb probe username

Configures a user name that is 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 6400, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> ip slb probe web_server http username subnet1
```

Release History

Release 6.1; command was introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
show ip slb probes	Displays the configuration of SLB probes.

MIB Objects

```
slbProbeTable
   slbProbeName
   slbProbeMethod
   slbProbeHttpUsername
```

ip slb probe password

Configures a password that is 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 6400, 6850E, 9000E

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 6.1; command was introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
show ip slb probes	Displays the configuration of SLB probes.

MIB Objects

```
slbProbeTable
   slbProbeName
   slbProbeMethod
   slbProbeHttpPassword
```

ip slb probe url

Configures a URL that is 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 6400, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
->ip slb probe web_server http url pub/index.html
```

Release History

Release 6.1; command was introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
show ip slb probes	Displays 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 6400, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> ip slb probe web_server http status 404
```

Release History

Release 6.1; command was introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
show ip slb probes	Displays the configuration of SLB probes.

MIB Objects

```
slbProbeTable
   slbProbeName
   slbProbeMethod
   slbProbePeriod
   slbProbeHttpStatus
```

ip slb probe send

Configures an ASCII string that is sent to a server to invoke a server response and verify the health of the server.

ip slb probe *probe_name* **{tcp | udp} send** *send_string*

Syntax Definitions

probe_name	Specifies the name of the Server Load Balancing (SLB) 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 6400, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> ip slb probe web_server tcp send test
```

Release History

Release 6.1; command was introduced.
Release 6.1.3; **http** and **https** parameters removed.

Related Commands

ip slb probe	Configures and deletes SLB probes.
show ip slb probes	Displays 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_string	Specifies the ASCII string used to compare a response from a server.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> ip slb probe web_server http expect test
```

Release History

Release 6.1; command was introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
show ip slb probes	Displays 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 6400, 6850E, 9000E

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 (**Enabled** or **Disabled**).
Operational status	The current operational status of Server Load Balancing (SLB) on this switch, which is either **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 16 SLB clusters per switch is allowed.

Release History

Release 6.1; 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

Displays the status and basic configuration for all Server Load Balancing (SLB) clusters on a switch. This command also displays traffic statistics for QoS policy condition clusters.

show ip slb clusters [statistics]

Syntax Definitions

statistics	Displays SLB statistics for QoS policy condition clusters.

Defaults

By default, the status and basic configuration for all clusters is displayed; statistics are not shown.

Platforms Supported

OmniSwitch 6400, 6850E, 9000E

Usage Guidelines

Use the **statistics** parameter to display the total number of packets that were passed to clusters because they met the QoS condition criteria configured for that cluster. The polling interval used to obtain such statistics is every 15 minutes. See the second example below.

Examples

```
-> show ip slb clusters
                                  Admin    Operational          #     %
Cluster Name     VIP/COND         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 the SLB cluster.
VIP/COND	The virtual IP (VIP) address or the policy condition name for the SLB cluster.
Admin Status	The administrative status of the SLB cluster (**Enabled** or **Disabled**).
Operational Status	The operational status of the SLB cluster; **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 the SLB cluster. It is possible to configure up 16 servers per cluster and up to 16 clusters per switch. This allows a maximum of 256 physical servers per switch.
% Avail	The percentage of flows successfully routed to the SLB cluster.

```
-> show ip slb clusters statistics
                         Admin    Operational
Cluster Name             Status   Status                Count
-----------------------+--------+--------------------+--------
Cluster1                 Enabled  In Service            4 Servers
Cluster2                 Enabled  In Service            4 Servers
Cluster3                 Enabled  In Service            4 Servers
Cluster4                 Enabled  In Service            2 Servers
```

output definitions

Cluster Name	The name of the SLB cluster. This field also contains the administrative and operational status for the cluster and either the VIP address or QoS policy condition value that identifies the cluster.
Count	The total number of physical servers that belong to the cluster, and the total number of packets serviced by the cluster.

Release History

Release 6.1; command was introduced.
Release 6.1.5; **statistics** parameter added; **Count** field added.

Related Commands

ip slb reset statistics	Resets SLB statistics for all clusters.
show ip slb cluster	Displays detailed status and configuration information for a single SLB cluster.
show ip slb servers	Displays the status of all physical servers belonging to each SLB cluster on a switch.
show ip slb cluster server	Displays detailed status and configuration information for a single physical server in an SLB cluster.

MIB Objects

```
slbClusterTable
   slbClusterName
   slbClusterVIP
   slbClusterCondition
   slbClusterAdminStatus
   slbClusterOperStatus
   slbClusterNumberOfServers
   slbClusterNewFlows
slbStatsTable
   slbStatsClusterName
   slbStatsIndex
   slbStatsCounter
slbStatsQualTable
   slbStatsQualType
   slbStatsQualData
```

show ip slb cluster

Displays detailed statistics and configuration information for a single Server Load Balancing (SLB) cluster. This command also displays traffic statistics for single QoS policy condition cluster.

show ip slb cluster *name* **[statistics]**

Syntax Definitions

name	Specifies the name of the SLB cluster.
statistics	Displays SLB statistics for the specified cluster.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 9000E

Usage Guidelines

Use the **statistics** parameter to display the total number of packets that were passed to the cluster because they met the QoS condition criteria configured for that cluster. The polling interval used to obtain such statistics is every 15 minutes. See the second example below:

Examples

```
-> show ip slb cluster Intranet
Cluster Intranet
  VIP                           : 128.241.130.205,
  Type                         : L3
  Admin status                  : Enabled,
  Operational status            : In Service,
  Ping period (seconds)         : 60,
  Ping timeout (milliseconds)   : 3000,
  Ping retries                  : 3,
  Probe                        : None,
  Number of packets             : 45768,
  Number of servers             : 2
    Server 128.241.130.4
      Admin status = Enabled, Operational Status = In Service,
      Availability (%) = 98
    Server 128.241.130.5
      Admin status = Enabled, Operational Status = Discovery,
      Availability (%) = 0
```

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.
Type	The classifier for the hypothetical packet, which can be **L2** or **L3**.

output definitions (continued)

Admin status	The current administrative status of this Server Load Balancing (SLB) cluster (**Enabled** or **Disabled**).
Operational status	The current operational status of this Server Load Balancing (SLB) cluster, which is **In Service** (i.e., at least one physical server is operational in the cluster) or **Out of Service**.
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**.
Probe	The probe configured for this cluster.
Number of packets	The number of packets 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 (**Enabled** or **Disabled)**.
Operational Status	The operational state of this server. The possible states are described as follows: • **Disabled** (this server is 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 used for SLB cluster client connections). • **Discovery** (the SLB cluster is pinging this physical server). • **Retrying** (the SLB cluster is making another attempt to bring up this server).
Availability (%)	The percentage of time that this physical server has been available for processing client requests. In other words, 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.

```
-> show ip slb cluster Cluster6 statistics
Cluster Name                                              Count
----------------------------------------------------------+--------
Cluster6                Enabled  In Service              2 Servers
      Src IP 202.202.1.0/255.255.255.0                    6527831
      Src Port 2/49
```

output definitions

Cluster Name	The name of the SLB cluster. This field also contains the administrative and operational status for the cluster and either the VIP address or QoS policy condition value that identifies the cluster.
Count	The total number of physical servers that belong to the cluster, and the total number of packets serviced by the cluster.

Release History

Release 6.1; command was introduced.
Release 6.1.3; **Type** field added; **Routed flows success ratio (%)** field removed.
Release 6.1.5; **statistics** parameter added; **Count** field added.

Related Commands

ip slb reset statistics	Resets SLB statistics for all clusters.
show ip slb clusters	Displays detailed status and configuration information for all Server Load Balancing clusters on a switch.
show ip slb servers	Displays the status of all physical servers belonging to 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
   slbClusterRowStatus
   slbClusterPackets
   slbClusterCondition
   slbClusterType
slbServerTable
   slbServerClusterName
   slbServerIpAddress
   slbServerAdminStatus
   slbServerOperStatus
slbStatsTable
   slbStatsClusterName
   slbStatsIndex
   slbStatsCounter
slbStatsQualTable
   slbStatsQualType
   slbStatsQualData
```

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 *cluster_name* **server** *ip_address*

Syntax Definitions

cluster_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 6400, 6850E, 9000E

Usage Guidelines

Specifying a value for the *cluster_name* and *ip_address* parameters is required.

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                            : 3,
      MAC addr                                : 00:00:1f:40:53:6a,
      Slot number                             : 1,
      Port number                             : 4,
      Admin status                            : Enabled,
      Oper status                             : In Service,
      Probe                                   : None,
      Availability time (%)                   : 95,
      Ping failures                           : 0,
      Last ping round trip time (milliseconds) : 20,
      Probe status                            : OK,
```

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.

output definitions (continued)

Admin weight	The weight assigned to this physical server.. A weight of 0 (zero) indicates that no new connections will be assigned to the server. A higher weight value indicates that the server can accept more network traffic.
MAC addr	The MAC address of this physical server.
Slot number	The slot number of the network interface (NI) module to which this physical server is attached.
Port number	The port number to which this physical server is attached.
Admin status	The current administrative status of this physical server (**Enabled** or **Disabled**).
Oper status	The operational state of this server. The possible states are described as follows: • **Disabled** (this server is 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 used for SLB cluster client connections). • **Discovery** (the SLB cluster is pinging this physical server). • **Retrying** (the SLB cluster is making another attempt to bring up this 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 words, 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.
Probe status	The status of the probe configured for this server.

Release History

Release 6.1; command was introduced.
Release 6.4.2; **Admin weight** 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	Displays detailed status and configuration information for a single Server Load Balancing cluster.

MIB Objects

```
slbClusterTable
   slbClusterVIP
slbServerTable
   slbServerClusterName
   slbServerIpAddress
   slbServerAdminStatus
   slbServerAdminWeight
   slbServerOperStatus
   slbServerMacAddress
   slbServerSlotNumber
   slbServerPortNumber
   slbServerUpTime
   slbServerProbeName
   slbServerLastRTT
   slbServerPingFails
   slbServerProbeStatus
   slbServerWeight
```

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 6400, 6850E, 9000E

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 to which this physical server belongs.
Admin Status	The current administrative status of this physical server (**Enabled** or **Disabled**).

output definitions (continued)

Operational Status	The operational state of this server. The possible states are described as follows: • **Disabled** (this server is 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 used for SLB cluster client connections). • **Discovery** (the SLB cluster is pinging this physical server). • **Retrying** (the SLB cluster is making another attempt to bring up this server).
% Avail	The percentage of time that this physical server has been available for processing client requests. In other words, 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 6.1; 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

Displays 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 6400, 6850E, 9000E

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.

The name of a probe that is not an HTTP/HTTPS probe is specified:

```
-> show ip slb probes mail_server
Probe mail_server
  Type                          : SMTP,
  Period (seconds)              : 60,
  Timeout (milliseconds)        : 3000,
  Retries                       : 3,
  Port                          : 0,
```

The name of an HTTP/HTTPS probe 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 on which the probe is sent.
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 6.1; 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
```

32 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-Lucent's IPMS software is compatible with the following RFCs:

RFC 1112 — Host Extensions for IP Multicasting
RFC 2236 — Internet Group Management Protocol, Version 2
RFC 2933 — Internet Group Management Protocol MIB
RFC 3376 — Internet Group Management Protocol, Version 3

Alcatel-Lucent's IPv6MS software is compatible with the following RFCs:

RFC 2710 — Multicast Listener Discovery for IPv6
RFC 3019 — IPv6 MIB for Multicast Listener Discovery Protocol
RFC 3810 — Multicast Listener Discovery Version 2 for IPv6

MIB information for the IPMS commands is as follows:

Filename: AlcatelIND1Igmp.mib
Module: ALCATEL-IGMP-IND1-MIB

MIB information for the IPv6MS commands is as follows:

Filename: AlcatelIND1Mld.mib
Module: ALCATEL-MLD-IND1-MIB

The following table summarizes the available IP and IPv6 multicast commands:

ip multicast status
ip multicast router-timeout
ip multicast querier-forwarding
ip multicast version
ip multicast max-group
ip multicast vlan max-group
ip multicast port max-group
ip multicast static-neighbor
ip multicast static-querier
ip multicast static-group
ip multicast query-interval
ip multicast last-member-query-interval
ip multicast query-response-interval
ip multicast unsolicited-report-interval
ip multicast router-timeout
ip multicast source-timeout
ip multicast querying
ip multicast robustness
ip multicast spoofing
ip multicast zapping
ip multicast proxying
ip multicast helper-address
ip multicast helper-address
ipv6 multicast querier-forwarding
ipv6 multicast version
ipv6 multicast max-group
ipv6 multicast vlan max-group
ipv6 multicast port max-group
ipv6 multicast static-neighbor
ipv6 multicast static-querier
ipv6 multicast static-group
ipv6 multicast query-interval
ipv6 multicast last-member-query-interval
ipv6 multicast query-response-interval
ipv6 multicast unsolicited-report-interval
ipv6 multicast router-timeout
ipv6 multicast source-timeout
ipv6 multicast querying
ipv6 multicast robustness
ipv6 multicast spoofing
ipv6 multicast zapping
ipv6 multicast proxying
ip multicast static-ssm-map
show ip multicast static-ssm-map
show ip multicast
show ip multicast port
show ip multicast forward
show ip multicast neighbor
show ip multicast querier
show ip multicast group
show ip multicast source
show ip multicast tunnel
show ipv6 multicast
show ipv6 multicast port
show ipv6 multicast forward
show ipv6 multicast neighbor
show ipv6 multicast querier
show ipv6 multicast group
show ipv6 multicast source
show ipv6 multicast tunnel

ip multicast status

Enables or disables IP Multicast Switching and Routing on the specified VLAN, or on the system if no VLAN is specified.

ip multicast [vlan *vid***] status [{enable | disable}]**

Syntax Definitions

vid	VLAN on which to apply the configuration.
enable	Enable IP Multicast Switching and Routing.
disable	Disable IP Multicast Switching and Routing.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- If an IP Multicast Routing protocol is already running on the system, the **ip multicast status** command will override the existing configuration and always enable IP Multicast Switching and Routing.
- If IP Multicast Switching and Routing is already enabled on the system, then the VLAN configuration will override the system's configuration.
- You can also restore the IP Multicast Switching and Routing to its default (that is, disabled) status on the system if no VLAN is specified, by using only **ip multicast status** (for example, ip multicast status).
- You can also restore the IP Multicast Switching and Routing to its default (that is, disabled) status on the specified VLAN, by using only **ip multicast vlan** *vid* **status** (for example, ip multicast vlan 2 status).

Examples

```
-> ip multicast status enable
-> ip multicast status disable
-> ip multicast status
-> ip multicast vlan 2 status enable
-> ip multicast vlan 2 status disable
-> ip multicast vlan 2 status
```

Release History

Release 6.1.1; command was introduced.

ip multicast flood-unknown

Enables or disables the flooding of new multicast packets until the multicast group membership table is updated.

ip multicast flood-unknown {enable | disable}

Syntax Definitions

enable	Enable the flooding of multicast packets until membership table updated.
disable	Disable the flooding of multicast packets.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- When flood-unknown is enabled and IP multicast switching is enabled, multicast packets are flooded on the VLAN until the multicast group membership table is updated. They are then forwarded based on the multicast group membership table.
- When flood-unknown is enabled and IP multicast switching is disabled, all multicast traffic will be flooded on the VLAN.
- When flood-unknown is disabled and IP multicast switching is enabled, multicast packets are not flooded on the VLAN but will be forwarded once the multicast group membership table is updated.
- If IP multicast switching is disabled and flood-unknown is disabled, all multicast packets are flooded on the VLAN.

Examples

```
-> ip multicast flood-unknown enable
-> ip multicast flood-unknown disable
```

Release History

Release 6.3.4; command was introduced.

Related Commands

ip multicast status	Enables or disables IP Multicast Switching and Routing on the specified VLAN, or on the system if no VLAN is specified.
show ip multicast	Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaIgmp
   alaIgmpStatus
alaIgmpVlan
   alaIgmpVlanStatus
```

ip multicast querier-forwarding

Enables or disables IGMP querier forwarding on the specified VLAN or on the system if no VLAN is specified.

ip multicast [vlan *vid***] querier-forwarding [{enable | disable}]**

no ip multicast [vlan *vid***] querier-forwarding**

Syntax Definitions

vid	The VLAN on which configuration is applied.
enable	Enable IGMP querier forwarding.
disable	Disable IGMP querier forwarding.

Defaults

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

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to remove an IGMP querier forwarding entry on the specified VLAN or on the system and return to its default behavior.
- If the IGMP querier forwarding is already enabled on the system, then the VLAN configuration will override the system's configuration.
- IGMP querier forwarding refers to promoting detected IGMP queriers to receive all IP multicast data traffic.

Examples

```
-> ip multicast querier-forwarding enable
-> ip multicast querier-forwarding disable
-> ip multicast querier-forwarding
-> ip multicast vlan 2 querier-forwarding enable
-> ip multicast vlan 2 querier-forwarding disable
-> ip multicast vlan 2 querier-forwarding
-> no ip multicast vlan 2 querier-forwarding
```

Release History

Release 6.3.1; command was introduced.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaIgmp
   alaIgmpQuerierForwarding
alaIgmpVlan
   alaIgmpVlanQuerierForwarding
```

ip multicast version

Sets the default version of the IGMP protocol on the specified VLAN or on the system if no VLAN is specified.

ip multicast [vlan *vid***] version [***version***]**

Syntax Definitions

vid	VLAN on which to apply the configuration.
version	Default IGMP protocol version to run. Valid range is 1 to 3.

Defaults

parameter	default
version	2

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- IP Multicast Switching and Routing must be enabled to set the default IGMP protocol version on the system and/or the specified VLANs.
- If the default IGMP protocol version is already configured on the system, then the VLAN configuration will override the system's configuration.
- Due to protocol inter-operation requirements, this command specifies only a default version of the IGMP protocol to run.
- To restore the IGMP multicast version to the default (that is, 2) version on the system if no VLAN is specified, use **ip multicast version** followed by the value 0 (for example, ip multicast version 0) or use only **ip multicast version** (for example, ip multicast version).
- To restore the IGMP multicast version to the default (that is, 2) version on the specified VLAN, use **ip multicast vlan** *vid* **version**, followed by the value 0 (for example, ip multicast vlan 2 version 0) or use only **ip multicast vlan** *vid* **version** (for example, ip multicast vlan 2 version).

Examples

```
-> ip multicast version 3
-> ip multicast version 0
-> ip multicast version
-> ip multicast vlan 2 version 3
-> ip multicast vlan 2 version 0
-> ip multicast vlan 2 version
```

Release History

Release 6.1.1; command was introduced.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaIgmp
   alaIgmpVersion
alaIgmpVlan
   alaIgmpVlanVersion
```

ip multicast max-group

Configures the global maximum group limit that can be learned per port/VLAN instance.The limit is applied to each port/VLAN instance and an action is taken when it exceeds the limit.

ip multicast max-group [*num***] [action {none | drop | replace}]**

Syntax Definitions

num	Specifies the maximum IGMP group count. Valid range is 0 to 4294967295.
none	Disables the maximum group limit configuration
drop	Drops the incoming membership request.
replace	Replaces an existing membership with the incoming membership request.

Defaults

By default, the max-group limit is set to zero.

parameter	defaults
action	**none**

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Configuring a max-group value will have no affect on existing group memberships until the memberships are refreshed on the port/VLAN instance.
- The configuration is allowed even when the ip multicast status is disabled.
- If the num and action parameters are not specified, then the limit is removed.
- The max-group configuration on a specific VLAN or port will override the global configuration.
- IGMP zapping must be enabled when the max-group limit is enabled and the action is dropped.

Examples

```
-> ip multicast max-group 10 action drop
-> ip multicast max-group 20 action replace
-> ip multicast max-group
```

Release History

Release 6.3.4; command was introduced.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaIgmpMaxGroupLimit
   alaIgmpMaxGroupExceedAction
```

ip multicast vlan max-group

Configures the maximum group limit learned per port on a VLAN. The limit is applied to each port that is a member of the given VLAN.

ip multicast vlan *vid* **max-group [***num***] [action {none | drop | replace}]**

Syntax Definitions

vid	VLAN on which to apply the configuration.
num	The maximum IGMP group count. Valid range is 0 to 4294967295.
none	Disables the maximum group limit configuration.
drop	Drops the incoming membership request.
replace	Replaces an existing membership with the incoming membership request.

Defaults

By default, the max-group limit is set to zero.

parameter	defaults
Action	**none**

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Configuring a max-group value will have no affect on existing group memberships until the memberships are refreshed on the port/VLAN instance
- The configuration is allowed even when the ip multicast status is disabled.
- If the num and action parameters are not specified, then the limit is removed.
- The max-group configuration on a VLAN will override the global configuration.
- IGMP zapping must be enabled when the max-group limit is enabled and the action is dropped.

Examples

```
-> ip multicast vlan 10 max-group 10 action drop
-> ip multicast vlan 10 max-group
```

Release History

Release 6.3.4; command was introduced.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaIgmpVlanTable
   alaIgmpVlanMaxGroupLimit
   alaIgmpVlanMaxGroupExceedAction
```

ip multicast port max-group

Configures the maximum group limit learned per port. The limit is applicable on the given port for all VLAN instances of the port.

ip multicast port *slot* | *port* **max-group [***num***] [action {none | drop | replace}]**

Syntax Definitions

slot	*port*	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
num	The maximum IGMP group count. Valid range is 0 to 4294967295.
none	Disables the maximum group limit configuration.
drop	Drops the incoming membership request.
replace	Replaces an existing membership with the incoming membership request.

Defaults

By default, the max-group limit is set to zero.

parameter	defaults
Action	**none**

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Configuring a max-group value will have no affect on existing group memberships until the memberships are refreshed on the port/VLAN instance
- The configuration is allowed even when the ip multicast status is disabled.
- If the num and action parameters are not specified, then the limit is removed.
- The max-group configuration on a port will override the VLAN or global configuration.
- IGMP zapping must be enabled when the max-group limit is enabled and the action is dropped.

Examples

```
-> ip multicast port 1/1 max-group 10 action drop
-> ip multicast port 6/14 max-group 20 action replace
```

Release History

Release 6.3.4; command was introduced.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaIgmpPortTable
   alaIgmpPortMaxGroupLimit
   alaIgmpPortMaxGroupExceedAction
```

ip multicast static-neighbor

Creates a static IGMP neighbor entry on a specified port on a specified VLAN.

ip multicast static-neighbor vlan *vid* **port** *slot/port*

no ip multicast static-neighbor vlan *vid* **port** *slot/port*

Syntax Definitions

vid	VLAN to include as a static IGMP neighbor.
slot/port	The slot/port number you want to configure as a static IGMP neighbor.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to remove an IGMP static neighbor entry on a specified port on a specified VLAN.
- The **ip multicast static-neighbor** command allows you to create an IGMP static neighbor entry on a specified port on a specified VLAN. This, in turn, enables that network segment to receive all the IGMP traffic.
- You can also create an IGMP static neighbor entry on a link aggregate port by entering **ip multicast static-neighbor vlan** *vid* **port**, followed by the link aggregation group number (for example, ip multicast static-neighbor vlan 2 port 7).

Examples

```
-> ip multicast static-neighbor vlan 4 port 1/1
-> no ip multicast static-neighbor vlan 4 port 1/1
-> ip multicast static-neighbor vlan 4 port 7
-> no ip multicast static-neighbor vlan 4 port 7
```

Release History

Release 6.1.1; command was introduced.

Related Commands

show ip multicast neighbor	Displays the IGMP neighbor table entries of IP Multicast Switching and Routing.

MIB Objects

```
alaIgmpStaticNeighborTable
   alaIgmpStaticNeighborVlan
   alaIgmpStaticNeighborIfIndex
   alaIgmpStaticNeighborRowStatus
```

ip multicast static-querier

Creates a static IGMP querier entry on a specified port on a specified VLAN.

ip multicast static-querier vlan *vid* **port** *slot/port*

no ip multicast static-querier vlan *vid* **port** *slot/port*

Syntax Definitions

vid	VLAN to include as a static IGMP querier.
slot/port	The slot/port number you want to configure as a static IGMP querier.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to remove an IGMP static querier entry on a specified port on a specified VLAN.
- The **ip multicast static-querier** command allows you to create an IGMP static querier entry on a specified port on a specified VLAN. This, in-turn, enables that network segment to receive all the IGMP traffic.
- You can also create an IGMP static querier entry on a link aggregate port by entering **ip multicast static-querier vlan** *vid* **port**, followed by the link aggregation group number (for example, ip multicast static-querier vlan 2 port 7).

Examples

```
-> ip multicast static-querier vlan 4 port 1/1
-> no ip multicast static-querier vlan 4 port 1/1
-> ip multicast static-querier vlan 4 port 7
-> no ip multicast static-querier vlan 4 port 7
```

Release History

Release 6.1.1; command was introduced.

Related Commands

show ip multicast querier	Displays the IGMP querier table entries of IP Multicast Switching and Routing.

MIB Objects

```
alaIgmpStaticQuerierTable
   alaIgmpStaticQuerierVlan
   alaIgmpStaticQuerierIfIndex
   alaIgmpStaticQuerierRowStatus
```

ip multicast static-group

Creates a static IGMP group entry on a specified port, VLAN and receiver VLAN.

ip multicast static-group *ip_address* **vlan** *vid* **port** *slot/port* **receiver-vlan** *num*

no ip multicast static-group *ip_address* **vlan** *vid* **port** *slot/port* **receiver-vlan** *num*

Syntax Definitions

ip_address	The IP address of the multicast group.
vid	VLAN to include as a static IGMP group.
slot/port	The slot/port number you want to configure as a static IGMP group.
receiver-vlan	Receiver VLAN ID.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to remove an IGMP static group entry on a specified port on a specified VLAN.
- The **ip multicast static-group** command allows you to create an IGMP static group entry on a specified port on a specified VLAN. This, in-turn, enables that network segment to receive IGMP traffic addressed to the specified IP multicast group address.
- You can also create an IGMP static group entry on a link aggregate port by entering **ip multicast static-group** *ip_address* **vlan** *vid* **port**, followed by the link aggregation group number (for example, ip multicast static-group 11.0.0.1 vlan 2 port 7).
- The RVLAN and receiver port should be associated before creating a static group. Use the command **vlan ipmvlan** *ipmvlan-id* **receiver-port port** *slot/port***[***-port2***]** **receiver-vlan** *num* for creating the association between RVLAN and receiver port.

Examples

```
-> ip multicast static-group 229.10.10.10 vlan 4 port 1/1
-> no ip multicast static-group 229.10.10.10 vlan 4 port 1/1
-> ip multicast static-group 225.11.11.11 vlan 4 port 7
-> no ip multicast static-group 225.11.11.11 vlan 4 port 7
-> ip multicast static-group 224.1.1.1 vlan 10 port 1/1 receiver-vlan 20
-> no ip multicast static-group 224.1.1.1 vlan 10 port 1/1 receiver-vlan 20
```

Release History

Release 6.1.1; command was introduced.
Release 6.4.5; **receiver-vlan** parameter added.

Related Commands

show ip multicast group	Displays the IGMP group membership table entries of IP Multicast Switching and Routing for the specified IP multicast group address or all entries if no IP multicast group address is specified.

MIB Objects

```
alaIgmpStaticMemberTable
   alaIgmpStaticMemberVlan
   alaIgmpStaticMemberIfIndex
   alaIgmpStaticMemberGroupAddress
   alaIgmpStaticMemberRowStatus
alaipmvReceiverVlanPortTable
   alaipmvReceiverVlanPortIPMVlanNumber
   alaipmvReceiverVlanPortNumber
   alaipmvReceiverVlanPortRcvrVlanNumber
   alaipmvReceiverVlanPortRowStatus
```

ip multicast query-interval

Sets the IGMP query interval on the specified VLAN or on the system if no VLAN is specified.

ip multicast [vlan *vid***] query-interval [***seconds***]**

Syntax Definitions

vid	VLAN on which to apply the configuration.
seconds	IGMP query interval in seconds. Valid range is 1 to 65535.

Defaults

parameter	default
seconds	125

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- IP Multicast Switching and Routing must be enabled to set the IGMP query interval on the system and/or the specified VLANs.
- If the IGMP query interval is already configured on the system, then the VLAN configuration will override the system's configuration.
- The IGMP query interval refers to the time period between IGMP query messages.
- To restore the IGMP query interval to its default (that is, 125 seconds) value on the system if no VLAN is specified, use **ip multicast query-interval** followed by the value 0 (for example, ip multicast query-interval 0) or use only **ip multicast query-interval** (for example, ip multicast query-interval).
- To restore the IGMP query interval to its default (that is, 125 seconds) value on the specified VLAN, use **ip multicast vlan** *vid* **query-interval**, followed by the value 0 (for example, ip multicast vlan 2 query-interval 0) or use only **ip multicast vlan** *vid* **query-interval** (for example, ip multicast vlan 2 query-interval).

Examples

```
-> ip multicast query-interval 100
-> ip multicast query-interval 0
-> ip multicast query-interval
-> ip multicast vlan 2 query-interval 100
-> ip multicast vlan 2 query-interval 0
-> ip multicast vlan 2 query-interval
```

Release History

Release 6.1.1; command was introduced.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaIgmp
   alaIgmpQueryInterval
alaIgmpVlan
   alaIgmpVlanQueryInterval
```

ip multicast last-member-query-interval

Sets the IGMP last member query interval value on the specified VLAN or on the system if no VLAN is specified.

ip multicast [vlan *vid***] last-member-query-interval [***tenths-of-seconds***]**

Syntax Definitions

vid	VLAN on which to apply the configuration.
tenths-of-seconds	IGMP last member query interval in tenths of seconds. Valid range is 1 to 65535.

Defaults

parameter	default
tenths-of-seconds	10

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- IP Multicast Switching and Routing must be enabled to set the IGMP last member query interval on the system and/or the specified VLANs.
- If the IGMP last member query interval is already configured on the system, then the VLAN configuration will override the system's configuration.
- The IGMP last member query interval refers to the time period to reply to an IGMP query message sent in response to a leave group message.
- To restore the IGMP last member query interval to its default (that is, 10 tenths-of-seconds) value on the system if no VLAN is specified, use **ip multicast last-member-query-interval** followed by the value 0 (for example, ip multicast last-member-query-interval 0) or use only **ip multicast last-member-query-interval** (for example, ip multicast last-member-query-interval).
- To restore the IGMP last member query interval to its default (that is, 10 tenths-of-seconds) value on the specified VLAN, use **ip multicast vlan** *vid* **last-member-query interval** followed by the value 0 (for example, ip multicast vlan 2 last-member-query-interval 0) or use only **ip multicast vlan** *vid* **last-member-query-interval** (for example, ip multicast vlan 2 last-member-query-interval).

Examples

```
-> ip multicast last-member-query-interval 22
-> ip multicast last-member-query-interval 0
-> ip multicast last-member-query-interval
-> ip multicast vlan 2 last-member-query-interval 22
-> ip multicast vlan 2 last-member-query-interval 0
-> ip multicast vlan 2 last-member-query-interval
```

Release History

Release 6.1.1; command was introduced.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaIgmp
   alaIgmpLastMemberQueryInterval
alaIgmpVlan
   alaIgmpVlanLastMemberQueryInterval
```

ip multicast query-response-interval

Sets the IGMP query response interval on the specified VLAN or on the system if no VLAN is specified.

ip multicast [vlan *vid***] query-response-interval [***tenths-of-seconds***]**

Syntax Definitions

vid	VLAN on which to apply the configuration.
tenths-of-seconds	IGMP query response interval in tenths of seconds. Valid range is 1 to 65535.

Defaults

parameter	default
tenths-of-seconds	100

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- IP Multicast Switching and Routing must be enabled to set the IGMP query response interval on the system and/or the specified VLANs.
- If the IGMP query response interval is already configured on the system, then the VLAN configuration will override the system's configuration.
- The query response interval refers to the time period to reply to an IGMP query message.
- To restore the IGMP query response interval to its default (that is, 100 tenths-of-seconds) value on the system if no VLAN is specified, use **ip multicast query-response-interval** followed by the value 0 (for example, ip multicast query-response-interval 0) or use only **ip multicast query-response-interval** (for example, ip multicast query-response-interval).
- To restore the IGMP last member query interval to its default (that is, 100 tenths-of-seconds) value on the specified VLAN, use **ip multicast vlan** *vid* **query-response-interval** followed by the value 0 (for example, ip multicast vlan 2 query-response-interval 0) or use only **ip multicast vlan** *vid* **query-response-interval** (for example, ip multicast vlan 2 query-response-interval).

Examples

```
-> ip multicast query-response-interval 200
-> ip multicast query-response-interval 0
-> ip multicast query-response-interval
-> ip multicast vlan 2 query-response-interval 300
-> ip multicast vlan 2 query-response-interval 0
-> ip multicast vlan 2 query-response-interval
```

Release History

Release 6.1.1; command was introduced.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaIgmp
   alaIgmpQueryResponseInterval
alaIgmpVlan
   alaIgmpVlanQueryResponseInterval
```

ip multicast unsolicited-report-interval

Sets the value of the IGMP unsolicited report interval on the specified VLAN or on the system if no VLAN is specified.

ip multicast [vlan *vid***] unsolicited-report-interval [***seconds***]**

Syntax Definitions

vid	VLAN on which to apply the configuration.
seconds	IGMP query response interval in seconds. Valid range is 1 to 65535, where 0 represents the default setting.

Defaults

parameter	default
seconds	1

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- IP Multicast Switching and Routing must be enabled to set the IGMP unsolicited report interval on the system and/or the specified VLANs.
- If the IGMP query response interval is already configured on the system, then the VLAN configuration will override the system's configuration.
- The unsolicited report interval refers to the time period to proxy any changed IGMP membership state.
- To restore the IGMP unsolicited report interval to its default (that is, 1 second) value on the system if no VLAN is specified, use **ip multicast unsolicited-report-interval** followed by the value 0 (for example, ip multicast unsolicited-report-interval 0) or use only **ip multicast unsolicited-report-interval** (for example, ip multicast unsolicited-report-interval).
- To restore the IGMP unsolicited report interval to its default (that is, 1 second) value on the specified VLAN, use **ip multicast vlan** *vid* **unsolicited-report-interval** followed by the value 0 (for example, ip multicast vlan 2 unsolicited-report-interval 0) or use only **ip multicast vlan** *vid* **unsolicited-report-interval** (for example, ip multicast vlan 2 unsolicited-report-interval).

Examples

```
-> ip multicast unsolicited-report-interval 200
-> ip multicast unsolicited-report-interval 0
-> ip multicast unsolicited-report-interval
-> ip multicast vlan 2 unsolicited-report-interval 300
-> ip multicast vlan 2 unsolicited-report-interval 0
-> ip multicast vlan 2 unsolicited-report-interval
```

Release History

Release 6.1.3; command was introduced.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaIgmp
   alaIgmpUnsolicitedReportInterval
alaIgmpVlan
   alaIgmpVlanUnsolicitedReportInterval
```

ip multicast router-timeout

Configures the expiry time of IP multicast routers on the specified VLAN or on the system if no VLAN is specified.

ip multicast [vlan *vid***] router-timeout [***seconds***]**

Syntax Definitions

vid	VLAN on which to apply the configuration.
seconds	IGMP router timeout in seconds. Valid range is 1 to 65535.

Defaults

parameter	default
seconds	90

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- IP Multicast Switching and Routing must be enabled to set the IGMP router timeout on the system and/or the specified VLANs.
- If the IGMP router timeout is already configured on the system, then the VLAN configuration will override the system's configuration.
- To restore the IGMP router timeout to its default (that is, 90 seconds) value on the system if no VLAN is specified, use **ip multicast router-timeout** followed by the value 0 (for example, ip multicast router-timeout 0) or use only **ip multicast router-timeout** (for example, ip multicast router-timeout).
- To restore the IGMP router timeout to its default (that is, 90 seconds) value on the specified VLAN, use **ip multicast vlan** *vid* **router-timeout** followed by the value 0 (for example, ip multicast vlan 2 router-timeout 0) or use only **ip multicast vlan** *vid* **router-timeout** (for example, ip multicast vlan 2 router-timeout).

Examples

```
-> ip multicast router-timeout 100
-> ip multicast router-timeout 0
-> ip multicast router-timeout
-> ip multicast vlan 2 router-timeout 100
-> ip multicast vlan 2 router-timeout 0
-> ip multicast vlan 2 router-timeout
```

Release History

Release 6.1.1; command was introduced.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaIgmp
   alaIgmpRouterTimeout
alaIgmpVlan
   alaIgmpVlanRouterTimeout
```

ip multicast source-timeout

Configures the expiry time of IP multicast sources on the specified VLAN or on the system if no VLAN is specified.

ip multicast [vlan *vid***] source-timeout [***seconds***]**

Syntax Definitions

vid	VLAN on which to apply the configuration.
seconds	IGMP source timeout in seconds. Valid range is 1 to 65535.

Defaults

parameter	default
seconds	30

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- IP Multicast Switching and Routing must be enabled to set the IGMP source timeout on the system and/or the specified VLANs.
- If the IGMP source timeout is already configured on the system, then the VLAN configuration will override the system's configuration.
- To restore the IGMP source timeout to its default (that is, 30 seconds) value on the system if no VLAN is specified, use **ip multicast source-timeout** followed by the value 0 (for example, ip multicast source-timeout 0) or use only **ip multicast source-timeout** (for example, ip multicast source-timeout).
- To restore the IGMP source timeout to its default (that is, 30 seconds) value on the specified VLAN, use **ip multicast vlan** *vid* **source-timeout** followed by the value 0 (for example, ip multicast vlan 2 source-timeout 0) or use only **ip multicast vlan** *vid* **source-timeout** (for example, ip multicast vlan 2 source-timeout).

Examples

```
-> ip multicast source-timeout 100
-> ip multicast source-timeout 0
-> ip multicast source-timeout
-> ip multicast vlan 2 source-timeout 100
-> ip multicast vlan 2 source-timeout 0
-> ip multicast vlan 2 source-timeout
```

Release History

Release 6.1.1; command was introduced.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaIgmp
   alaIgmpSourceTimeout
alaIgmpVlan
   alaIgmpVlanSourceTimeout
```

ip multicast querying

Enables or disables IGMP querying on the specified VLAN or on the system if no VLAN is specified.

ip multicast [vlan *vid***] querying [{enable | disable}]**

Syntax Definitions

vid	VLAN on which configuration is applied.
enable	Enable IGMP querying.
disable	Disable IGMP querying.

Defaults

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

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- IP Multicast Switching and Routing must be enabled to enable IGMP querying on the system and/or specified VLANs.
- If the IGMP querying is already enabled/disabled on the system, then the VLAN configuration will override the system's configuration.
- IGMP querying refers to requesting the network's IGMP group membership information by sending out IGMP queries. IGMP querying also involves participating in IGMP querier election.
- You can also restore the IGMP querying to its default (that is, disabled) setting on the system if no VLAN is specified, by using only **ip multicast querying** (for example, ip multicast querying).
- You can also restore the IGMP querying to its default (that is, disabled) setting on the specified VLAN, by using only **ip multicast vlan** *vid* **querying** (for example, ip multicast vlan 2 querying).

Examples

```
-> ip multicast querying enable
-> ip multicast querying disable
-> ip multicast querying
-> ip multicast vlan 2 querying enable
-> ip multicast vlan 2 querying disable
-> ip multicast vlan 2 querying
```

Release History

Release 6.1.1; command was introduced.
Release 6.3.1; **no** parameter added.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaIgmp
   alaIgmpQuerying
alaIgmpVlan
   alaIgmpVlanQuerying
```

ip multicast robustness

Sets the IGMP robustness variable on the specified VLAN or on the system if no VLAN is specified.

ip multicast [vlan *vid***] robustness [***robustness***]**

Syntax Definitions

vid	VLAN on which to apply the configuration.
robustness	IGMP robustness variable. Valid range is 1 to 7.

Defaults

parameter	default
robustness	2

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- IP Multicast Switching and Routing must be enabled to set the IGMP robustness variable on the system and/or the specified VLANs.
- If the IGMP robustness variable is already configured on the system, then the VLAN configuration will override the system's configuration.
- Robustness variable allows fine-tuning on the network, where the expected packet loss would be greater.
- To restore the IGMP robustness variable to its default (that is, 2) value on the system if no VLAN is specified, use **ip multicast robustness** followed by the value 0 (for example, ip multicast robustness 0) or use only
  ip multicast robustness (for example, ip multicast robustness).
- To restore the IGMP robustness variable to its default (that is, 2) value on the specified VLAN, use **ip multicast vlan** *vid* **robustness** followed by the value 0 (for example, ip multicast vlan 2 robustness 0) or use only **ip multicast vlan** *vid* **robustness** (for example, ip multicast vlan 2 robustness).

Examples

```
-> ip multicast robustness 3
-> ip multicast robustness 0
-> ip multicast robustness
-> ip multicast vlan 2 robustness 3
-> ip multicast vlan 2 robustness 0
-> ip multicast vlan 2 robustness
```

Release History

Release 6.1.1; command was introduced.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaIgmp
   alaIgmpRobustness
alaIgmpVlan
   alaIgmpVlanRobustness
```

ip multicast spoofing

Enables or disables IGMP spoofing on the specified VLAN or on the system if no VLAN is specified.

ip multicast [vlan *vid***] spoofing [{enable | disable}]**

Syntax Definitions

vid	VLAN on which to apply the configuration.
enable	Enable IGMP spoofing.
disable	Disable IGMP spoofing.

Defaults

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

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- If the IGMP spoofing is already enabled on the system, then the VLAN configuration will override the system's configuration.
- IGMP spoofing refers to replacing a client's MAC and IP address with the system's MAC and IP address when proxying aggregated IGMP group membership information.
- You can also restore the IGMP spoofing to its default (that is, disabled) setting on the system if no VLAN is specified, by using only **ip multicast spoofing** (for example, ip multicast spoofing).
- You can also restore the IGMP spoofing to its default (that is, disabled) setting on the specified VLAN, by using only **ip multicast vlan** *vid* **spoofing** (for example, ip multicast vlan 2 spoofing).

Examples

```
-> ip multicast spoofing enable
-> ip multicast spoofing disable
-> ip multicast spoofing
-> ip multicast vlan 2 spoofing enable
-> ip multicast vlan 2 spoofing disable
-> ip multicast vlan 2 spoofing
```

Release History

Release 6.1.1; command was introduced.
Release 6.3.1; **no** parameter added.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaIgmp
   alaIgmpSpoofing
alaIgmpVlan
   alaIgmpVlanSpoofing
```

ip multicast zapping

Enables or disables IGMP zapping on the specified VLAN or on the system if no VLAN is specified.

ip multicast [vlan *vid***] zapping [{enable | disable}]**

Syntax Definitions

vid	VLAN on which to apply the configuration.
enable	Enable IGMP zapping.
disable	Disable IGMP zapping.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- If the IGMP zapping is already enabled on the system, then the VLAN configuration will override the system's configuration.
- IGMP zapping refers to processing membership, immediate source filter removals and will not wait for the protocol's specified time period. This mode facilitates IP TV applications looking for quick changes between IP multicast groups.
- To restore the IGMP querying to its default (that is, disabled) setting on the system if no VLAN is specified, use the command **ip multicast zapping** (for example, ip multicast zapping).
- To restore the IGMP querying to its default (that is, disabled) setting on the specified VLAN, use the command **ip multicast vlan** *vid* **zapping** (for example, ip multicast vlan 2 zapping).

Examples

```
-> ip multicast zapping enable
-> ip multicast zapping disable
-> ip multicast zapping
-> ip multicast vlan 2 zapping enable
-> ip multicast vlan 2 zapping disable
-> ip multicast vlan 2 zapping
```

Release History

Release 6.1.1; command was introduced.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaIgmp
   alaIgmpZapping
alaIgmpVlan
   alaIgmpVlanZapping
```

ip multicast proxying

Enables or disables IGMP proxying on the specified VLAN or on the system if no VLAN is specified.

ip multicast [vlan *vid***] proxying [enable | disable]**

Syntax Definitions

vid	VLAN on which to apply the configuration.
enable	Enable IGMP proxying.
disable	Disable IGMP proxying.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- If the IGMP proxying is already enabled on the system, then the VLAN configuration will override the system's configuration.
- IGMP proxying refers to processing membership information on behalf of client systems and reporting membership on their behalf.
- To restore the IGMP querying to its default (that is, disabled) setting on the system if no VLAN is specified, use the command **ip multicast zapping** (for example, ip multicast zapping).
- To restore the IGMP querying to its default (that is, disabled) setting on the specified VLAN, use the command **ip multicast vlan** *vid* **zapping** (for example, ip multicast vlan 2 zapping).

Note Proxying feature is not supported on MCLAG Primary and Secondary switches in MCLAG environment**.**

Examples

```
-> ip multicast proxying enable
-> ip multicast proxying disable
-> ip multicast proxying
-> ip multicast vlan 2 proxying enable
-> ip multicast vlan 2 proxying disable
-> ip multicast vlan 2 proxying
```

Release History

Release 6.1.3; command was introduced.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaIgmp
   alaIgmpProxying
alaIgmpVlan
   alaIgmpVlanProxying
```

ip multicast helper-address

Specifies the destination IP address of a relay host where IGMP host reports and Leave messages are to be sent.

ip multicast helper-address [*ip-address***]**

Syntax Definitions

ip-address	The IP address of the relay host

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- After the destination IP address is specified, the IPMS reporting feature is enabled.
- To disable IPMS reporting feature, use 0.0.0.0 as the IP address. IPMS reporting feature can also be disabled by omitting the IP address from the command.

Examples

```
-> ip multicast helper-address 10.1.1.198
-> ip multicast helper-address 0.0.0.0
```

Release History

Release 6.4.2; command was introduced.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaIgmp
   alaIgmpHelperAddress
   alaIgmpHelperAddressType
```

ipv6 multicast status

Enables or disables IPv6 Multicast Switching and Routing on the specified VLAN or on the system if no VLAN is specified.

ipv6 multicast [vlan *vid***] status [{enable | disable}]**

Syntax Definitions

vid	VLAN on which to apply the configuration.
enable	Enable IPv6 Multicast Switching and Routing.
disable	Disable IPv6 Multicast Switching and Routing.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- If an IPv6 multicast routing protocol is already running on the system, the **ipv6 multicast status** command will override this configuration and always enable IPv6 Multicast Switching and Routing.
- If the IPv6 Multicast Switching and Routing is already enabled on the system, then the VLAN configuration overrides the system's configuration.
- To restore the MLD querying to its default (that is, disabled) status on the system if no VLAN is specified, use the command **ipv6 multicast status** (for example, ipv6 multicast status).
- To restore the MLD querying to its default (that is, disabled) status on the specified VLAN, use the command **ipv6 multicast vlan** *vid* **status** (for example, ipv6 multicast vlan 2 status).

Examples

```
-> ipv6 multicast status enable
-> ipv6 multicast status disable
-> ipv6 multicast status
-> ipv6 multicast vlan 2 status enable
-> ipv6 multicast vlan 2 status disable
-> ipv6 multicast vlan 2 status
```

Release History

Release 6.1.1; command was introduced.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaMld
   alaMldStatus
alaMldVlan
   alaMldVlanStatus
```

ipv6 multicast querier-forwarding

Enables or disables MLD querier forwarding on the specified VLAN or on the system if no VLAN is specified.

ipv6 multicast [vlan *vid***] querier-forwarding [{enable | disable}]**

no ipv6 multicast [vlan *vid***] querier-forwarding**

Syntax Definitions

vid	The VLAN on which configuration is applied.
enable	Enable MLD querier forwarding.
disable	Disable MLD querier forwarding.

Defaults

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

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to remove an MLD querier forwarding entry on the specified VLAN or on the system and return to its default behavior.
- If the MLD querier forwarding is already enabled on the system, then the VLAN configuration will override the system's configuration.
- MLD querier forwarding refers to promoting detected MLD queriers to receive all IP multicast data traffic.

Examples

```
-> ipv6 multicast querier-forwarding enable
-> ipv6 multicast querier-forwarding disable
-> ipv6 multicast querier-forwarding
-> ipv6 multicast vlan 2 querier-forwarding enable
-> ipv6 multicast vlan 2 querier-forwarding disable
-> ipv6 multicast vlan 2 querier-forwarding
-> no ipv6 multicast vlan 2 querier-forwarding
```

Release History

Release 6.3.1; command was introduced.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaMld
   alaMldQuerierForwarding
alaMldVlan
   alaMldVlanQuerierForwarding
```

ipv6 multicast version

Sets the default version of the MLD protocol on the specified VLAN or on the system if no VLAN is specified.

ipv6 multicast [vlan *vid***] version [***version***]**

Syntax Definitions

vid	VLAN on which to apply the configuration.
version	Default MLD protocol version to run. Valid range is 1 to 2.

Defaults

parameter	default
version	1

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- IPv6 Multicast Switching and Routing must be enabled to set the default MLD protocol version on the system and/or the specified VLANs.
- If the default MLD protocol version is already configured on the system, then the VLAN configuration overrides the system's configuration.
- Due to protocol inter-operation requirements, this command specifies only a default version of the MLD protocol to run.
- To restore the MLD multicast version to the default (that is, 1) version on the system if no VLAN is specified, use **ipv6 multicast version** followed by the value 0 (for example, ipv6 multicast version 0) or use
  only **ipv6 multicast version** (for example, ipv6 multicast version).
- To restore the MLD multicast version to the default (that is, 1) version on the specified VLAN, use **ipv6 multicast vlan** *vid* **version** followed by the value 0 (for example, ipv6 multicast vlan 2 version 0) or use only **ipv6 multicast vlan** *vid* **version** (for example, ipv6 multicast vlan 2 version).

Examples

```
-> ipv6 multicast version 2
-> ipv6 multicast version 0
-> ipv6 multicast version
-> ipv6 multicast vlan 2 version 2
-> ipv6 multicast vlan 2 version 0
-> ipv6 multicast vlan 2 version
```

Release History

Release 6.1.1; command was introduced.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaMld
   alaMldVersion
alaMldVlan
   alaMldVlanVersion
```

ipv6 multicast max-group

Configures the global maximum group limit that can be learned per port/VLAN instance.The limit is applied to each port/VLAN instance and an action is taken when it exceeds the limit.

ipv6 multicast max-group [*num***] [action {none | drop | replace}]**

Syntax Definitions

num	Specifies the maximum MLD group count. Valid range is 0 to 4294967295.
none	Disables the maximum group limit configuration
drop	Drops the incoming membership request.
replace	Replaces an existing membership with the incoming membership request.

Defaults

By default, the max-group limit is set to zero.

parameter	defaults
Action	**none**

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Configuring a max-group value will have no affect on existing group memberships until the memberships are refreshed on the port/VLAN instance.
- The configuration is allowed even when the ip multicast status is disabled.
- If the num and action parameters are not specified, then the limit is removed.
- The max-group configuration on a specific VLAN or port will override the global configuration.
- MLD zapping must be enabled when the max-group limit is enabled and the action is dropped.

Examples

```
-> ipv6 multicast max-group 10 action drop
-> ipv6 multicast max-group 20 action replace
-> ipv6 multicast max-group
```

Release History

Release 6.3.4; command was introduced.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaIgmpMaxGroupLimit
   alaIgmpMaxGroupExceedAction
```

ipv6 multicast vlan max-group

Configures the maximum group limit learned per port on a VLAN. The limit is applied to each port that is a member of the given VLAN.

ipv6 multicast vlan *vid* **max-group [***num***] [action {none | drop | replace}]**

Syntax Definitions

vid	VLAN on which to apply the configuration.
num	The maximum MLD group count. Valid range is 0 to 4294967295.
none	Disables the maximum group limit configuration.
drop	Drops the incoming membership request.
replace	Replaces an existing membership with the incoming membership request.

Defaults

By default, the max-group limit is set to zero.

parameter	defaults
Action	none

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Configuring a max-group value will have no affect on existing group memberships until the memberships are refreshed on the port/VLAN instance.
- The configuration is allowed even when the ip multicast status is disabled.
- If the num and action parameters are not specified, then the limit is removed.
- The max-group configuration on a VLAN will override the global configuration.
- MLD zapping must be enabled when the max-group limit is enabled and the action is dropped.

Examples

```
-> ipv6 multicast vlan 10 max-group 10 action drop
-> ipv6 multicast vlan 10 max-group 20 action replace
```

Release History

Release 6.3.4; command was introduced.

Related Commands

show ipv6 multicast	Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaIgmpVlanTable
   alaIgmpVlanMaxGroupLimit
   alaIgmpVlanMaxGroupExceedAction
```

ipv6 multicast port max-group

Configures the maximum group limit learned per port. The limit is applicable on the given port for all VLAN instances of the port.

ipv6 multicast port *slot* | *port* **max-group [***num***] [action {none | drop | replace}]**

Syntax Definitions

slot | *port*	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
num	The maximum MLD group count. Valid range is 0 to 4294967295.
none	Disables the maximum group limit configuration.
drop	Drops the incoming membership request.
replace	Replaces an existing membership with the incoming membership request.

Defaults

By default, the max-group limit is set to zero.

parameter	defaults
Action	**none**

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Configuring a max-group value will have no affect on existing group memberships until the memberships are refreshed on the port/VLAN instance.
- The configuration is allowed even when the ip multicast status is disabled.
- If the num and action parameters are not specified, then the limit is removed.
- The max-group configuration on a port will override the VLAN or global configuration.
- MLD zapping must be enabled when the max-group limit is enabled and the action is dropped.

Examples

```
-> ipv6 multicast port 1/1 max-group 10 action drop
-> ipv6 multicast port 1/1 max-group action replace
```

Release History

Release 6.3.4; command was introduced.

Related Commands

show ipv6 multicast	Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaIgmpPortTable
   alaIgmpPortMaxGroupLimit
   alaIgmpPortMaxGroupExceedAction
```

ipv6 multicast static-neighbor

Creates a static MLD neighbor entry on a specified port on a specified VLAN.

ipv6 multicast static-neighbor vlan *vid* **port** *slot/port*

no ipv6 multicast static-neighbor vlan *vid* **port** *slot/port*

Syntax Definitions

vid	VLAN to include as a static MLD neighbor.
slot/port	The slot/port number you want to configure as a static MLD neighbor.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to remove an MLD static neighbor entry on a specified port on a specified VLAN.
- The **ipv6 multicast static-neighbor** command allows you to create an MLD static neighbor entry on a specified port on a specified VLAN. This, in turn, enables that network segment to receive all MLD traffic.
- You can also create an MLD static neighbor entry on a link aggregate port by entering **ipv6 multicast static-neighbor vlan** *vid* **port**, followed by the link aggregation group number (for example, ipv6 multicast static-neighbor vlan 2 port 7).

Examples

```
-> ipv6 multicast static-neighbor vlan 4 port 1/1
-> no ipv6 multicast static-neighbor vlan 4 port 1/1
-> ipv6 multicast static-neighbor vlan 4 port 7
-> no ipv6 multicast static-neighbor vlan 4 port 7
```

Release History

Release 6.1.1; command was introduced.

Related Commands

show ipv6 multicast neighbor	Displays the MLD neighbor table entries of IPv6 Multicast Switching and Routing.

MIB Objects

```
alaMldStaticNeighborTable
   alaMldStaticNeighborVlan
   alaMldStaticNeighborIfIndex
   alaMldStaticNeighborRowStatus
```

ipv6 multicast static-querier

Creates a static MLD querier entry on a specified port on a specified VLAN.

ipv6 multicast static-querier vlan *vid* **port** *slot/port*

no ipv6 multicast static-querier vlan *vid* **port** *slot/port*

Syntax Definitions

vid	VLAN to include as a static MLD querier.
slot/port	The slot/port number you want to configure as a static MLD querier.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to remove an MLD static querier entry on a specified port on a specified VLAN.
- The **ipv6 multicast static-querier** command allows you to create an MLD static querier entry on a specified port on a specified VLAN. This, in turn, enables that network segment to receive all MLD traffic.
- You can also create an MLD static querier entry on a link aggregate port by entering **ipv6 multicast static-querier vlan** *vid* **port**, followed by the link aggregation group number (for example, ipv6 multicast static-querier vlan 2 port 7).

Examples

```
-> ipv6 multicast static-querier vlan 4 port 1/1
-> no ipv6 multicast static-querier vlan 4 port 1/1
-> ipv6 multicast static-querier vlan 4 port 7
-> no ipv6 multicast static-querier vlan 4 port 7
```

Release History

Release 6.1.1; command was introduced.

Related Commands

show ipv6 multicast querier	Displays the MLD querier table entries of IPv6 Multicast Switching and Routing.

MIB Objects

```
alaMldStaticQuerierTable
   alaMldStaticQuerierVlan
   alaMldStaticQuerierIfIndex
   alaMldStaticQuerierRowStatus
```

ipv6 multicast static-group

Creates a static MLD group entry on a specified port on a specified VLAN.

ipv6 multicast static-group *ip_address* **vlan** *vid* **port** *slot/port*

no ipv6 multicast static-group *ip_address* **vlan** *vid* **port** *slot/port*

Syntax Definitions

ip_address	IPv6 multicast group address.
vid	VLAN to include as a static MLD group.
slot/port	The slot/port number you want to configure as a static MLD group.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to remove an MLD static group entry on a specified port on the specified VLAN.
- The **ipv6 multicast static-group** command allows you to create an MLD static group entry on a specified port on a specified VLAN. This, in turn, enables that network segment to receive MLD traffic addressed to the specified IPv6 multicast group address.
- You can also create an MLD static group entry on a link aggregate port by entering **ipv6 multicast static-group** *ip_address* **vlan** *vid* **port**, followed by the link aggregation group number (for example, ipv6 multicast static-group ff05::5 vlan 2 port 7).

Examples

```
-> ipv6 multicast static-group ff05::4681 vlan 4 port 1/1
-> no ipv6 multicast static-group ff05::4681 vlan 4 port 1/1
-> ipv6 multicast static-group ff05::4681 vlan 4 port 7
-> no ipv6 multicast static-group ff05::4681 vlan 4 port 7
```

Release History

Release 6.1.1; command was introduced.

Related Commands

show ipv6 multicast group	Displays the MLD group membership table entries of IPv6 Multicast Switching and Routing for the specified IPv6 multicast group address or all entries if no IPv6 multicast group address is specified.

MIB Objects

```
alaMldStaticMemberTable
   alaMldStaticMemberVlan
   alaMldStaticMemberIfIndex
   alaMldStaticMemberGroupAddress
   alaMldStaticMemberRowStatus
```

ipv6 multicast query-interval

Sets the MLD query interval on the specified VLAN or on the system if no VLAN is specified.

ipv6 multicast [vlan *vid***] query-interval [***seconds***]**

Syntax Definitions

vid	VLAN on which to apply the configuration.
seconds	MLD query interval in seconds. Valid range is 1 to 65535.

Defaults

parameter	default
seconds	125

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- IPv6 Multicast Switching and Routing must be enabled to set the MLD query interval on the system and/or the specified VLANs.
- If the MLD query interval is already configured on the system, then the VLAN configuration will override the system's configuration.
- The MLD query interval refers to the time period between MLD query messages.
- To restore the MLD query interval to its default (that is, 125 seconds) value on the system if no VLAN is specified, use **ipv6 multicast query-interval** followed by the value 0 (for example, ipv6 multicast query-interval 0) or use only **ipv6 multicast query-interval (**for example, ipv6 multicast query-interval).
- To restore the MLD query interval to its default (that is, 125 seconds) value on the specified VLAN, use **ipv6 multicast vlan** *vid* **query-interval** followed by the value 0 (for example, ipv6 multicast vlan 2 query-interval 0) or use only **ipv6 multicast vlan** *vid* **query-interval** (for example, ipv6 multicast vlan 2 query-interval).

Examples

```
-> ipv6 multicast query-interval 100
-> ipv6 multicast query-interval 0
-> ipv6 multicast query-interval
-> ipv6 multicast vlan 2 query-interval 100
-> ipv6 multicast vlan 2 query-interval 0
-> ipv6 multicast vlan 2 query-interval
```

Release History

Release 6.1.1; command was introduced.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaMld
   alaMldQueryInterval
alaMldVlan
   alaMldVlanQueryInterval
```

ipv6 multicast last-member-query-interval

Sets the MLD last member query interval on the specified VLAN or on the system if no VLAN is specified.

ipv6 multicast [vlan *vid***] last-member-query-interval [***milliseconds***]**

Syntax Definitions

vid	VLAN on which to apply the configuration.
milliseconds	MLD last member query interval in milliseconds. Valid range is 1 to 65535.

Defaults

parameter	default
milliseconds	1000

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- IPv6 Multicast Switching and Routing must be enabled to set the MLD last member query interval to use on the system and/or the specified VLANs. apply this configuration.
- If the MLD last member query interval is already configured on the system, then the VLAN configuration will override the system's configuration.
- The MLD last member query interval refers to the time period to reply to an MLD query message sent in response to a leave group message.
- To restore the MLD last member query interval to its default (that is, 1000 milliseconds) value on the system if no VLAN is specified, use **ipv6 multicast last-member-query-interval** followed by the value “0” (for example, ipv6 multicast last-member-query-interval “0”) or use only **ipv6 multicast last-member-query-interval** (for example, ipv6 multicast last-member-query-interval).
- To restore the MLD last member query interval to its default (that is, 1000 milliseconds) value on the specified VLAN, use **ipv6 multicast vlan** *vid* **last-member-query interval** followed by the value 0 (for example, ipv6 multicast vlan 2 last-member-query-interval 0) or use only **ipv6 multicast vlan** *vid* **last-member-query-interval** (for example, ipv6 multicast vlan 2 last-member-query-interval).

Examples

```
-> ipv6 multicast last-member-query-interval 2200
-> ipv6 multicast last-member-query-interval 0
-> ipv6 multicast last-member-query-interval
-> ipv6 multicast vlan 4 last-member-query-interval 2200
-> ipv6 multicast vlan 4 last-member-query-interval 0
-> ipv6 multicast vlan 4 last-member-query-interval
```

Release History

Release 6.1.1; command was introduced.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaMld
   alaMldLastMemberQueryInterval
alaMldVlan
   alaMldVlanLastMemberQueryInterval
```

ipv6 multicast query-response-interval

Sets the MLD query response interval on the specified VLAN or on the system if no VLAN is specified.

ipv6 multicast [vlan *vid***] query-response-interval [***milliseconds***]**

Syntax Definitions

vid	VLAN on which to apply the configuration.
milliseconds	MLD query response interval in milliseconds. Valid range is 1 to 65535.

Defaults

parameter	default
milliseconds	10000

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- IPv6 Multicast Switching and Routing must be enabled to set the MLD query response interval to use on the system and/or the specified VLANs.
- If the MLD query response interval is already configured on the system, then the VLAN configuration will override the system's configuration.
- The MLD query response interval refers to the time period to reply to an MLD query message.
- To restore the MLD query response interval to its default (that is, 10000 milliseconds) value on the system if no VLAN is specified, use **ipv6 multicast query-response-interval** followed by the value 0 (for example, ipv6 multicast query-response-interval 0) or use only **ipv6 multicast query-response-interval** (for example, ipv6 multicast query-response-interval).
- To restore the MLD last member query interval to its default (that is, 10000 milliseconds) value on the specified VLAN, use **ipv6 multicast vlan** *vid* **query-response-interval** followed by the value 0 (for example, ipv6 multicast vlan 2 query-response-interval 0) or use only **ipv6 multicast vlan** *vid* **query-response-interval** (for example, ipv6 multicast vlan 2 query-response-interval).

Examples

```
-> ipv6 multicast query-response-interval 20000
-> ipv6 multicast query-response-interval 0
-> ipv6 multicast query-response-interval
-> ipv6 multicast vlan 2 query-response-interval 20000
-> ipv6 multicast vlan 2 query-response-interval 0
-> ipv6 multicast vlan 2 query-response-interval
```

Release History

Release 6.1.1; command was introduced.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaMld
   alaMldQueryResponseInterval
alaMldVlan
   alaMldVlanQueryReponseInterval
```

ipv6 multicast unsolicited-report-interval

Sets the MLD unsolicited report interval on the specified VLAN or on the system if no VLAN is specified.

ipv6 multicast [vlan *vid***] unsolicited-report-interval [***seconds***]**

Syntax Definitions

vid	VLAN on which to apply the configuration.
seconds	MLD unsolicited report interval in seconds. Valid range is 1 to 65535, where 0 represents the default setting.

Defaults

parameter	default
seconds	1

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- IPv6 Multicast Switching and Routing must be enabled to set the MLD unsolicited report interval to use on the system and/or the specified VLANs.
- If the MLD unsolicited report interval is already configured on the system, then the VLAN configuration will override the system's configuration.
- The unsolicited report interval refers to the time period to proxy any changed MLD membership state.
- To restore the MLD unsolicited interval to its default (that is, 1 second) value on the system if no VLAN is specified, use **ipv6 multicast unsolicited-report-interval** followed by the value 0 (for example, ipv6 multicast unsolicited-report-interval 0) or use only **ipv6 multicast unsolicited-report-interval** (for example, ipv6 multicast unsolicited-report-interval).
- To restore the MLD unsolicited report interval to its default (that is, 1 second) value on the specified VLAN, use **ipv6 multicast vlan** *vid* **unsolicited-report-interval** followed by the value 0 (for example, ipv6 multicast vlan 2 unsolicited-report-interval 0) or use only **ipv6 multicast vlan** *vid* **unsolicited-report-interval** (for example, ipv6 multicast vlan 2 unsolicited-report-interval).

Examples

```
-> ipv6 multicast unsolicited-report-interval 20000
-> ipv6 multicast unsolicited-report-interval 0
-> ipv6 multicast unsolicited-report-interval
-> ipv6 multicast vlan 2 unsolicited-report-interval 20000
-> ipv6 multicast vlan 2 unsolicited-report-interval 0
-> ipv6 multicast vlan 2 unsolicited-report-interval
```

Release History

Release 6.1.3; command was introduced.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaMld
   alaMldUnsolicitedReportInterval
alaMldVlan
   alaMldVlanUnsolicitedReportInterval
```

ipv6 multicast router-timeout

Configures the expiry time of IPv6 multicast routers on the specified VLAN or on the system if no VLAN is specified.

ipv6 multicast [vlan *vid***] router-timeout [***seconds***]**

Syntax Definitions

vid	VLAN on which to apply the configuration.
seconds	MLD router timeout in seconds. Valid range is 1 to 65535.

Defaults

parameter	default
seconds	90

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- IPv6 Multicast Switching and Routing must be enabled to set the MLD router timeout on the system and/or the specified VLANs. apply this configuration.
- If the MLD router timeout is already configured on the system, then the VLAN configuration will override the system's configuration.
- To restore the MLD router timeout to its default (that is, 90 seconds) value on the system if no VLAN is specified, use **ipv6 multicast router-timeout** followed by the value 0 (for example, ipv6 multicast router-timeout 0) or use only **ipv6 multicast router-timeout** (for example, ipv6 multicast router-timeout).
- To restore the MLD router timeout to its default (that is, 90 seconds) value on the specified VLAN, use **ipv6 multicast vlan** *vid* **router-timeout** followed by the value 0 (for example, ipv6 multicast vlan 2 router-timeout 0) or use only **ipv6 multicast vlan** *vid* **router-timeout** (for example, ipv6 multicast vlan 2 router-timeout).

Examples

```
-> ipv6 multicast router-timeout 100
-> ipv6 multicast router-timeout 0
-> ipv6 multicast router-timeout
-> ipv6 multicast vlan 2 router-timeout 100
-> ipv6 multicast vlan 2 router-timeout 0
-> ipv6 multicast vlan 2 router-timeout
```

Release History

Release 6.1.1; command was introduced.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaMld
   alaMldRouterTimeout
alaMldVlan
   alaMldVlanRouterTimeout
```

ipv6 multicast source-timeout

Configures the expiry time of IPv6 multicast sources on the specified VLAN or on the system if no VLAN is specified.

ipv6 multicast [vlan *vid***] source-timeout [***seconds***]**

Syntax Definitions

vid	VLAN on which to apply the configuration.
seconds	MLD source timeout in seconds. Valid range is 1 to 65535.

Defaults

parameter	default
seconds	30

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- IPv6 Multicast Switching and Routing must be enabled to set the MLD source timeout on the system and/or the specified VLANs.
- If the MLD source timeout is already configured on the system, then the VLAN configuration will override the system's configuration.
- To restore the MLD router timeout to its default (that is, 30 seconds) value on the system if no VLAN is specified, use **ipv6 multicast source-timeout** followed by the value 0 (for example, ipv6 multicast source-timeout 0) or use only **ipv6 multicast source-timeout** (for example, ipv6 multicast source-timeout).
- To restore the MLD router timeout to its default (that is, 30 seconds) value on the specified VLAN, use **ipv6 multicast vlan** *vid* **source-timeout** followed by the value 0 (for example, ipv6 multicast vlan 2 source-timeout 0) or use only **ipv6 multicast vlan** *vid* **source-timeout** (for example, ipv6 multicast vlan 2 source-timeout).

Examples

```
-> ipv6 multicast source-timeout 100
-> ipv6 multicast source-timeout 0
-> ipv6 multicast source-timeout
-> ipv6 multicast vlan 2 source-timeout 100
-> ipv6 multicast vlan 2 source-timeout 0
-> ipv6 multicast vlan 2 source-timeout
```

Release History

Release 6.1.1; command was introduced.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaMld
   alaMldSourceTimeout
alaMldVlan
   alaMldVlanSourceTimeout
```

ipv6 multicast querying

Enables or disables MLD querying on the specified VLAN or on the system if no VLAN is specified.

ipv6 multicast [vlan *vid***] querying [{enable | disable}]**

Syntax Definitions

vid	VLAN on which to apply the configuration.
enable	Enable MLD querying.
disable	Disable MLD querying.

Defaults

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

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- IPv6 Multicast Switching and Routing must be enabled to enable MLD querying on the system and/or specified VLANs.
- If the MLD querying is already enabled/disabled on the system, then the VLAN configuration will override the system's configuration.
- MLD querying refers to requesting the network's MLD group membership information by sending out MLD queries. MLD querying also involves participating in MLD querier election.
- You can also restore the MLD querying to its default (that is, disabled) setting on the system if no VLAN is specified, by using only **ipv6 multicast querying** (for example, ipv6 multicast querying).
- You can also restore the MLD querying to its default (that is, disabled) setting on the specified VLAN, by using only **ipv6 multicast vlan** *vid* **querying** (for example, ipv6 multicast vlan 2 querying).

Examples

```
-> ipv6 multicast querying enable
-> ipv6 multicast querying disable
-> ipv6 multicast querying
-> ipv6 multicast vlan 2 querying enable
-> ipv6 multicast vlan 2 querying disable
-> ipv6 multicast vlan 2 querying
```

Release History

Release 6.1.1; command was introduced.
Release 6.3.1; **no** parameter added.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaMld
   alaMldQuerying
alaMldVlan
   alaMldVlanQuerying
```

ipv6 multicast robustness

Sets the MLD robustness variable on the specified VLAN or on the system if no VLAN is specified.

ipv6 multicast [vlan *vid***] robustness [***robustness***]**

Syntax Definitions

vid	VLAN on which to apply the configuration.
robustness	MLD robustness variable. Valid range is 1 to 7.

Defaults

parameter	default
robustness	2

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- IPv6 Multicast Switching and Routing must be enabled to set the MLD robustness variable on the system and/or the specified VLANs.
- If the MLD robustness variable is already configured on the system, then the VLAN configuration will override the system's configuration.
- Robustness variable allows fine-tuning on the network, where the expected packet loss would be greater.
- To restore the MLD robustness variable to its default (that is, 2) value on the system if no VLAN is specified, use **ipv6 multicast robustness** followed by the value 0 (for examplef, ipv6 multicast robustness 0) or use only **ipv6 multicast robustness** (for example, ipv6 multicast robustness).
- To restore the MLD robustness variable to its default (that is, 2) value on the specified VLAN, use **ipv6 multicast vlan** *vid* **robustness** followed by the value 0 (for example, ipv6 multicast vlan 2 robustness 0) or use only **ipv6 multicast vlan** *vid* **robustness** (for example, ipv6 multicast vlan 2 robustness).

Examples

```
-> ipv6 multicast robustness 3
-> ipv6 multicast robustness 0
-> ipv6 multicast robustness
-> ipv6 multicast vlan 2 robustness 3
-> ipv6 multicast vlan 2 robustness 0
-> ipv6 multicast vlan 2 robustness
```

Release History

Release 6.1.1; command was introduced.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaMld
   alaMldRobustness
alaMldVlan
   alaMldVlanRobustness
```

ipv6 multicast spoofing

Enables or disables MLD spoofing on the specified VLAN or on the system if no VLAN is specified.

ipv6 multicast [vlan *vid***] spoofing [{enable | disable}]**

Syntax Definitions

vid	VLAN on which to apply the configuration.
enable	Enable MLD spoofing.
disable	Disable MLD spoofing.

Defaults

parameter	defaults
enable | **disable**	**disable**

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- If the MLD spoofing is already enabled on the system, then the VLAN configuration will override the system's configuration.
- MLD spoofing refers to replacing a client's MAC and IP address with the system's MAC and IP address when proxying aggregated MLD group membership information.
- You can also restore the MLD spoofing to its default (that is, disabled) setting on the system if no VLAN is specified, by using only **ipv6 multicast spoofing** (that is, ipv6 multicast spoofing).
- You can also restore the MLD spoofing to its default (that is, disabled) setting on the specified VLAN, by using only **ipv6 multicast vlan** *vid* **spoofing** (that is, ipv6 multicast vlan 2 spoofing).

Examples

```
-> ipv6 multicast spoofing enable
-> ipv6 multicast spoofing disable
-> ipv6 multicast spoofing
-> ipv6 multicast vlan 2 spoofing enable
-> ipv6 multicast vlan 2 spoofing disable
-> ipv6 multicast vlan 2 spoofing
```

Release History

Release 6.1.1; command was introduced.
Release 6.3.1; **no** parameter added.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaMld
   alaMldSpoofing
alaMldVlan
   alaMldVlanSpoofing
```

ipv6 multicast zapping

Enables or disables MLD zapping on the specified VLAN or on the system if no VLAN is specified.

ipv6 multicast [vlan *vid***] zapping [{enable | disable}]**

Syntax Definitions

vid	VLAN on which to apply the configuration.
enable	Enable MLD zapping.
disable	Disable MLD zapping.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- If the MLD zapping is already enabled on the system, then the VLAN configuration will override the system's configuration.
- MLD zapping refers to processing membership and source filter removals immediately and not waiting for the protocol's specified time period. This mode facilitates IP TV applications looking for quick changes between IP multicast groups.
- You can also restore the MLD zapping to its default (that is, disabled) setting on the system if no VLAN is specified, by using only **ipv6 multicast zapping** (for example, ipv6 multicast zapping).
- You can also restore the MLD zapping to its default (that is, disabled) setting on the specified VLAN, by using only **ipv6 multicast vlan** *vid* **zapping** (for example, ipv6 multicast vlan 2 zapping).

Examples

```
-> ipv6 multicast zapping enable
-> ipv6 multicast zapping disable
-> ipv6 multicast zapping
-> ipv6 multicast vlan 2 zapping enable
-> ipv6 multicast vlan 2 zapping disable
-> ipv6 multicast vlan 2 zapping
```

Release History

Release 6.1.1; command was introduced.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaMld
   alaMldZapping
alaMldVlan
   alaMldVlanZapping
```

ipv6 multicast proxying

Enables or disables MLD proxying on the specified VLAN or on the system if no VLAN is specified.

ipv6 multicast [vlan *vid***] proxying [enable | disable]**

Syntax Definitions

vid	VLAN on which to apply the configuration.
enable	Enable MLD proxying.
disable	Disable MLD proxying.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- If the MLD proxying is already enabled on the system, then the VLAN configuration will override the system's configuration.
- MLD proxying refers to processing membership information on behalf of client systems and reporting membership on their behalf.
- You can also restore the MLD proxying to its default (that is, disabled) setting on the system if no VLAN is specified, by using only **ipv6 multicast proxying** (for example, ipv6 multicast proxying).
- You can also restore the MLD proxying to its default (that is, disabled) setting on the specified VLAN, by using only **ipv6 multicast vlan** *vid* **proxying** (for example, ipv6 multicast vlan 2 proxying).

Examples

```
-> ipv6 multicast proxying enable
-> ipv6 multicast proxying disable
-> ipv6 multicast proxying
-> ipv6 multicast vlan 2 proxying enable
-> ipv6 multicast vlan 2 proxying disable
-> ipv6 multicast vlan 2 proxying
```

Release History

Release 6.1.3; command was introduced.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaMld
   alaMldProxying
alaMldVlan
   alaMldVlanProxying
```

ip multicast static-ssm-map

Configure the static-ssm mapping in the system. This is a global command.

ipv6 multicast static-ssm-map [group *group_address***] /** *prefix* **[source** *source_address***]**

no ipv6 multicast static-ssm-map [group *group_address***] /** *prefix* **[source** *source_address***]**

Syntax Definitions

group_address	Group address for which the source addresses are to be mapped. This should be in PIM-SSM range. That is, 232.x.x.x.
prefix	Mask of the group address.
source_address	Source that will statically be mapped for the given group address.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- This command configures the mapping even when the switch is working in IGMPv1/v2 mode and when the group address is not configured in PIM-SSM group address. But the mapping will NOT be active under this condition. It has to be ensured that these two requirements are met when trying to map the IGMP v2 reports to PIM-SSM.
- When the group-address provided is not within range, when the given group-address is not having the correct host portion wrt mask or when the given source-address is either 0.0.0.0 or 255.255.255.255, error messages are displayed.
- The **no** form of this command removes the previously configured static-ssm mapping in the system and is a global command. This command will remove the previously configured mapping even when the switch is working in IGMPv1/v2 mode and when the group address is not configured in PIM-SSM group address. After this, the IGMPv1/v2 reports will not be mapped to any source address.

Examples

```
-> ip multicast static-ssm-map group 232.1.1.0/24 source 5.5.5.5
```

Release History

Release 6.4.5; command introduced.

Related Commands

ip multicast version	Sets the default version of the IGMP protocol on the specified VLAN or on the system if no VLAN is specified.
ip pim ssm group	Statically maps the specified IP multicast group(s) to the PIM Source Specific Multicast mode (SSM).
show ip multicast static-ssm-map	Displays the configured static-ssm group and source mapping in the system.
show ip multicast	Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alcatelIND1IgmpMIB
   alaIgmpStaticSsmMapGrpAddressType
   alaIgmpStaticSsmMapGrpAddress
   alaIgmpStaticSsmMapSrcAddressType
   alaIgmpStaticSsmMapSrcAddress
   alaIgmpStaticSsmMapGrpPrefixLength
   alaIgmpStaticSsmMapRowStatus
```

show ip multicast static-ssm-map

Displays the configured static-ssm group and source mapping in the system.

show ip multicast static-ssm-map

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show ip multicast static-ssm-map
Group Address/Prefix Source Address
--------------------+---------------
232.1.1.0/24         5.5.5.5
232.4.4.4/32         2.2.2.2
```

Release History

Release 6.4.5; command introduced.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.
show ip pim ssm group	Displays the static configuration of multicast group mappings for the PIM-Source Specific Multicast (SSM) mode.

MIB Objects

```
alcatelIND1IgmpMIB
   alaIgmpStaticSsmMapGrpAddressType
   alaIgmpStaticSsmMapGrpAddress
   alaIgmpStaticSsmMapSrcAddressType
   alaIgmpStaticSsmMapSrcAddress
   alaIgmpStaticSsmMapGrpPrefixLength
   alaIgmpStaticSsmMapRowStatus
```

show ip multicast

Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

show ip multicast [vlan *vid***]**

Syntax Definitions

vid	VLAN ID number (1–4094).

Defaults

By default the status and general configuration parameters for the system.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

Specify a VLAN ID to display the configuration information for an individual VLAN.

Examples

```
-> show ip multicast

Status:                                      Enabled
Querying:                                    Disabled
Proxying                                    Disabled
Spoofing:                                    Disabled
Zapping:                                     Disabled
Querier Forwarding:                          Disabled
Version:                                     2
Robustness:                                  2
Query Interval (seconds):                    125
Query Response Interval (tenths of seconds):  100
Last Member Query Interval(tenths of seconds):10
Unsolicited Report Interval(seconds):        1
Router Timeout (seconds):                    90
Source Timeout (seconds):                    30
Max-group:                                   10,
Max-group action:                            replace
Helper-address                              10.1.1.198
Lookup Mode                                 source-group
```

```
-> show ip multicast vlan 10

Status:                                          Enabled
Querying:                                        Disabled
Proxying                                        Disabled
Spoofing:                                        Disabled
Zapping:                                         Disabled
Querier Forwarding:                              Disabled
Version:                                         2
Robustness:                                      2
Query Interval (seconds):                        125
Query Response Interval (tenths of seconds):  100
Last Member Query Interval(tenths of seconds):10
Unsolicited Report Interval(seconds):        1
Router Timeout (seconds):                        90
Source Timeout (seconds):                        30
Max-group:                                       0,
Max-group action:                                none
```

Output fields are described here:

output definitions

Status	Whether the IP Multicast Switching and Routing is **Enabled** or **Disabled** (the default status).You can enable or disable IP Multicast Switching and Routing with the **ip multicast status** command, which is described on page 32-4.
Querying	The current state of IGMP querying, which can be **Enabled** or **Disabled** (the default status). You can enable or disable IGMP querying with the **ip multicast querying** command, which is described on page 32-35.
Proxying	The current state of IGMP proxying on the system, which can be **Enabled** or **Disabled** (the default status)**.** You can enable or disable IGMP spoofing with the **ip multicast proxying** command, which is described on page 32-43.
Spoofing	The current state of IGMP spoofing on the system, which can be **Enabled** or **Disabled** (the default status)**.** You can enable or disable IGMP spoofing with the **ip multicast spoofing** command, which is described on page 32-39.
Zapping	The current state of IGMP zapping on the system, which can be **Enabled** or **Disabled** (the default status)**.** You can enable or disable IGMP zapping with the **ip multicast zapping** command, which is described on page 32-41.
Querier Forwarding	The current state of IGMP querier forwarding on the system, which can be **Enabled** or **Disabled** (the default status)**.** You can enable or disable IGMP Querier forwarding with the **ip multicast querier-forwarding** command, which is described on page 32-7.
Version	Displays the default IGMP version, which can be **1, 2** or **3**. Use the **ip multicast version** command to modify this parameter.
Robustness	Displays the IGMP robustness value, ranging from **1** to **7.** (The default value is 2). Use the **ip multicast robustness** command to modify this parameter.

output definitions

Query Interval (seconds)	Displays the time (in seconds) between IGMP queries. (The default value is 125 seconds). You can modify this parameter with the **ip multicast query-interval** command, which is described on page 32-23.
Query Response Interval (tenths of seconds)	Displays the time (in tenths of seconds) taken to reply to an IGMP query message. (The default value is 100 tenths-of-seconds). You can modify this parameter with the **ip multicast query-response-interval** command, which is described on page 32-27.
Last Member Query Interval (tenths of seconds)	Displays the time (in tenths of seconds) taken to reply to an IGMP query message sent in response to a leave group message. (The default value is 10 tenths-of-seconds.) You can modify this parameter with the **ip multicast last-member-query-interval** command, which is described on page 32-25.
Unsolicited Report Interval (seconds)	Displays the time period (in seconds) to proxy any changed IGMP membership state. (The default value is 1 second). You can modify this parameter with the **ip multicast unsolicited-report-interval** command, which is described on page 32-29.
Router Timeout (seconds)	Displays the IGMP router timeout in seconds. (The default value is 90 seconds.) You can modify this parameter with the **ip multicast router-timeout** command, which is described on page 32-31.
Source Timeout (seconds)	Displays the IGMP source timeout in seconds. (The default value is 30 seconds.) You can modify this parameter with the **ip multicast source-timeout** command, which is described on page 32-33.
Max-group	The global or VLAN specific maximum group count allowed.
Max-group action	The action to be taken when the group membership limit is exceeded.
Helper-address	Displays the configured helper address. Use the **ip multicast helper-address** command to modify this parameter, which is described on page 32-45.

Release History

Release 6.1.1; command was introduced.
Release 6.3.1; **Querier Forwarding** field added.
Release 6.3.4; **Max-group and Max-group action** field added.
Release 6.4.2; **Helper-address** field added.

.

Related Commands

ip multicast status	Enables or disables IP Multicast Switching and Routing on the specified VLAN, or on the system if no VLAN is specified.
ip multicast helper-address	Sets the ip address of relay host on the system.
ip multicast version	Sets the default version of the IGMP protocol on the specified VLAN or on the system if no VLAN is specified.
ip multicast querying	Enables or disables IGMP querying on the specified VLAN or on the system if no VLAN is specified.
ip multicast robustness	Sets the IGMP robustness variable on the specified VLAN or on the system if no VLAN is specified.
ip multicast spoofing	Enables or disables IGMP spoofing on the specified VLAN or on the system if no VLAN is specified.
ip multicast zapping	Enables or disables IGMP zapping on the specified VLAN or on the system if no VLAN is specified.
ip multicast proxying	Enables or disables IGMP proxying on the specified VLAN or on the system if no VLAN is specified.
ip multicast query-interval	Sets the IGMP query interval on the specified VLAN or on the system if no VLAN is specified.
ip multicast last-member-query-interval	Sets the IGMP last member query interval value on the specified VLAN or on the system if no VLAN is specified.
ip multicast query-response-interval	Sets the IGMP query response interval on the specified VLAN or on the system if no VLAN is specified.
ip multicast unsolicited-report-interval	Sets the value of the IGMP unsolicited report interval on the specified VLAN or on the system if no VLAN is specified.
ip multicast router-timeout	Configures the expiry time of IP multicast routers on the specified VLAN or on the system if no VLAN is specified.
ip multicast source-timeout	Configures the expiry time of IP multicast sources on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaIgmp
   alaIgmpStatus
   alaIgmpQuerying
   alaIgmpProxying
   alaIgmpSpoofing
   alaIgmpZapping
   alaIgmpQuerierForwarding
   alaIgmpHelperAddressType
   alaIgmpHelperAddress
   alaIgmpVersion
   alaIgmpRobustness
   alaIgmpQueryInterval
   alaIgmpQueryResponseInterval
   alaIgmpLastMemberQueryInterval
   alaIgmpUnsolicitedReportInterval
   alaIgmpRouterTimeout
   alaIgmpSourceTimeout
```

```
alaIgmpVlan
   alaIgmpVlanStatus
   alaIgmpVlanQuerying
   alaIgmpVlanProxying
   alaIgmpVlanSpoofing
   alaIgmpVlanZapping
   alaIgmpVlanQuerierForwarding
   alaIgmpVlanVersion
   alaIgmpVlanRobustness
   alaIgmpVlanQueryInterval
   alaIgmpVlanQueryResponseInterval
   alaIgmpVlanLastMemberQueryInterval
   alaIgmpVlanUnsolicitedReportInterval
   alaIgmpVlanRouterTimeout
   alaIgmpVlanSourceTimeout
```

show ip multicast port

Displays the max-group configuration applicable for all port or vlan instances of a given port or all ports. The current number of groups learnt on a given port or vlan instance will also be displayed.

show ip multicast port [*slot/port*]

Syntax Definitions

slot | *port*	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3)).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

Specify a slot and port number to display the configuration information for a specific switch port.

Examples

```
-> show ip multicast port
Legends: Port Max-group      = Max-group limit on the port
         Port Action         = Max-group action on the port
         Port-VLAN Max-group = Active Max-group limit on the Port-Vlan instance
         Port-VLAN Action    = Active Max-group action on the Port-Vlan instance

Total 18 Port-Vlan Pairs

Rem - remote port
Port  VLAN  Current Igmp    Port      Port    Port-VLAN  Port-VLAN
            Groups        Max-group  Action   Max-group  Action
-----+-----+-------------+----------+--------+----------+--------
1/1    10   2             0          none     0          none
1/3    20   0             0          none     0          none
1/6    1    0             0          none     0          none
Rem    4094 0             0          none     0          none
Rem    30   0             0          none     0          none
Rem    20   0             0          none     0          none
Rem    10   2             0          none     0          none
Rem    1    0             0          none     0          none
Rem    4094 0             0          none     0          none
Rem    30   0             0          none     0          none
Rem    20   0             0          none     0          none
Rem    10   0             0          none     0          none
Rem    1    0             0          none     0          none
3/5    1    0             0          none     0          none
3/9    1    0             0          none     0          none
5/5    1    0             0          none     0          none
5/6    1    0             0          none     0          none
```

```
5/9    1    0             0          none     0          none

-> show ip multicast port 1/24
Port  VLAN  Current Igmp    Port      Port    Port-VLAN  Port-VLAN
            Groups        Max-group  Action   Max-group  Action
-----+-----+-------------+----------+--------+----------+--------
1/24   172  0             0          none     0          none

Max-group 0 Action none
```

output definitions

Port	The slot and port number of the IP multicast port. **Rem** indicates that a new member, neighbour, querier or source on VFL port is discovered.
VLAN	The VLAN associated with the IP multicast port.
Current Groups	The current group associated with the IP Current groups.
IGMP	The IGMP associated with the IP multicast port.
Port Max-group	The maximum group count allowed on the port.
Port Action	The maximum group action allowed on the port.
Port-VLAN Max-group	Active Max-group limit on the Port-Vlan instance
Port-VLAN action	The action to be taken when the group membership limit is exceeded.

Release History

Release 6.3.4; command was introduced.
Release 6.4.5; Status of **Rem** added.

Related Commands

ip multicast status	Enables or disables IP Multicast Switching and Routing on the specified VLAN, or on the system if no VLAN is specified.
ip multicast version	Sets the default version of the IGMP protocol on the specified VLAN or on the system if no VLAN is specified.
ip multicast querying	Enables or disables IGMP querying on the specified VLAN or on the system if no VLAN is specified.
ip multicast robustness	Sets the IGMP robustness variable on the specified VLAN or on the system if no VLAN is specified.
ip multicast spoofing	Enables or disables IGMP spoofing on the specified VLAN or on the system if no VLAN is specified.
ip multicast zapping	Enables or disables IGMP zapping on the specified VLAN or on the system if no VLAN is specified.
ip multicast proxying	Enables or disables IGMP proxying on the specified VLAN or on the system if no VLAN is specified.
ip multicast query-interval	Sets the IGMP query interval on the specified VLAN or on the system if no VLAN is specified.
ip multicast last-member-query-interval	Sets the IGMP last member query interval value on the specified VLAN or on the system if no VLAN is specified.
ip multicast query-response-interval	Sets the IGMP query response interval on the specified VLAN or on the system if no VLAN is specified.
ip multicast unsolicited-report-interval	Sets the value of the IGMP unsolicited report interval on the specified VLAN or on the system if no VLAN is specified.
ip multicast router-timeout	Configures the expiry time of IP multicast routers on the specified VLAN or on the system if no VLAN is specified.
ip multicast source-timeout	Configures the expiry time of IP multicast sources on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaIgmpPortTable
   alaIgmpPortMaxGroupLimit
   alaIgmpPortMaxGroupExceedAction
alaIgmpPortVlanTable
   alaIgmpPortVlanCurrentGroupCount
   alaIgmpPortVlanMaxGroupLimit
   alaIgmpPortVlanMaxGroupExceedAction
```

show ip multicast forward

Displays the IP Multicast Switching and Routing forwarding table entries for the specified IP multicast group address or all the entries if no IP multicast group address is specified.

show ip multicast forward [*ip_address***]**

Syntax Definitions

ip_address	IP multicast group address.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show ip multicast forward

Total 4 Forwards

Rem - remote port
                                                Ingress     Egress
Group Address   Host Address    Tunnel Address  VLAN  Port  VLAN  Port  RVLAN
---------------+---------------+---------------+-----+-----+-----+-----+------
225.1.1.1       50.10.10.123    0.0.0.0          20   1/3    10   105   -
225.1.1.1       50.10.10.123    0.0.0.0          20   1/3    20   128   -
225.1.1.2       50.10.10.123    0.0.0.0          20   1/3    10   105   -
225.1.1.2       50.10.10.123    0.0.0.0          20   1/3    20   128   -

-> show ip multicast forward 228.0.0.1

                                                  Ingress     Egress
Group Address   Host Address    Tunnel Address  VLAN   Port  VLAN  Port   RVALN
---------------+---------------+---------------+-----+-----+-----+------+--------
228.0.0.1       1.0.0.2         0.0.0.0          1     Rem    1    2/23    20
```

Output fields are described here:

output definitions

Group Address	IP group address of the IP multicast forward.
Host Address	IP host address of the IP multicast forward.
Tunnel Address	IP source tunnel address of the IP multicast forward.
VLAN	VLAN associated with the IP multicast forward.

output definitions (continued)

Port	The slot and port number of the IP multicast forward. **Rem** indicates that a new member, neighbour, querier or source on VFL port is discovered.
RVLAN	Displays the receiver VLAN association with the receiver port.

Release History

Release 6.1.1; command was introduced.
Release 6.4.5; **Rem** status and **RVLAN** added in output.

Related Commands

ip multicast static-group	Creates a static IGMP group entry on a specified port on a specified VLAN.

MIB Objects

```
alaIgmpForwardTable
   alaIgmpForwardVlan
   alaIgmpForwardIfIndex
   alaIgmpForwardGroupAddress
   alaIgmpForwardHostAddress
   alaIgmpForwardDestAddress
   alaIgmpForwardOrigAddress
   alaIgmpForwardType
   alaIgmpForwardNextVlan
   alaIgmpForwardNextIfIndex
   alaIgmpForwardNextTunnelAddress
   alaIgmpForwardNextType
   alaIgmpForwardTtl
```

show ip multicast neighbor

Displays the IGMP neighbor table entries of IP Multicast Switching and Routing.

show ip multicast neighbor

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show ip multicast neighbor

Total 5 Neighbors

Rem - remote port
Host Address    VLAN  Port  Static  Count  Life
---------------+-----+-----+-------+------+-----
10.10.10.106     10   Rem   no      490    98
20.10.10.107     20   1/3   no      488    77
20.10.10.106     20   Rem   no      491    99
30.10.10.106     30   Rem   no      491    99
30.10.10.107     30   Rem   no      980    78
```

Output fields are described here:

output definitions

Host Address	The IP address of the IP multicast neighbor.
VLAN	The VLAN associated with the IP multicast neighbor.
Port	The slot and port number of the IP multicast neighbor. **Rem** indicates that a new member, neighbour, querier or source on VFL port is discovered.
Static	Whether it is a static IP multicast neighbor or not.
Count	Displays the count of IP multicast neighbor.
Life	The life time of the IP multicast neighbor.

Release History

Release 6.1.1; command was introduced.
Release 6.4.5; **Rem** status added in ouput

Related Commands

ip multicast static-neighbor	Creates a static IGMP neighbor entry on a specified port on a specified VLAN.

MIB Objects

```
alaIgmpNeighborTable
   alaIgmpNeighborVlan
   alaIgmpNeighborIfIndex
   alaIgmpNeighborHostAddress
   alaIgmpNeighborCount
   alaIgmpNeighborTimeout
   alaIgmpNeighborUpTime
alaIgmpStaticNeighborTable
   alaIgmpStaticNeighborVlan
   alaIgmpStaticNeighborIfIndex
   alaIgmpStaticNeighborRowStatus
```

show ip multicast querier

Displays the IGMP querier table entries of IP Multicast Switching and Routing.

show ip multicast querier

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show ip multicast querier

Total 3 Queriers

Rem - remote port
Host Address    VLAN  Port  Static  Count  Life
---------------+-----+-----+-------+------+-----
10.10.10.105     10   CPU   no      0      77
20.10.10.105     20   CPU   no      0      15
30.10.10.105     30   CPU   no      0      81
```

Output fields are described here:

output definitions

Host Address	The IP address of the IP multicast querier.
VLAN	The VLAN associated with the IP multicast querier.
Port	The slot and port number of the IP multicast querier. **Rem** indicates that a new member, neighbour, querier or source on VFL port is discovered.
Static	Whether it is a static multicast neighbor or not.
Count	Displays the count of the IP multicast querier.
Life	The life time of the IP multicast querier.

Release History

Release 6.1.1; command was introduced.
Release 6.4.5; **Rem** status added in output.

Related Commands

ip multicast static-querier	Creates a static IGMP querier entry on a specified port on a specified VLAN.

MIB Objects

```
alaIgmpQuerierTable
   alaIgmpQuerierVlan
   alaIgmpQuerierIfIndex
   alaIgmpQuerierHostAddress
   alaIgmpQuerierCount
   alaIgmpQuerierTimeout
   alaIgmpQuerierUpTime
alaIgmpStaticQuerierTable
   alaIgmpStaticQuerierVlan
   alaIgmpStaticQuerierIfIndex
   alaIgmpStaticQuerierRowStatus
```

show ip multicast group

Displays the IGMP group membership table entries of IP Multicast Switching and Routing for the specified IP multicast group address or all entries if no IP multicast group address is specified. It also displays the receiver VLAN association with the receiver port.

show ip multicast group [*ip_address***]**

Syntax Definitions

ip_address	IP multicast group address.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show ip multicast group

Total 3 Groups
Group Address   Source Address  VLAN  Port  Mode     Static  Count  Life  RVLAN
---------------+---------------+-----+-----+--------+-------+------+-----+-----
231.0.0.3       1.0.0.5         1     2/1   exclude  no      1      257    20
234.0.0.4       0.0.0.0         1     Rem   exclude  no      1      218
229.0.0.1       0.0.0.0         1     2/13  exclude  yes     0      0

-> show ip multicast group 234.0.0.4

Group Address   Source Address  VLAN  Port  Mode     Static  Count  Life   RVLAN
---------------+---------------+-----+-----+--------+-------+------+-----+-------
234.0.0.4       0.0.0.0         1     Rem   exclude  no      1      218
```

Output fields are described here:

output definitions

Group Address	IP address of the IP multicast group.
Source Address	IP address of the IP multicast source.
VLAN	The VLAN associated with the IP multicast group.
Port	The slot and port number of the IP multicast group. **Rem** indicates that a new member, neighbour, querier or source on VFL port is discovered.
Mode	IGMP source filter mode.

output definitions

Static	Whether it is a static multicast group or not.
Count	Number of IGMP membership requests made.
Life	Life time of the IGMP group membership.
RVLAN	Displays the receiver VLAN association with the receiver port.

Release History

Release 6.1.1; command was introduced.
Release 6.4.5; **Rem** status and **RVLAN** added in output.

Related Commands.

ip multicast static-group	Creates a static IGMP group entry on a specified port on a specified VLAN.

MIB Objects

```
alaIgmpMemberTable
   alaIgmpMemberVlan
   alaIgmpMemberIfIndex
   alaIgmpMemberGroupAddress
   alaIgmpMemberSourceAddress
   alaIgmpMemberMode
   alaIgmpMemberCount
   alaIgmpMemberTimeout
alaIgmpStaticMemberTable
   alaIgmpStaticMemberVlan
   alaIgmpStaticMemberIfIndex
   alaIgmpStaticMemberGroupAddress
   alaIgmpStaticMemberRowStatus
```

show ip multicast source

Displays the IP Multicast Switching and Routing source table entries matching the specified IP multicast group address or all entries if no IP multicast group address is specified.

show ip multicast source [*ip_address***]**

Syntax Definitions

ip_address	IP multicast group address.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show ip multicast source

Total 1 Sources
Rem - remote port
Group Address   Host Address    Tunnel Address  VLAN  Port
---------------+---------------+---------------+-----+-----
225.1.1.1       50.10.10.123    0.0.0.0          20   1/3
225.1.1.2       50.10.10.123    0.0.0.0          20   1/3

-> show ip multicast source 228.0.0.1

Total 2 Sources
Group Address   Host Address    Tunnel Address  VLAN  Port
---------------+---------------+---------------+-----+-----
228.0.0.1       1.0.0.2         0.0.0.0         1     2/1
```

output definitions

Group Address	IP group address of the IP multicast source.
Host Address	IP host address of the IP multicast source.
Tunnel Address	IP destination tunnel address of the IP multicast source.
VLAN	VLAN associated with the IP multicast source.
Port	The slot and port number of the IP multicast source. **Rem** indicates that a new member, neighbour, querier or source on VFL port is discovered.

Release History

Release 6.1.1; command was introduced.
Release 6.4.5; **Rem** status added in output.

Related Commands

show ip multicast tunnel	Display the IP Multicast Switching and Routing tunneling table entries matching the specified IP multicast group address or all entries if no IP multicast address is specified.

MIB Objects

```
alaIgmpSourceTable
   alaIgmpSourceVlan
   alaIgmpSourceIfIndex
   alaIgmpSourceGroupAddress
   alaIgmpSourceHostAddress
   alaIgmpSourceDestAddress
   alaIgmpSourceOrigAddress
   alaIgmpSourceType
   alaIgmpSourceUpTime
```

show ip multicast tunnel

Display the IP Multicast Switching and Routing tunneling table entries matching the specified IP multicast group address or all entries if no IP multicast address is specified.

show ip multicast tunnel [address]

Syntax Definitions

address	IP multicast group address.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show ip multicast tunnel
Total 1 Tunnels

Rem - remote port
                                                 Ingress
Group Address   Host Address    Tunnel Address  VLAN  Port
--------------+---------------+---------------+-----+-----
228.0.0.1       1.0.0.2         2.1.2.3         1     Rem
```

output definitions

Group Address	IP group address of the IP multicast tunnel.
Host Address	IP host address of the IP multicast tunnel.
Tunnel Address	IP source tunnel address of the IP multicast tunnel.
VLAN	VLAN associated with the IP multicast tunnel.
Port	The slot and port number of the IP multicast source. **Rem** indicates that a new member, neighbour, querier or source on VFL port is discovered.

Release History

Release 6.1.1; command was introduced.
Release 6.4.5; **Rem** status added in output.

show ipv6 multicast

Displays the IPv6 Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

show ipv6 multicast [vlan *vid***]**

Syntax Definitions

vid	VLAN for which to display the configuration.

Defaults

By default the status and general configuration parameters for the system.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

Specify a VLAN ID to display the configuration information for an individual VLAN.

Examples

```
-> show ipv6 multicast vlan 100

Status:                                          = Enabled
Querying:                                        = Disabled
Proxying:                                       = Disabled
Spoofing:                                        = Disabled
Zapping:                                         = Disabled
Querier Forwarding:                              = Disabled
Version:                                         = 1
Robustness:                                      = 2
Query Interval (seconds):                        = 125
Query Response Interval (milliseconds):          = 10000
Last Member Query Interval (milliseconds):       = 1000
Unsolicited Report Interval (seconds)            = 1,
Router Timeout (seconds):                        = 90
Source Timeout (seconds):                        = 30
Max-group                                         = 5,
Max-group action                                  = drop
```

```
-> show ipv6 multicast vlan 100

Status:                                          = Enabled
Querying:                                        = Disabled
Proxying:                                        = Disabled
Spoofing:                                        = Disabled
Zapping:                                         = Disabled
Querier Forwarding:                              = Disabled
Version:                                         = 1
Robustness:                                      = 2
Query Interval (seconds):                        = 125
Query Response Interval (milliseconds):          = 10000
Last Member Query Interval (milliseconds):       = 1000
Unsolicited Report Interval (seconds)            = 1,
Router Timeout (seconds):                        = 90
Source Timeout (seconds):                        = 30:
Max-group                                         = 23,
Max-group action                                  = none
```

output definitions

Status	Whether the IPv6 Multicast Switching and Routing is **Enabled** or **Disabled** (the default status).You can enable or disable IPv6 Multicast Switching and Routing with the **ip multicast helper-address** command, which is described on page 32-45
Querying	The current state of MLD querying, which can be **Enabled** or **Disabled** (the default status). You can enable or disable MLD querying with the **ipv6 multicast querying** command, which is described on page 32-76
Proxying	The current state of MLD proxying on the system, which can be **Enabled** or **Disabled** (the default status)**.** You can enable or disable MLD spoofing with the **ipv6 multicast proxying** command, which is described on page 32-84
Spoofing	The current state of MLD spoofing on the system, which can be **Enabled** or **Disabled** (the default status)**.** You can enable or disable MLD spoofing with the **ipv6 multicast spoofing** command, which is described on page 32-39
Zapping	The current state of MLD zapping on the system, which can be **Enabled** or **Disabled** (the default status)**.** You can enable or disable MLD zapping with the **ipv6 multicast zapping** command, which is described on page 32-82
Querier Forwarding	The current state of MLD querier forwarding on the system, which can be **Enabled** or **Disabled** (the default status)**.** You can enable or disable MLD Querier forwarding with the **ipv6 multicast querier-forwarding** command, which is described on page 32-48.
Version	Displays the default MLD version, which can be **1, 2** or **3**. Use the **ipv6 multicast version** command to modify this parameter.
Robustness	Displays the MLD robustness value, ranging from **1** to **7**. Use the **ipv6 multicast robustness** command to modify this parameter.
Query Interval (seconds)	Displays the time (in seconds) between MLD queries. (The default value is 125 seconds). You can modify this parameter with the **ipv6 multicast query-interval** command, which is described on page 32-64.

output definitions

Query Response Interval (milliseconds)	Displays the time (in milliseconds) to reply to an MLD query message. (The default value is 10000 milliseconds.) You can modify this parameter with the **ipv6 multicast query-response-interval** command, which is described on page 32-68.
Last Member Query Interval (milliseconds)	Displays the time (in milliseconds) to reply to an MLD query message sent in response to a leave group message. (The default value is 1000 milliseconds.) You can modify this parameter with the **ipv6 multicast last-member-query-interval** command, which is described on page 32-66.
Unsolicited Report Interval (seconds)	Displays the time period (in seconds) to proxy any changed MLD membership state. (The default value is 1 second). You can modify this parameter with the **ipv6 multicast unsolicited-report-interval** command, which is described on page 32-70.
Router Timeout (seconds)	Displays the MLD router timeout in seconds (The default value is 90 seconds.) You can modify this parameter with the **ipv6 multicast router-timeout** command, which is described on page 32-72
Source Timeout (seconds)	Displays the IGMP source timeout in seconds (The default is 30 seconds.) You can modify this parameter with the **ipv6 multicast source-timeout** command, which is described on page 32-74
Max-group	The global or VLAN specific maximum group count allowed.
Max-group action	The action to be taken when the group membership limit is exceeded.

Release History

Release 6.1.1; command was introduced.
Release 6.3.1; **Querier Forwarding** field added.
Release 6.3.4; **Max-group and Max-group action** field added.

Related Commands

ipv6 multicast status	Enables or disables IPv6 Multicast Switching and Routing on the specified VLAN or on the system if no VLAN is specified.
ipv6 multicast version	Sets the default version of the MLD protocol on the specified VLAN or on the system if no VLAN is specified.
ipv6 multicast query-interval	Sets the MLD query interval on the specified VLAN or on the system if no VLAN is specified.
ipv6 multicast last-member-query-interval	Sets the MLD last member query interval on the specified VLAN or on the system if no VLAN is specified.
ipv6 multicast query-response-interval	Sets the MLD query response interval on the specified VLAN or on the system if no VLAN is specified.
ipv6 multicast unsolicited-report-interval	Sets the MLD unsolicited report interval on the specified VLAN or on the system if no VLAN is specified.
ipv6 multicast router-timeout	Configures the expiry time of IPv6 multicast routers on the specified VLAN or on the system if no VLAN is specified.
ipv6 multicast source-timeout	Configures the expiry time of IPv6 multicast sources on the specified VLAN or on the system if no VLAN is specified.
ipv6 multicast querying	Enables or disables MLD querying on the specified VLAN or on the system if no VLAN is specified.
ipv6 multicast robustness	Sets the MLD robustness variable on the specified VLAN or on the system if no VLAN is specified.
ipv6 multicast spoofing	Enables or disables MLD spoofing on the specified VLAN or on the system if no VLAN is specified.
ipv6 multicast zapping	Enables or disables MLD zapping on the specified VLAN or on the system if no VLAN is specified.
ipv6 multicast proxying	Enables or disables MLD proxying on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaMld
   alaMldStatus
   alaMldQuerying
   alaMldProxying
   alaMldSpoofing
   alaMldZapping
   alaMldQuerierForwarding
   alaMldVersion
   alaMldRobustness
   alaMldQueryInterval
   alaMldQueryResponseInterval
   alaMldLastMemberQueryInterval
   alaMldUnsolicitedReportInterval
   alaMldRouterTimeout
   alaMldSourceTimeout
   alaMldHelperInterfaceIndex
alaMldVlan
   alaMldVlanStatus
   alaMldVlanQuerying
```

```
alaMldVlanProxying
alaMldVlanSpoofing
alaMldVlanZapping
alaMldVlanQuerierForwarding
alaMldVlanVersion
alaMldVlanRobustness
alaMldVlanQueryInterval
alaMldVlanQueryResponseInterval
alaMldVlanLastMemberQueryInterval
alaMldVlanUnsolicitedReportInterval
alaMldVlanRouterTimeout
alaMldVlanSourceTimeout
```

show ipv6 multicast port

Display the max-group configuration applicable for all port or vlan instances of a given port or all ports. The current number of groups learnt on a given port or vlan instance will also be displayed in this show output.

show ipv6 multicast port [*slot/port*]

Syntax Definitions

slot | *port*	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

Specify a VLAN ID to display the configuration information for an individual VLAN.

Examples

```
-> show ipv6 multicast port 1/6
Max-group 9 Action replace

Total 1 Port-Vlan Pairs
  Port   VLAN  Current Mld  Max-group   Action
                  Groups
-------+-----+-------------+----------+---------
    1/6    15             5           0     none
```

Output fields are described here:

output definitions

Port	The slot and port number of the IP multicast port.
VLAN	The VLAN associated with the IP multicast port.
Current Groups	The current group associated with the IP Current groups.
IGMP	The IGMP associated with the IP multicast port.
Max-group	The maximum group count allowed on the port.
Action	The action to be taken when the group membership limit is exceeded.

Release History

Release 6.3.4; command was introduced.

Related Commands

ip multicast status	Enables or disables IP Multicast Switching and Routing on the specified VLAN, or on the system if no VLAN is specified.
ip multicast version	Sets the default version of the IGMP protocol on the specified VLAN or on the system if no VLAN is specified.
ip multicast querying	Enables or disables IGMP querying on the specified VLAN or on the system if no VLAN is specified.
ip multicast robustness	Sets the IGMP robustness variable on the specified VLAN or on the system if no VLAN is specified.
ip multicast spoofing	Enables or disables IGMP spoofing on the specified VLAN or on the system if no VLAN is specified.
ip multicast zapping	Enables or disables IGMP zapping on the specified VLAN or on the system if no VLAN is specified.
ip multicast proxying	Enables or disables IGMP proxying on the specified VLAN or on the system if no VLAN is specified.
ip multicast query-interval	Sets the IGMP query interval on the specified VLAN or on the system if no VLAN is specified.
ip multicast last-member-query-interval	Sets the IGMP last member query interval value on the specified VLAN or on the system if no VLAN is specified.
ip multicast query-response-interval	Sets the IGMP query response interval on the specified VLAN or on the system if no VLAN is specified.
ip multicast unsolicited-report-interval	Sets the value of the IGMP unsolicited report interval on the specified VLAN or on the system if no VLAN is specified.
ip multicast router-timeout	Configures the expiry time of IP multicast routers on the specified VLAN or on the system if no VLAN is specified.
ip multicast source-timeout	Configures the expiry time of IP multicast sources on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaIgmpPortTable
   alaIgmpPortMaxGroupLimit
   alaIgmpPortMaxGroupExceedAction
alaIgmpPortVlanTable
   alaIgmpPortVlanCurrentGroupCount
   alaIgmpPortVlanMaxGroupLimit
   alaIgmpPortVlanMaxGroupExceedAction
```

show ipv6 multicast forward

Display the IPv6 Multicast Switching and Routing forwarding table entries for the specified IPv6 multicast group address or all entries if no IPv6 multicast address is specified.

show ipv6 multicast forward [*ipv6_ddress***]**

Syntax Definitions

ipv6_ddress	IPv6 multicast group address.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show ipv6 multicast forward

Total 1 Forwards
                                                  Ingress    Egress
Group Address   Host Address    Tunnel Address  VLAN  Port  VLAN  Port
--------------- +---------------+---------------+-----+-----+-----+------
ff05::6         4444::2         ::                1     2/1   1     2/23

-> show ipv6 multicast forward ff05::6

                                                  Ingress     Egress
Group Address   Host Address    Tunnel Address  VLAN  Port  VLAN  Port
--------------- +---------------+---------------+-----+-----+-----+------
ff05::6         4444::2         ::                1     2/1   1     2/23
```

output definitions

Group Address	IPv6 group address of the IPv6 multicast forward.
Host Address	IPv6 host address of the IPv6 multicast forward.
Tunnel Address	IPv6 source tunnel address of the IPv6 multicast forward.
VLAN	VLAN associated with the IPv6 multicast forward.
Port	The slot and port number of the IPv6 multicast forward.

Release History

Release 6.1.1; command was introduced.

Related Commands

ipv6 multicast static-group	Creates a static MLD group entry on a specified port on a specified VLAN.

MIB Objects

```
alaMldForwardTable
   alaMldForwardVlan
   alaMldForwardIfIndex
   alaMldForwardGroupAddress
   alaMldForwardHostAddress
   alaMldForwardDestAddress
   alaMldForwardOrigAddress
   alaMldForwardType
   alaMldForwardNextVlan
   alaMldForwardNextIfIndex
   alaMldForwardNextDestAddress
   alaMldForwardNextType
   alaMldForwardTtl
```

show ipv6 multicast neighbor

Displays the MLD neighbor table entries of IPv6 Multicast Switching and Routing.

show ipv6 multicast neighbor

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show ipv6 multicast neighbor

Total 2 Neighbors
Host Address              VLAN  Port  Static  Count  Life
--------------------------+-----+-----+-------+------+-----
fe80::2a0:ccff:fed3:2853  1     2/1   no      1      6
::                        1     2/13  yes     0      0
```

output definitions

Host Address	The IPv6 address of the IPv6 multicast neighbor.
VLAN	The VLAN associated with the IPv6 multicast neighbor.
Port	The slot and port number of the IPv6 multicast neighbor.
Static	Whether it is a static MLD neighbor or not.
Count	Displays the count of the IPv6 multicast neighbor.
Life	The life time of the IPv6 multicast neighbor.

Release History

Release 6.1.1; command was introduced.

Related Commands

ipv6 multicast static-neighbor	Creates a static MLD neighbor entry on a specified port on a specified VLAN.

MIB Objects

```
alaMldNeighborTable
   alaMldNeighborVlan
   alaMldNeighborIfIndex
   alaMldNeighborHostAddress
   alaMldNeighborCount
   alaMldNeighborTimeout
   alaMldNeighborUpTime
alaMldStaticNeighborTable
   alaMldStaticNeighborVlan
   alaMldStaticNeighborIfIndex
   alaMldStaticNeighborRowStatus
```

show ipv6 multicast querier

Displays the MLD querier table entries of IPv6 Multicast Switching and Routing.

show ipv6 multicast querier

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show ipv6 multicast querier

Total 2 Queriers
Host Address              VLAN  Port  Static  Count  Life
--------------------------+-----+-----+-------+------+-----
fe80::2a0:ccff:fed3:2853  1     2/1   no      1      6
::                        1     2/13  yes     0      0
```

output definitions

Host Address	The IPv6 address of the IPv6 multicast querier.
VLAN	The VLAN associated with the IPv6 multicast querier.
Port	The slot and port number of the IPv6 multicast querier.
Static	Whether it is a static MLD neighbor or not.
Count	Displays the count of the IPv6 multicast querier.
Life	The life time of the IPv6 multicast querier.

Release History

Release 6.1.1; command was introduced

Related Commands

ipv6 multicast static-querier	Creates a static MLD querier entry on a specified port on a specified VLAN.

MIB Objects

```
alaMldQuerierTable
   alaMldQuerierVlan
   alaMldQuerierIfIndex
   alaMldQuerierHostAddress
   alaMldQuerierCount
   alaMldQuerierTimeout
   alaMldQuerierUpTime
alaMldStaticQuerierTable
   alaMldStaticQuerierVlan
   alaMldStaticQuerierIfIndex
   alaMldStaticQuerierRowStatus
```

show ipv6 multicast group

Displays the MLD group membership table entries of IPv6 Multicast Switching and Routing for the specified IPv6 multicast group address or all entries if no IPv6 multicast group address is specified.

show ipv6 multicast group [*ip_address***]**

Syntax Definitions

ip_address	IPv6 multicast group address.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show ipv6 multicast group

Total 3 Groups
Group Address    Source Address  VLAN  Port  Mode     Static  Count  Life
-----------------+---------------+-----+-----+--------+-------+------+-----
ff05::5          ::              1     2/1   exclude  no      1      145
ff05::6          3333::1         1     2/1   exclude  no      1      242
ff05::9          ::              1     2/13  exclude  yes     0      0

-> show ipv6 multicast group ff05::5

Group Address    Source Address  VLAN  Port  Mode     Static  Count  Life
-----------------+---------------+-----+-----+--------+-------+------+-----
ff05::5          ::              1     2/1   exclude  no      1      145
```

output definitions

Group Address	IPv6 address of the IPv6 multicast group.
Source Address	IPv6 address of the IPv6 multicast source.
VLAN	The VLAN associated with the IPv6 multicast group.
Port	The slot and port number of the IPv6 multicast group.
Mode	MLD source filter mode.
Static	Whether it is a static MLD group or not.
Count	Number of MLD membership requests made.
Life	Life time of the MLD group membership.

Related Commands

ipv6 multicast static-group	Creates a static MLD group entry on a specified port on a specified VLAN.

MIB Objects

```
alaMldMemberTable
   alaMldMemberVlan
   alaMldMemberIfIndex
   alaMldMemberGroupAddress
   alaMldMemberSourceAddress
   alaMldMemberMode
   alaMldMemberCount
   alaMldMemberTimeout
   alaMldMemberUpTime
alaMldStaticMemberTable
   alaMldStaticMemberVlan
   alaMldStaticMemberIfIndex
   alaMldStaticMemberGroupAddress
   alaMldStaticMemberRowStatus
```

show ipv6 multicast source

Displays the IPv6 Multicast Switching and Routing source table entries matching the specified IPv6 multicast group address or all entries if no IPv6 multicast group address is specified.

show ipv6 multicast source [*ip_address***]**

Syntax Definitions

ip_address	IPv6 multicast group address.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show ipv6 multicast source

Total 1 Sources
Group Address   Host Address    Tunnel Address  VLAN  Port
---------------+---------------+---------------+-----+-----
ff05::6         4444::2         ::              1     2/1

-> show ipv6 multicast source ff05::6

Total 1 Sources
Group Address   Host Address    Tunnel Address  VLAN  Port
---------------+---------------+---------------+-----+-----
ff05::6         4444::2         ::              1     2/1
```

output definitions

Group Address	IPv6 group address of the IPv6 multicast source.
Host Address	IPv6 host address of the IPv6 multicast source.
Tunnel Address	IPv6 source tunnel address of the IPv6 multicast source.
VLAN	VLAN associated with the IPv6 multicast source.
Port	The slot and port number of the IPv6 multicast source.

Release History

Release 6.1.1; command was introduced.

Related Commands

ipv6 multicast static-group	Creates a static MLD group entry on a specified port on a specified VLAN.

MIB Objects

```
alaMldSourceTable
   alaMldSourceVlan
   alaMldSourceIfIndex
   alaMldSourceGroupAddress
   alaMldSourceHostAddress
   alaMldSourceDestAddress
   alaMldSourceOrigAddress
   alaMldSourceType
   alaMldSourceUpTime
```

show ipv6 multicast tunnel

Displays the IPv6 Multicast Switching and Routing tunneling table entries matching the specified IPv6 multicast group address, or all entries if no IPv6 multicast address is specified.

show ipv6 multicast tunnel [*address***]**

Syntax Definitions

address	IPv6 multicast group address.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show ipv6 multicast tunnel
Total 1 Tunnels
                                                 Ingress
Group Address    Host Address   Tunnel Address  VLAN  Port
----------------+--------------+---------------+-----+-----
ff05::6          4444::2        3333::2         1     2/1
```

output definitions

Group Address	IPv6 group address of the IPv6 multicast tunnel.
Host Address	IPv6 host address of the IPv6 multicast tunnel.
Tunnel Address	IPv6 source tunnel address of the IPv6 multicast tunnel.
VLAN	VLAN associated with the IPv6 multicast tunnel.
Port	The slot and port number of the IPv6 multicast tunnel.

Release History

Release 6.1.1; command was introduced.

33 IP Multicast VLAN Commands

The IP Multicast VLAN (IPMV) is a distribution Multicast VLAN that flows into the customer ports. These distribution VLANs connect to the nearest multicast router and support multicast traffic only. Multicast traffic flows from the distribution VLAN to the customer VLAN and not vice-versa. Customer-generated multicast traffic should flow via the customer VLANs so that the Multicast router can control distribution of this traffic. IPMV feature is invisible to the customer. The customer VLANs can be tagged or untagged.

IPMV works in both the Enterprise environment as well as the VLAN Stacking environment. The ports are separately classified as VLAN Stacking ports or as legacy ports (fixed ports/tagged ports). VLAN Stacking VLAN contains only VLAN Stacking ports as its members, while Normal data VLAN contains normal legacy ports. This ensures that data flow is confined to a single broadcast domain.

MIB information for the IP Multicast VLAN commands is as follows:

Filename: AlcatelIND1IPMV.MIB
Module: Alcatel-IND1-IPM-VLAN-MIB

Filename: AlcatelIND1VlanStacking.MIB
Module: Alcatel-IND1-VLAN-STACKING-MIB

Filename: AlcatelIND1VlanManager.MIB
Module: Alcatel-IND1-VLAN-MGR-MIB

A summary of the available commands is listed here:

VLAN Manager Commands	**vlan ipmvlan**
VLAN Stacking Commands	**vlan ipmvlan ctag** **vlan ipmvlan address** **vlan ipmvlan sender-port** **vlan ipmvlan receiver-port** **show vlan ipmvlan c-tag** **show vlan ipmvlan address** **show vlan ipmvlan port-config** **show ipmvlan port-config**

vlan ipmvlan

Creates an IP Multicast VLAN.

vlan ipmvlan *ipmvlan-id* **[{enable | disable} | [{1x1 | flat} stp {enable | disable}]] [name** *name-string***]**

no vlan ipmvlan *ipmvlan-id* **[-***ipmvlan-id2***]**

Syntax Definitions

ipmvlan-id	Specifies the IP Multicast VLAN number. The valid range is 2–4094.
enable	Enables IPMVLAN.
disable	Disables IPMVLAN.
1x1	Specifies that the switch is running in the 1x1 Spanning Tree mode.
flat	Specifies that the switch is running in the Flat Spanning Tree mode.
stp enable	Enables Spanning Tree for the specified IPMVLAN.
stp disable	Disables Spanning Tree for the specified IPMVLAN.
name-string	Alphanumeric string up to 32 characters. Use quotes around the string if the name contains multiple words with spaces between them (for example, “Alcatel-Lucent VLAN”).
ipmvlan-id2	The last IPMVLAN number in a range of IPMVLANs that you want to configure.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to delete a single or multiple IPMVLANs. If the specified IPMVLAN(s) does not exist, an error message will be displayed.
- If *ipmvlan-id* does not exist or if *ipmvlan-id* exists as VLAN Stacking VLAN or Standard VLAN, an error message will be displayed.
- The default mode of the IPMVLAN is the Enterprise mode.
- If an IPMVLAN is disabled, all the ports bound to an IPMVLAN will be blocked for that VLAN instance.
- A maximum of 256 IPMVLANs can be configured.

Examples

```
-> vlan ipmvlan 1003 name "multicast vlan"
-> vlan ipmvlan 1333 1x1 stp enable name "multicast vlan"
-> no vlan ipmvlan 1003
```

Release History

Release 6.2.1; command was introduced.
Release 6.3.1; support added for entering a range and/or multiple entries of IPMVLANs; **1x1, flat, stp enable,** and **stp disable** parameters added.

Related Commands

show vlan ipmvlan	Displays IPMVLAN information for a specific IPMVLAN or all IPMV-LANs.
show vlan	Displays a list of VLANs and their types configured on the switch.

MIB Objects

```
vlanTable
   vlanNumber
   vlanDescription
   vlanTraffictype
   vlanAdmStatus
   alavlanOperStatus
   alavlanStpStatus
   alavlan1x1StpStatus
   alavlanflatStpStatus
   vlanStatus
```

vlan ipmvlan ctag

Defines the mapping between an IPMVLAN and a customer VLAN ID (c-tag) to be used in the c-tag translation rule.

vlan ipmvlan *ipmvlan-id* **ctag {***ctag* | *ctag1-ctag2***}**

no vlan ipmvlan *ipmvlan-id* **ctag {***ctag* | *ctag1-ctag2***}**

Syntax Definitions

ipmvlan-id	Specifies the IP Multicast VLAN number for which the c-tag is to be assigned.The valid range is 2–4094.
ctag	The customer VLAN ID number is used in the translation rule. The valid range is 1–4094.
ctag1-ctag2	Specifies the range of the customer VLAN ID numbers.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to remove the mapping between the IPMVLAN and the customer VLAN ID.
- If the c-tag is already assigned to another IPMVLAN, the configuration request will fail.
- If you assign a range of c-tags to an IPMVLAN, an error message will be displayed for the c-tags already assigned to the IPMVLAN.
- The command will not work in Enterprise Mode.

Examples

```
-> vlan ipmvlan 1003 ctag 10
-> no vlan ipmvlan 1003 ctag 10
```

Release History

Release 6.2.1; command was introduced.

Related Commands

show vlan ipmvlan c-tag	Displays the customer VLAN IDs associated with a single IP Multicast VLAN or all the configured IP Multicast VLANs.

MIB Objects

```
alaipmvVlanCtagTable
   alaipmvVlanNumber
   alaipmvVlanCtag
   alaipmvVlanCtagRowStatus
```

vlan ipmvlan address

Assigns an IPv4 address, or a range of addresses to an existing IPMVLAN.

vlan ipmvlan *ipmvlan-id* **address {***ipv4addr/prefixlen* | *ipv4addr-ipv4addr* | *ip_address* | **mask** *mask***}**

no vlan ipmvlan *ipmvlan-id* **address {***ipv4addr/prefixlen* | *ipv4addr-ipv4addr* | *ip_address* | **mask** *mask***}**

Syntax Definitions

ipmvlan-id	Specifies the IP Multicast VLAN number to which the IP address will be assigned. The valid range is 2–4094.
ip_address	Specifies a 32-bit IP Multicast address that will be assigned to the IPMVLAN.
/prefixlen	Specifies the Prefix Length of mask.
mask	Specifies the IPv4 address mask.
ipv4addr-ipv4addr	Specifies the IPv4 Multicast address range.

Defaults

parameter	default
prefixlen	32
mask	255.255.255.255

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to disassociate the already assigned IPv4 address from the IPMV-LAN.
- Use optional parameters **mask** or *prefixlen* with this command to assign subnet mask to IPv4 Multicast Group Address.
- IPMVLAN overlapping is allowed. The same address can be assigned to different IPMVLANs as long as the IPMVLANs do not share a common receiver port. (Not supported on OS9000E)
- If you assign a range of addresses containing duplicate addresses already assigned to the IPMVLAN, an error message will be displayed and no addresses will be added from that range.
- The recommended maximum number of addresses to be specified in a range is 256. Larger ranges should be broken up into separate commands. Continguous address ranges entered with separate commands are treated as a single range and should be broken up using the *prefixlen* or *mask* parameters.
- IPv4 multicast group address with longest Prefix Length association takes preference over other IPv4 multicast group address.

- Non-zero host bits are not allowed for the creation of IPv4 addresses with mask/prefix-length. E.g. 225.1.3.4/24 is not allowed; the correct group/mask should be 225.1.3.0/24.
- Optional parameters *Prefixlen* and **mask** are not supported in OS9000E.

Examples

```
-> vlan ipmvlan 1003 address 225.0.0.1
-> vlan ipmvlan 1033 address 226.0.1.0/24
-> vlan ipmvlan 1033 address 226.0.1.0 mask 255.255.255.0
-> vlan ipmvlan 1033 address 224.1.1.7-224.1.1.9
-> no vlan ipmvlan 1003 address 225.0.0.1
-> no vlan ipmvlan 1033 address 226.0.1.0/24
-> no vlan ipmvlan 1033 address 226.0.1.0 mask 255.255.255.0
-> no vlan ipmvlan 1033 address 224.1.1.7-224.1.1.9
```

Release History

Release 6.2.1; command was introduced.
Release 6.3.4; ability to assign the same multicast address to different IPMVLANs was added.
Release 6.4.2; *Prefixlen* and **mask** parameters added.

Related Commands

show vlan ipmvlan address	Displays the IPv4 addresses assigned to single IP Multicast VLAN or all the configured IP Multicast VLANs.

MIB Objects

```
alaipmvVlanIpAddrMaskTable
   alaipmvVlanIpAddrVlanNumber
   alaipmvVlanIpAddrType
   alaipmvVlanIpAddress
   alaipmvVlanIpAddrMaskEntry
   alaipmvVlanIpAddrRowStatus
```

vlan ipmvlan sender-port

Configures a port, a range of ports, an aggregate of ports, or a range of aggregates as sender port for the IP Multicast VLAN. This sender port can receive multicast data for the configured multicast groups.

vlan ipmvlan *ipmvlan-id* **sender-port {port** *slot/port***[**-*port2***]** | **linkagg** *agg_num* **[**-*agg_num2***]}**

no vlan ipmvlan *ipmvlan-id* **sender-port {port** *slot/port***[**-*port2***]** | **linkagg** *agg_num* **[**-*agg_num2***]}**

Syntax Definitions

ipmvlan-id	Specifies the IP Multicast VLAN number to which the port will be attached as a sender port. The valid range is 2–4094.
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).
port2	The last port number in a range of ports that you want to configure on the same slot (e.g, 3/1-4 specifies ports 1-4 on slot 3).
agg_num	The link aggregate ID number (0–31) to be assigned as a sender port to the IPMVLAN.
agg_num2	The last link aggregate ID number in a range of aggregates that you want to configure.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a single port, a range of ports, an aggregate of ports, or a range of aggregates assigned as the sender port(s) for the IPMVLAN.
- Multiple sender ports can be assigned to an IPMVLAN and a port can be configured as a sender port for multiple IPMVLANs.
- In the Enterprise mode, the configuration fails if the port configured as a sender port is not a tagged port, or if the port is an aggregated port (member port of a logical aggregate) or a VLAN Stacking port.
- In the VLAN Stacking mode, the configuration fails if the port configured as a sender port is not a VLAN Stacking port (network port).

Examples

The following command configures the sender port in an Enterprise mode:

```
-> vlan ipmvlan 1003 sender-port port 1/45-50
```

The following commands configure the sender port in the VLAN Stacking mode:

```
-> ethernet-service svlan 1001
-> ethernet-service svlan 1001 nni 1/49
-> ethernet-servicee ipmvlan 1033
-> vlan ipmvlan 1033 sender-port port 1/49
```

Note that in the above example, port 1/49 was first configured as a VLAN Stacking network (NNI) port before it was configured as a sendor port for the IPMVLAN. See the “VLAN Stacking Commands” chapter for more information.

The following command removes the port configured as sender port:

```
-> no vlan ipmvlan 1003 sender-port port 1/50
```

Release History

Release 6.2.1; command was introduced.
Release 6.3.1; support added for entering a range and/or multiple entries of ports and aggregates.

Related Commands

show vlan ipmvlan port-config	Displays the sender and receiver ports for a specific IP Multicast VLAN or all the IP Multicast VLANs.

MIB Objects

```
alaipmvVlanPortTable
   alaipmvVlanPortIPMVlanNumber
   alaipmvVlanPortPortNumber
   alaipmvVlanPortPortType
   alaipmvVlanPortRowStatus
```

vlan ipmvlan receiver-port

Configures a port, a range of ports, or an aggregate of ports as receiver ports for the IP Multicast VLAN and associate receiver VLAN (RVLAN) to receiver port (or a range of receiver ports).

vlan ipmvlan *ipmvlan-id* **receiver-port {port** *slot/port***[**-*port2***]** | **linkagg** *agg_num* **[**-*agg_num2***]} [receiver-vlan** *num***]**

no vlan ipmvlan *ipmvlan-id* **receiver-port {port** *slot/port***[**-*port2***]** | **linkagg** *agg_num* **[**-*agg_num2***]} [receiver-vlan** *num***]**

Syntax Definitions

ipmvlan-id	Specifies the IP Multicast VLAN number to which the port will be attached as a receiver port. The valid range is 2–4094.
slot/port	The slot number for the module and physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
port2	Last port number in a range of ports you want to configure on the same slot (e.g, 3/1-4 specifies ports 1-4 on slot 3).
agg_num	The link aggregate ID number to be assigned as a receiver port to the specified IPMVLAN. The valid range is 0–31.
agg_num2	Last link aggregate ID number in a range of aggregates you want to configure.
receiver-vlan	Receiver VLAN ID. This ID is associated to the receiver port (or a range of receiver ports).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to remove the port assigned as a receiver port for the IPMVLAN.
- A single port can be configured as a receiver port for multiple IPMVLANs as long as the IPMVLANs are not associated with the same address. An IPMVLAN can contain multiple receiver ports.
- In Enterprise mode, receiver vlan should be created as normal vlan in the system and receiver port should be configured as a tagged member of this vlan.
- In E-Service (VLAN stacking) mode, receiver vlan should be created using E-Service receiver vlan CLI before associating with the receiver port.
- The receiver VLAN associated to the receiver port should not have any IP interface configured.
- Use the **no** form of this command to delete the receiver port & receiver vlan association.

Examples

The following commands configure the receiver port in the Enterprise mode:

```
-> vlan ipmvlan 1003 receiver-port port 1/51-60
-> vlan ipmvlan 1033 receiver-port port 1/62
```

The following commands configure the receiver port in the VLAN Stacking mode:

```
-> ethernet-service ipmvlan 1002
-> vlan ipmvlan 1002 receiver-port port 1/1
```

Note that in the above example, port 1/1 was previously configured as a VLAN Stacking user port. See the "VLAN Stacking Commands" chapter for more information.

The following command removes the port configured as a sender port:

```
-> no vlan ipmvlan 1002 receiver-port port 1/1
```

The following example shows the configuration of receiver-vlan with receiver-port and linkagg:

```
-> Vlan ipmvlan 1000 receiver-port port 1/1 receiver-vlan 10
-> Vlan ipmvlan 1000 receiver-port linkagg 1 receiver-vlan 20
```

The following example shows to delete a receiver port association with a receiver vlan:

```
-> no vlan ipmvlan 1000 receiver-port port 1/1 receiver-vlan 10
```

The following example shows to delete a receiver port from an IPMVLAN:

```
-> no vlan ipmvlan 1000 receiver-port port 1/1
```

Release History

Release 6.2.1; command was introduced.
Release 6.4.5; **receiver-vlan** parameter introduced.

Related Commands

show vlan ipmvlan port-config	Displays the sender and receiver ports for a specific IP Multicast VLAN or all the configured IP Multicast VLANs.

MIB Objects

```
alaipmvVlanPortTable
   alaipmvVlanPortIPMVlanNumber
   alaipmvVlanPortPortNumber
   alaipmvVlanPortPortType
   alaipmvVlanPortRowStatus

alaipmvReceiverVlanPortTable

   alaipmvReceiverVlanPortIPMVlanNumber
   alaipmvReceiverVlanPortNumber
   alaipmvReceiverVlanPortRcvrVlanNumber
   alaipmvReceiverVlanPortRowStatus
```

show vlan ipmvlan c-tag

Displays the customer VLAN IDs associated with a single IP Multicast VLAN or all the configured IP Multicast VLANs.

show vlan ipmvlan [*ipmvlan-id***] c-tag**

Syntax Definitions

ipmvlan-id	Specifies the IP Multicast VLAN number. The valid range is 2–4094.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show vlan ipmvlan c-tag

 ipmvlan      ctag
+----------+-------+
  100          10
  100          20
  200          30
```

output definitions

ipmvlan	The numerical IPMVLAN ID.
ctag	The customer VLAN-ID associated with the IPMVLAN.

Release History

Release 6.2.1; command was introduced.

Related Commands

vlan ipmvlan ctag	Defines the mapping between a IPMVLAN and a customer VLAN ID (c-tag) to be used in the c-tag translation rule.

MIB Objects

```
alaipmvVlanCtagTable
   alaipmvVlanNumber
   alaipmvVlanCtag
```

show vlan ipmvlan address

Displays the IPv4 addresses assigned to a single IP Multicast VLAN or all the configured IP Multicast VLANs.

show vlan ipmvlan [*ipmvlan-id***] address [ipv4 | ipv6]**

Syntax Definitions

ipmvlan-id	Specifies the IP Multicast VLAN number. The valid range is 2–4094.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show vlan ipmvlan 10 address
IpAddress              ipAddressType
--------------------+------------------
224.1.1.1               Ipv4
224.1.1.2               Ipv4
224.1.1.3               Ipv4

-> show vlan ipmvlan 10 address ipv4
IpAddress              ipAddressType
--------------------+------------------
224.1.1.1               Ipv4
224.1.1.2               Ipv4
224.1.1.3               Ipv4
224.1.1.7-224.1.1.9     Ipv4

-> show vlan ipmvlan address

   ipmvlan      ipAddress        ipAddressType
+----------+-----------------+------------------+
      100        224.1.2.3        Ipv4
      100        225.1.1.1        Ipv4
      200        224.1.1.2        Ipv4
```

output definitions

ipmvlan	The numerical IPMVLAN ID.

output definitions

ipAddress	The IPv4 address.
ipAddressType	The IP address type.

Release History

Release 6.2.1; command was introduced.

Related Commands

vlan ipmvlan address	Assigns an IPv4 address, or a range of addresses to an existing IPMV-LAN.

MIB Objects

```
alaipmvVlanIpAddrMaskTable
   alaipmvVlanIpAddrVlanNumber
   alaipmvVlanIpAddrType
   alaipmvVlanIpAddress
```

show vlan ipmvlan port-config

Displays the sender ports, receiver ports, and receiver vlan associations for a specific IP Multicast VLAN or all the IP Multicast VLANs.

show vlan ipmvlan [*ipmvlan-id***] port-config**

Syntax Definitions

ipmvlan-id	Specifies the IP Multicast VLAN number for which the sender and receiver ports will be displayed. The valid range is 2–4094.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show vlan ipmvlan port-config
 ipmvlan     port     type      RVLAN
+---------+--------+-----------+--------
    50       2/1     receiver
    50       2/10    sender
    51       2/2     receiver
    51       0/2     receiver
   100       2/2     receiver
   101       0/1     sender

-> show vlan ipmvlan 50 port-config
  port      type      RVLAN
+--------+-----------+-------
  2/1      receiver    20
  2/10     sender      30

-> show vlan ipmvlan 51 port-config
  port      type      RVLAN
+--------+-----------+--------
  2/2      receiver
  0/2      receiver
```

```
-> show vlan ipmvlan 100 port-config
  port      type       RVLAN
+--------+-----------+-------
  2/2      receiver

-> show vlan ipmvlan 101 port-config
  port      type      RVLAN
+--------+-----------+--------
  0/1      sender
```

output definitions

ipmvlan	The numerical IPMVLAN ID.
port	Displays the slot number of the module and the physical port number on that module for which the IPMVLAN is configured.
type	The type (**sender** or **receiver**) of the IPMVLAN port.
RVLAN	Displays the receiver VLAN association with the receiver port.

Release History

Release 6.2.1; command was introduced.
Release 6.3.1; command was modified.
Release 6.4.5; RVLAN added in output.

Related Commands

vlan ipmvlan sender-port	Configures a port or an aggregate of ports as the sender port for the IP Multicast VLAN.
vlan ipmvlan receiver-port	Configures a port (or a range of ports) or an aggregate of ports as the receiver port for the IP Multicast VLAN.

MIB Objects

```
alaipmvVlanPortTable
   alaipmvVlanPortIPMVlanNumber
   alaipmvVlanPortPortNumber
   alaipmvVlanPortPortType
alaipmvReceiverVlanPortTable
   alaipmvReceiverVlanPortIPMVlanNumber
   alaipmvReceiverVlanPortNumber
   alaipmvReceiverVlanPortRcvrVlanNumber
   alaipmvReceiverVlanPortRowStatus
```

show ipmvlan port-config

Displays the sender and receiver IPMVLANs for a specific slot or port.

show vlan ipmvlan port-config [*slot/port* | *agg_num***]**

Syntax Definitions

slot/port	The slot number for the module and physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
agg_num	The Link aggregate ID number. The valid range is 0–31.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show vlan ipmvlan port-config 2/1
  ipmvlan     type
+---------+------------+
    50       receiver

-> show vlan ipmvlan port-config 2/2
  ipmvlan     type
+---------+------------+
    51       receiver
   100       receiver

-> show vlan ipmvlan port-config 1
  ipmvlan     type
+---------+------------+
   101       sender
```

output definitions

ipmvlan	The numerical IPMVLAN ID.
type	The type (**sender** or **receiver**) of the IPMVLAN port.

Release History

Release 6.2.1; command was introduced.
Release 6.3.1; command was modified.

Related Commands

vlan ipmvlan sender-port	Configures a port or an aggregate of ports as the sender port for the IP Multicast VLAN.
vlan ipmvlan receiver-port	Configures a port (or a range of ports) or an aggregate of ports as the receiver port for the IP Multicast VLAN.

MIB Objects

```
alaipmvVlanPortTable
   alaipmvVlanPortIPMVlanNumber
   alaipmvVlanPortPortNumber
   alaipmvVlanPortPortType
```

34 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, and distribution of software, stock quotes, and news services are examples of multicast traffic.

For more information about configuring DVMRP, see the *OmniSwitch AOS Release 6 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 6855, 6850E, 9000E

Usage Guidelines

- This command must be executed before DVMRP can be configured on 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 34-3.
- The advanced routing image must be loaded before the DVMRP feature starts working on the switch.

Examples

```
-> ip load dvmrp
```

Release History

Release 6.1; command was introduced.

Related Commands

ip dvmrp status	Globally enables or disables DVMRP protocol on the switch.

MIB Objects

```
alaDrcTmConfig
   alaDrcTmIPDvmrpStatus
```

ip dvmrp status

Globally enables or disables DVMRP protocol on the switch.

ip dvmrp status {enable | disable}

Syntax Definitions

enable	Administratively enables DVMRP on the switch.
disable	Administratively disables DVMRP on the switch.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6855, 6850E, 9000E

Usage Guidelines

- This command must be set to **enable** before DVMRP can run on the switch. In addition, the **ip load dvmrp** command must be issued. For more information, refer to the **ip load dvmrp** command on page 34-2.
- The advanced routing image must be loaded before the DVMRP feature starts working on the switch.
- To enable or disable DVMRP for a particular interface, refer to the **ip dvmrp interface** command on page 34-7.

Examples

```
-> ip dvmrp status enable
-> ip dvmrp status disable
```

Release History

Release 6.1; command was introduced.

Related Commands

ip dvmrp interface	Enables or disables the DVMRP protocol 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 6855, 6850E, 9000E

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 6.1; 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 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> ip dvmrp graft-timeout 5
```

Release History

Release 6.1; command was introduced.

Related Commands

show ip dvmrp	Displays global DVMRP parameters.

MIB Objects

```
alaDvmrpGlobalConfig
   alaDvmrpGraftRetransmission
```

ip dvmrp interface

Enables or disables the DVMRP protocol on a specified interface.

ip dvmrp interface *interface_name*

no ip dvmrp interface *interface_name*

Syntax Definitions

interface_name	The name of the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 6855, 6850E, 9000E

Usage Guidelines

Use the **no** form of this command to delete an interface.

Examples

```
-> ip dvmrp interface vlan-10
-> no ip dvmrp interface vlan-10
```

Release History

Release 6.1; command was introduced.

Related Commands

ip dvmrp status	Globally enables or disables the DVMRP protocol 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 *interface_name* **metric** *value*

Syntax Definitions

interface_name	The name of the interface.
value	Specifies the metric value (1–31).

Defaults

parameter	default
value	1

Platforms Supported

OmniSwitch 6855, 6850E, 9000E

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 vlan-2 metric 1
```

Release History

Release 6.1; command was introduced.

Related Commands

ip dvmrp interface	Enables or disables the DVMRP protocol 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 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> ip dvmrp neighbor-interval 10
```

Release History

Release 6.1; 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 that 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 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> ip dvmrp neighbor-timeout 35
```

Release History

Release 6.1; 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 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.

ip dvmrp prune-lifetime *seconds*

Syntax Definitions

seconds	Specifies the prune lifetime, in seconds (180–86400).

Defaults

parameter	default
seconds	7200

Platforms Supported

OmniSwitch 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> ip dvmrp prune-lifetime 7200
```

Release History

Release 6.1; command was introduced.

Related Commands

ip dvmrp prune-timeout	Configures the prune packet retransmission value.
show ip dvmrp prune	Displays 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 duration of time 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 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> ip dvmrp prune-timeout 30
```

Release History

Release 6.1; 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 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 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> ip dvmrp report-interval 60
```

Release History

Release 6.1; 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 holddown 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 holddown time, in seconds (1–86400).

Defaults

parameter	default
seconds	120

Platforms Supported

OmniSwitch 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> ip dvmrp route-holddown 120
```

Release History

Release 6.1; 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 holddown 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 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> ip dvmrp route-timeout 140
```

Release History

Release 6.1; 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 6855, 6850E, 9000E

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 34-25.

Examples

```
-> ip dvmrp subord-default false
```

Release History

Release 6.1; 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_name remote_address*

no ip dvmrp tunnel *local_name remote_address*

Syntax Definitions

local_name	The name of the local router interface.
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.

Defaults

N/A

Platforms Supported

OmniSwitch 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to delete a tunnel.
- 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.

Examples

```
-> ip dvmrp tunnel vlan-2 168.22.2.120
-> no ip dvmrp tunnel vlan-2 168.22.2.120
```

-Release History

Release 6.1; command was introduced.

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 *interface_name remote_address* **ttl** *value*

Syntax Definitions

interface_name	The name of the interface.
remote_address	Remote IP address of the tunnel.
value	The Time to Live (TTL) value (0–255).

Defaults

parameter	default
value	255

Platforms Supported

OmniSwitch 6855, 6850E, 9000E

Usage Guidelines

- The local IP address for 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.

Examples

```
-> ip dvmrp tunnel vlan-2 172.22.2.120 ttl 0
```

Release History

Release 6.1; command was introduced.

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 protocol on 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; lower levels will display more basic messages.

Defaults

parameter	default
level	1

Platforms Supported

OmniSwitch 6855, 6850E, 9000E

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 6.1; 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 protocol on the switch, as well as the current status for all debugging types.

MIB Objects

N/A

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 34-22.

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 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this 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 34-22.
- 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 6.1; command was introduced.

Related Commands

ip dvmrp debug-level	Defines the level of debugging for DVMRP protocol on the switch.
show ip dvmrp debug	Displays the current level of debugging for DVMRP protocol on the switch, as well as the current status for all debugging types.

MIB Objects

N/A

show ip dvmrp

Displays the global DVMRP parameters.

show ip dvmrp

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> 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
```

output definitions

DVMRP Admin Status	The current global (i.e., switch-wide) status of DVMRP, which can be **enabled** or **disabled**. To change the current DVMRP global status, refer to the **ip dvmrp status** command on page 34-3.
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.

output definitions (continued)

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.
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 holddown time, in seconds. This value indicates the time during which DVMRP routes are kept in a holddown state. A holddown 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 34-16. Options include true and false. The default value is true.

output definitions (continued)

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 holddown state, and routes that have aged out are not considered reachable.

Release History

Release 6.1; command was introduced.

Related Commands

ip dvmrp status	Globally enables or disables DVMRP protocol on 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 also provides options to display only DVMRP-enabled or DVMRP-disabled interfaces.

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 6855, 6850E, 9000E

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

```
-> 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.
Vlan	The associated VLAN ID.
Tunnel	Indicates whether there is a DVMRP tunnel currently configured on the interface. This field is not relevant for Release 5.3.1 and later.
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 34-7.
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 34-3.

Release History

Release 6.1; command was introduced.

Related Commands

ip dvmrp interface	Enables or disables the DVMRP protocol 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 6855, 6850E, 9000E

Usage Guidelines

If a neighbor IP address is not specified, the entire DVMRP Neighbor Table is displayed.

Examples

```
-> 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 6.1; command was introduced.

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 6855, 6850E, 9000E

Usage Guidelines

If an IP address and IP mask are not specified, the entire DVMRP Next Hop table is displayed.

Examples

```
-> show ip dvmrp nexthop 172.22.2.115 255.255.255.0

Src Address/Mask       Interface Name     Vlan    Hop Type
-------------------+-------------------+-------+----------
172.22.2.115/24       vlan-22              22      branch
```

output definitions

Src 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 6.1; command was introduced.

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 6855, 6850E, 9000E

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 6.1; 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 representing route(s).
ip_mask	A 32-bit number that determines the subnet mask for the IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6855, 6850E, 9000E

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 6.1; 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 6855, 6850E, 9000E

Usage Guidelines

- If optional local and remote IP address information is not specified, 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

```
-> 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. This field is only displayed on OmniSwitch 6850E switch.
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 6.1; command was introduced.

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 protocol on 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 6855, 6850E, 9000E

Usage Guidelines

- The administrative debugging status for message types displayed in the table are determined by the **ip dvmrp debug-type** command on page 34-23.
- To configure debug levels, refer to the **ip dvmrp debug-level** command on page 34-22.

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 34-22.
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 6.1; command was introduced.

Related Commands

ip dvmrp debug-level	Defines the level of debugging for DVMRP protocol on 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

35 PIM 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. 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 through specific requests.

Downstream routers must explicitly join PIM-SM distribution trees to receive multicast streams on behalf of directly connected receivers or other downstream PIM-SM routers. This paradigm of receiver-initiated forwarding makes PIM ideal for network environments where receiver groups are thinly populated and bandwidth conservation is a concern, such as in wide area networks (WANs). PIM-DM uses RPF (Reverse Path Forwarding) to prevent looping of multicast datagrams while flooding. If some areas of the network do not have group members, PIM-DM will prune the forwarding branch by instantiating the prune state.

PIM-DM differs from PIM-SM in two essential ways:

- There are no periodic joins transmitted, only explicitly triggered prunes and grafts.
- There is no Rendezvous Point (RP). This is particularly important in networks that cannot tolerate a single point of failure.

Alcatel-Lucent implementation of PIM can also be configured in an IPv6 environment.

MIB information for the PIM commands is as follows:

Filename: AlcatelIND1Pim_mib.htm
Module: ALCATEL-IND1-PIM-MIB

Filename: IETF_PIM_BSR.mib
Module: PIM-BSR-MIB

Filename: IETF_PIM_STD.mib
Module: PIM-STD-MIB

A summary of the available commands is listed here:

ip load pim
ip pim sparse status
ip pim dense status
ip pim sparse bfd-std status
ip pim interface bfd-std
ip pim dense redundant path status
ip pim ssm group
ip pim dense group
ip pim cbsr
ip pim static-rp
ip pim candidate-rp
ip pim rp-threshold
ip pim keepalive-period
ip pim max-rps
ip pim probe-time
ip pim register checksum
ip pim register-suppress-timeout
ip pim spt status
ip pim state-refresh-interval
ip pim state-refresh-limit
ip pim state-refresh-ttl
ip pim interface
ip pim neighbor-loss-notification-period
ip pim invalid-register-notification-period
ip pim invalid-joinprune-notification-period
ip pim rp-mapping-notification-period
ip pim interface-election-notification-period
show ip pim dense
show ip pim sparse
show ip pim ssm group
show ip pim dense group
show ip pim neighbor
show ip pim candidate-rp
show ip pim group-map
show ip pim interface
show ip pim static-rp
show ip pim cbsr
show ip pim bsr
show ip pim notifications
show ip pim groute
show ip pim sgroute
ipv6 pim sparse status
ipv6 pim dense status
ipv6 pim ssm group
ipv6 pim dense group
ipv6 pim cbsr
ipv6 pim static-rp
ipv6 pim candidate-rp
ipv6 pim rp-switchover
ipv6 pim spt status
ipv6 pim interface
show ipv6 pim sparse
show ipv6 pim dense
show ipv6 pim ssm group
show ipv6 pim dense group
show ipv6 pim interface
show ipv6 pim neighbor
show ipv6 pim static-rp
show ipv6 pim group-map
show ipv6 pim candidate-rp
show ipv6 pim cbsr
show ipv6 pim bsr
show ipv6 pim groute
show ipv6 pim sgroute

ip load pim

Dynamically loads PIM to memory.

ip load pim

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- This command must be executed before PIM can run on the switch.
- This command is supported in both IPv4 and IPv6 PIM.
- The advanced routing image must be loaded to flash before the feature starts to work on the switch.

Examples

```
-> ip load pim
```

Release History

Release 6.1.1; command introduced.

Related Commands

ip pim sparse status	Globally enables or disables the PIM-SM protocol on the switch.
show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.
ip pim dense status	Globally enables or disables PIM-DM protocol on the switch.
show ip pim dense	Displays the status of the various global parameters for the PIM Dense mode.
ipv6 pim sparse status	Enables or disables the IPv6 PIM-SM (sparse mode) globally for IPv6.
show ipv6 pim sparse	Displays the status of the various global parameters for the IPv6 PIM sparse mode.
ipv6 pim dense status	Enables or disables the IPv6 PIM-DM (dense mode) globally for IPv6.
show ipv6 pim dense	Displays the status of the various global parameters for the IPv6 PIM dense mode.

MIB Objects

```
alaDrcTmConfig
   alaDrcTmIPPimStatus
```

ip pim sparse status

Globally enables or disables PIM-SM protocol on the switch.

ip pim sparse 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 6850E, 6855, 9000E

Usage Guidelines

- This command must be set to **enable** before PIM-SM can run on the switch. In addition, the **ip load pim** command must be executed. Refer to **ip load pim** for more information.
- The advanced routing image must be loaded to flash before the feature starts to work on the switch.

Examples

```
-> ip pim sparse status enable
-> ip pim sparse status disable
```

Release History

Release 6.1.1; command introduced.

Related Commands

ip pim interface	Enables or disables the PIM protocol on a specific interface.
ip load pim	Dynamically loads PIM to memory.
show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmAdminStatus
```

ip pim sparse bfd-std status

Enables or disables BFD protocol on PIM DM/SM.

ip pim {dense | sparse} bfd-std status {enable | disable}

Syntax Definitions

dense	Enables PIM dense mode.
sparce	Enables PIM sparce mode.
enable	Globally enables the BFD status for PIM DM/SM.
disable	Globally disables the BFD status for PIM DM/SM.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

The **ip load pim** command must be executed prior to executing this command. Refer to **ip load pim** for more information.

Examples

```
-> ip pim sparse bfd-std status enable
-> ip pim sparse bfd-std status disable
```

Release History

Release 6.4.5; command introduced.

Related Commands

show ip bfd-std	Displays the global BFD configuration table.
show ip bfd-std session	Displays information for an individual BFD session.
show ip bfd-std sessions	Displays all the BFD sessions for the switch.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimdmBfdStatus
   alaPimdmBfdStatus
```

ip pim interface bfd-std

Enables or disables BFD protocol for particular interfaces of PIM.

ip pim interface *name* **bfd-std status{enable | disable}**

Syntax Definitions

name	Name of the VLAN interface.
enable	Enables BFD in the PIM interface.
disable	Disables BFD in the PIM interface.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- The **ip load pim** command must be executed prior to executing this command. Refer to **ip load pim** for more information.
- Initially PIM DM/SM status has to be enabled globally. Then PIM DM/SM should be enabled on the interface.
- BFD status has to be enabled globally. Then enable BFD on the interface.
- BFD can then be enabled on PIM or any other protocol.

Examples

```
-> ip pim interface vlan-2 bfd-std enable
-> ip pim interface vlan-2 bfd-std disable
```

Release History

Release 6.4.5; command introduced.

Related Commands

ip pim interface	Enables or disables the PIM protocol on a specific interface.
ip load pim	Dynamically loads PIM to memory.
show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.
show ip bfd-std	Displays the global BFD configuration table.
show ip bfd-std sessions	Displays all the BFD sessions for the switch.

MIB Objects

```
pimInterfaceTable
   alaPimIfBfdStatus
   alaPimIfBfdStatus
```

ip pim dense redundant path status

Enables or disables PIM DM/SM for the redundant path.

ip pim dense redundant-path {enable | disable}

Syntax Definitions

enable	Enables the redundant path status for the PIM DM
disable	Disables the redundant path status for the PIM DM

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Redundant path configuration applies only to PIM-DIM mode.
- For this command to be effective, PIM status has to be disabled and then enabled.
- Applicable only for IPV4.
- To achieve maximum faster convergence, redundant path needs to be enabled on all the PIM routers along with OSPF sub-second convergence with BFD enabled in a network.
- On enabling redundant path, Assert does not take place, so there is consumption of bandwidth in the redundant path. There is no loop, but multicast traffic consumes bandwidth on redundant path that might be an active path for other traffic.

Examples

```
-> ip pim interface bfd-std enable
-> ip pim interface bfd-std disable
```

Release History

Release 6.4.5; command introduced.

Related Commands

ip pim interface	Enables or disables the PIM protocol on a specific interface.
ip load pim	Dynamically loads PIM to memory.
ip pim dense status	Globally enables or disables PIM-DM protocol on the switch.

MIB Objects

```
alaPimdmGlobalConfig
   alaPimdmRedudantStatus
```

ip pim dense status

Globally enables or disables PIM-DM protocol on the switch.

ip pim dense status {enable | disable}

Syntax Definitions

enable	Globally enables PIM-DM on the switch.
disable	Globally disables PIM-DM on the switch.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- This command must be set to **enable** before PIM-DM can run on the switch. In addition, the **ip load pim** command must be executed. Refer to **ip load pim** for more information.
- The advanced routing image must be loaded to flash before the feature starts to work on the switch.

Examples

```
-> ip pim dense status enable
-> ip pim dense status disable
```

Release History

Release 6.1.1; command introduced.

Related Commands

ip pim interface	Enables or disables the PIM protocol on a specific interface.
ip load pim	Dynamically loads PIM to memory.
show ip pim dense	Displays the status of the various global parameters for the PIM dense mode.

MIB Objects

```
alaPimdmGlobalConfig
   alaPimdmAdminStatus
```

ip pim ssm group

Statically maps the specified IP multicast group(s) to the PIM Source Specific Multicast mode (SSM).

ip pim ssm group *group_address/prefix_length* **[[no] override] [priority** *priority***]**

no ip pim ssm group *group_address/prefix_length*

Syntax Definitions

group_address	Specifies a 32-bit group address.
/prefix_length	Specifies the prefix length of the multicast group.
override	Specifies the static SSM mode mapping configuration to override the dynamically learned group mapping information for the specified group(s).
priority	Specifies the preference value to be used for this static SSM mode configuration and provides fine control over which configuration is overridden by this static configuration. Values may range from 0 to 128.

Defaults

By default, the priority option is not set and the override option is set to false.

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a static configuration of a SSM mode group mapping.
- The PIM Source-Specific Multicast (SSM) mode for the default SSM address range (232.0.0.0 through 232.255.255.255) reserved by the Internet Assigned Numbers Authority is not enabled automatically and needs to be configured manually to support SSM.
- You can also map additional multicast address ranges for the SSM group using this command. However, the multicast groups in the reserved address range can be mapped only to the SSM mode.
- If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range.
- Specifying the priority value obsoletes the **override** option.
- Note that once the priority option has been defined, a value of 65535 can be used to un-set the priority

Examples

```
-> ip pim ssm group 224.0.0.0/4 priority 50
```

Release History

Release 6.3.1; command introduced.

Related Commands

show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.
show ip pim ssm group	Displays the static configuration of multicast group mappings for the PIM-Source Specific Multicast (SSM) mode.
show ip pim group-map	Displays the PIM group mapping table.

MIB Objects

```
alaPimStaticRPTable
   alaPimStaticRPGrpAddress
   alaPimStaticRPGrpPrefixLength
   alaPimStaticRPOverrideDynamic
   alaPimStaticRPPrecedence
   alaPimStaticRPRowStatus
```

ip pim dense group

Statically maps the specified IP multicast group(s) to the PIM Dense mode (DM).

ip pim dense group *group_address/prefix_length* **[[no] override] [priority** *priority*]

no ip pim dense group *group_address/prefix_length*

Syntax Definitions

group_address	Specifies a 32-bit group address.
/prefix_length	Specifies the prefix length of the multicast group.
override	Specifies this static Dense mode mapping configuration to override the dynamically learned group mapping information for the specified group(s).
priority	Specifies the preference value to be used for this static configuration and provides fine control over which configuration is overridden by this static configuration. Values may range from 0 to 128.

Defaults

By default, the priority option is not set and the override option is set to false.

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a static configuration of a dense mode group mapping.
- This command specifies the mode as Dense (PIM-DM) for the specified multicast group address.
- If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range
- Specifying the priority value obsoletes the **override** option and once the priority option has been defined, a value of 65535 can be used to un-set the priority.

Examples

```
-> ip pim dense group 224.0.0.0/4 priority 50
```

Release History

Release 6.3.1; command introduced.

Related Commands

show ip pim dense	Displays the status of the various global parameters for the PIM dense mode.
show ip pim dense group	Displays the static configuration of multicast group mappings for PIM-Dense Mode (DM).
show ip pim group-map	Displays the PIM group mapping table.

MIB Objects

```
alaPimStaticRPTable
   alaPimStaticRPGrpAddress
   alaPimStaticRPGrpPrefixLength
   alaPimStaticRPOverrideDynamic
   alaPimStaticRPPrecedence
   alaPimStaticRPRowStatus
```

ip pim cbsr

Configures the local router as the Candidate-BSR for the PIM domain.

ip pim cbsr *ip_address* **[priority** *priority***] [mask-length** *bits***]**

no ip pim cbsr *ip_address*

Syntax Definitions

ip_address	Specifies the 32-bit address that the local router uses to advertise itself as a Candidate-BSR.
priority	Specifies the priority value of the local router as a Candidate-BSR. The higher the value, the higher the priority. Values may range from 0 to 255.
bits	Specifies a 32-bit mask length that is advertised in the Bootstrap messages (the length of the mask is used in the hash function when computing the Rendezvous Point (RP) for a multicast group).Values may range from 1 to 32.

Defaults

parameter	default
priority	64
bits	30

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove the local routers candidature as the BSR.
- This command is supported only in the sparse mode.
- The information configured using this command is used in the Bootstrap messages.
- Candidate-BSRs also avoid a single point of failure in a PIM domain.

Examples

```
-> ip pim cbsr 50.1.1.1 priority 100 mask-length 4
```

Release History

Release 6.3.1; command introduced.

Related Commands

show ip pim cbsr	Displays the Candidate-BSR information that is used in the Bootstrap messages.

MIB Objects

```
alaPimBSrCandidateBSRTable
   alaPimBsrCandidateBSRAddress
   alaPimBsrCandidateBSRPriority
   alaPimBsrCandidateBSRHashMaskLength
   alaPimBsrCandidateBSRRowStatus
```

ip pim static-rp

Adds, modifies, or deletes a static RP for a group (“modifies” applies only to the RP address, since the table is indexed from group address and mask parameters).

ip pim static-rp *group_address/prefix_length rp_address* **[[no] override] [priority** *priority***]**

no ip pim static-rp *group_address/prefix_length rp_address*

Syntax Definitions

group_address	Specifies a 32-bit group address.
/prefix_length	Specifies the prefix length of the multicast group.
rp_address	Specifies a 32-bit Rendezvous Point (RP) address.
override	Specifies this static RP configuration to override the dynamically learned RP information for the specified group(s).
priority	Specifies the preference value to be used for the static RP configuration and provides fine control over which configuration is overridden by this static configuration. Values may range from 0 to 128.

Defaults

By default, the priority option is not set and the override option is set to false.

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete a static RP configuration.
- Specifying the priority value obsoletes the **override** option.
- The PIM Source-Specific Multicast (SSM) mode for the default SSM address range (232.0.0.0 through 232.255.255.255) reserved by the Internet Assigned Numbers Authority is not enabled automatically and must be configured manually to support SSM. You can also map additional multicast address ranges for the SSM group. However, the multicast groups in the reserved address range can be mapped only to the SSM mode.
- This command is supported only in the sparse mode.
- If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range
- Once the priority option has been defined, a value of 65535 can be used to change the priority
- To view current static RP configuration settings, use the **show ip pim static-rp** command.

Examples

```
-> ip pim static-rp 224.0.0.0/4 10.1.1.1 priority 10
```

Release History

Release 6.1.1; command introduced.
Release 6.3.1; **override** and **priority** options added.

Related Commands

show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.
show ip pim static-rp	Displays the PIM static RP table for ASM mode, which includes group address/prefix length, the static Rendezvous Point (RP) address, and the current status of static RP configuration (that is, enabled or disabled).
show ip pim group-map	Displays the PIM group mapping table.

MIB Objects

```
alaPimStaticRPTable
   alaPimStaticRPGrpAddress
   alaPimStaticRPGrpPrefixLength
   alaPimStaticRPRPAddress
   alaPimStaticRPOverrideDynamic
   alaPimStaticRPPrecedence
   alaPimStaticRPRowStatus
```

ip pim candidate-rp

Configures the local router as the Candidate-Rendezvous Point (C-RP) for a specified IP multicast group(s).

ip pim candidate-rp *rp_address group-address/prefix_length* **[priority** *priority***] [interval** *seconds***]**

no ip pim candidate-rp *rp_address group-address/prefix_length*

Syntax Definitions

rp_address	Specifies a 32-bit address that will be advertised as a Candidate-RP.
group_address	Specifies a 32-bit group address for which the local router will advertise itself as a Candidate-RP.
/prefix_length	Specifies the prefix length of the multicast group.
priority	Specifies the priority value of the Candidate-RP. Values may range from 0 to 192. The lower the value, the higher the priority.
seconds	Specifies the interval at which the C-RP advertisements are sent to the Bootstrap router, in seconds. Values may range from 1 to 300.

Defaults

parameter	default
priority	192
seconds	60

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove the association of the device as a C-RP for a particular multicast group.
- The specified *rp_address* must belong to a PIM enabled interface.
- Only one RP address is supported per switch. If multiple candidate-RP entries are defined, they must specify the same *rp-address.*
- The priority and the interval values are used by the switch. If they are modified for one entry, the switch modifies these for all the candidate-rp entries.
- This command is supported only in the sparse mode.

Examples

```
-> ip pim candidate-rp 50.1.1.1 224.0.0.0/4 priority 100 interval 100
```

Release History

Release 6.3.1; command introduced.

Related Commands

show ip pim candidate-rp	Displays the IP multicast groups for which the local router advertises itself as a Candidate-RP.

MIB Objects

```
alaPimBsrCandidateRPTable
   alaPimBsrCandidateRPAddress
   alaPimBsrCandidateRPGroupAddress
   alaPimBsrCandidateRPGroupPrefixLength
   alaPimBsrCandidateRPPriority
   alaPimBsrCandidateRPAdvInterval
   alaPimBsrCandidateRPRowStatus
```

ip pim rp-threshold

Specifies the data rate, in bits per second (bps), at which the Rendezvous Point (RP) attempts to switch to native forwarding by issuing a source-specific (S, G) Join message toward the source.

ip pim rp-threshold *bps*

Syntax Definitions

bps	The data rate value, in bits per second, at which the RP attempts to switch to native forwarding (0–2147483647).

Defaults

parameter	default
bps	1

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- This command is supported only in the sparse mode.
- 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. It will issue a (S, G) Join message upon receiving the first data packet, if its bits per second value is 1.
- To view the current RP threshold, use the **show ip pim sparse** command.

Examples

```
-> ip pim rp-threshold 131072
```

Release History

Release 6.1.1; command introduced.

Related Commands

show ip pim sparse	Displays the global parameters for PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmRPThreshold
```

ip pim keepalive-period

Configures the period during which the (S,G) Join state is maintained in the absence of (S,G) Join messages or explicit (S,G) local membership.

ip pim keepalive-period *seconds*

Syntax Definitions

seconds	Specifies the timeout value, in seconds (0-65535).

Defaults

parameter	default
seconds	210

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- This timer is called the Keepalive Period in the PIM-SM specification and the Source Lifetime in the PIM-DM specification.
- This command includes support for both IPv4 PIM and IPv6 PIM.

Examples

```
-> ip pim keepalive-period 500
```

Release History

Release 6.3.1; command introduced.

Related Commands

show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.
show ip pim dense	Displays the status of the various global parameters for the PIM dense mode.
show ipv6 pim sparse	Displays the status of the various global parameters for the IPv6 PIM sparse mode.
show ipv6 pim dense	Displays the status of the various global parameters for the IPv6 PIM dense mode.

MIB Objects

```
alaPim
   alaPimKeepalivePeriod
```

ip pim max-rps

Configures the maximum number of C-RP routers allowed in the PIM-SM domain.

ip pim 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 6850E, 6855, 9000E

Usage Guidelines

- This command is supported only in the sparse mode.
- This command is used with both IPv4 and IPv6 PIM-SM. The PIM-SM must be disabled before changing **max-rps** value.
- PIM-SM must be globally disabled before changing the maximum number of C-RP routers. To globally disable PIM-SM, refer to the **ip pim sparse status** command on page 35-5.

Examples

```
-> ip pim max-rps 32
```

Release History

Release 6.1.1; command introduced.

Related Commands

ip pim sparse status	Globally enables or disables the PIM-SM protocol on the switch.
ipv6 pim sparse status	Enables or disables the IPv6 PIM-SM (sparse mode) globally for IPv6.
show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.
show ipv6 pim sparse	Displays the status of the various global parameters for the IPv6 PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmMaxRPs
```

ip pim 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 resumes encapsulating packets from the source to the RP.

ip pim probe-time *seconds*

Syntax Definitions

seconds	The probe time, in seconds (1–300).

Defaults

parameter	default
seconds	5

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- This command is used with both IPv4 and IPv6 PIM-SM.
- This command is supported only in the sparse mode.

Examples

```
-> ip pim probe-time 5
```

Release History

Release 6.1.1; command introduced.

Related Commands

show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.
show ipv6 pim sparse	Displays the status of the various global parameters for the IPv6 PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmProbeTime
```

ip pim register checksum

Configures the application of the checksum function on sent and received register messages in the domain.

ip pim 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 6850E, 6855, 9000E

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 domain.
- This command is supported only in the sparse mode.

Examples

```
-> ip pim register checksum header
-> ip pim register checksum full
```

Release History

Release 6.1.1; command introduced.

Related Commands

show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmOldRegisterMessageSupport
```

ip pim register-suppress-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 message.

ip pim register-suppress-timeout *seconds*

Syntax Definitions

seconds	The timeout value, in seconds (0–65535).

Defaults

parameter	default
seconds	60

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- This command is supported in both IPv4 and IPv6 PIM.
- This command is supported only in the sparse mode.

Examples

```
-> ip pim register-suppress-timeout 10
```

Release History

Release 6.1.1; command introduced.

Related Commands

show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.
show ipv6 pim sparse	Displays the status of the various global parameters for the IPv6 PIM sparse mode.

MIB Objects

```
alaPim
   alaPimRegisterSuppressionTime
```

ip pim 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 pim 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 6850E, 6855, 9000E

Usage Guidelines

- This command is supported only in the sparse mode.
- 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 pim sparse** command.

Examples

```
-> ip pim spt status enable
-> ip pim spt status disable
```

Release History

Release 6.1.1; command introduced.

Related Commands

show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmAdminSPTConfig
```

ip pim state-refresh-interval

Sets the interval between successive State Refresh messages originated by a router.

ip pim state-refresh-interval *seconds*

Syntax Definitions

seconds	The interval between successive State Refresh messages, in seconds. Values may range from 0 to 65535.

Defaults

parameter	default
seconds	60

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- This command is supported only in the dense mode.
- This value is used with both IPv4 PIM-DM and IPv6 PIM-DM.

Examples

```
-> ip pim state-refresh-interval 80
```

Release History

Release 6.1.1; command introduced.

Related Commands

ip pim interface	Enables or disables the PIM protocol on a specific interface.
ipv6 pim interface	Enables IPv6 PIM and configures the statistics.
show ip pim dense	Displays the status of the various global parameters for the PIM dense mode.
show ipv6 pim dense	Displays the status of the various global parameters for the IPv6 PIM dense mode.

MIB Objects

```
alaPim
   alaPimRefreshInterval
```

ip pim state-refresh-limit

Sets the limit at which a router will not forward successive State Refresh messages if they are received at less than the interval.

ip pim state-refresh- limit *ticks*

Syntax Definitions

ticks	The limit at which the received State Refresh messages is not forwarded, if the messages are received at less than the interval. Values may range from 0 to 65535.

Defaults

parameter	default
ticks	0

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- This command is supported only in the dense mode.
- This value is used with both IPv4 and IPv6.

Examples

```
-> ip pim state-refresh-limit 2
```

Release History

Release 6.1.1; command introduced.

Related Commands

ip pim interface	Enables or disables the PIM protocol on a specific interface.
ipv6 pim interface	Enables IPv6 PIM and configures the statistics.
show ip pim dense	Displays the status of the various global parameters for the PIM dense mode.
show ipv6 pim dense	Displays the status of the various global parameters for the IPv6 PIM dense mode.

MIB Objects

```
alaPimdmGlobalConfig
   alaPimdmStateRefreshLimitInterval
```

ip pim state-refresh-ttl

Sets the Time to Live to be used in a router's originated State Refresh messages if the data packet's Time to Live is not recorded.

ip pim state-refresh- ttl *num*

Syntax Definitions

num	The Time to Live to be used. Values may range from 0 to 255.

Defaults

parameter	default
num	16

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- This command is supported only in the dense mode.
- This value is used with both IPv4 and IPv6 PIM-DM.

Examples

```
-> ip pim state-refresh-ttl 122
```

Release History

Release 6.1.1; command introduced.

Related Commands

ip pim interface	Enables or disables the PIM protocol on a specific interface.
ipv6 pim interface	Enables IPv6 PIM and configures the statistics.
show ip pim dense	Displays the status of the various global parameters for the PIM dense mode.
show ipv6 pim dense	Displays the status of the various global parameters for the IPv6 PIM dense mode.

MIB Objects

```
alaPimdmGlobalConfig
   alaPimdmStateRefreshTimeToLive
```

ip pim interface

Enables PIM and configures PIM-related statistics such as hello-interval, triggered-hello, hello-holdtime, joinprune, prune-delay, override-interval, dr-priority, stub interface, prune limit interval, and graft retry interval on the interface.

ip pim interface *if_name* **[hello-interval** *seconds***] [triggered-hello** *seconds***] [joinprune-interval** *seconds***] [hello-holdtime** *seconds***] [joinprune-holdtime** *seconds***] [prune-delay** *milliseconds***] [override-interval** *milliseconds***] [dr-priority** *priority***] [[no] stub] [prune-limit-interval** *seconds***] [graft-retry-interval** *seconds***]**

no ip pim interface *if_name*

Syntax Definitions

if_name	The interface name on which PIM is being enabled or disabled.
hello-interval *seconds*	The frequency at which PIM Hello messages are transmitted on a specified interface, in seconds. Values may range from 0 to 18000.
triggered-hello *seconds*	Specifies the maximum time, in seconds, before a triggered PIM Hello message is sent on this interface. Values may range from 0 to 60.
joinprune-interval *seconds*	The frequency at which periodic Join/Prune messages are sent on this interface, in seconds. Values may range from 0 to 18000.
hello-holdtime *seconds*	Specifies the value set in the Holdtime field of PIM Hello messages sent on this interface, in seconds. Values may range from 0 to 65535.
joinprune-holdtime *seconds*	Specifies the value inserted into the Holdtime field of the Join/Prune messages sent on this interface, in seconds.Values may range from 0 to 65535.
prune-delay *milliseconds*	Specifies the value of the expected propagation delay between PIM routers on this network, inserted into the LAN prune-delay option of the Hello messages sent on this interface, in milliseconds. Values may range from 0 to 32767.
override-interval *milliseconds*	Specifies the value inserted into the Override Interval field of the LAN prune-delay option of the Hello messages sent on this interface, in *milliseconds.* Values may range from 0 to 65535.
dr-priority *priority*	Specifies the Designated Router priority inserted into the DR priority option on a specified interface. The DR priority option value can range between 1 to 192. A higher numeric value denotes a higher priority.
prune-limit-interval *seconds*	Specifies the minimum interval that must elapse between two successive prune messages sent on this interface, in seconds. Values may range from 0 to 65535.
graft-retry-interval *seconds*	Specifies the minimum interval that must elapse between two successive graft messages sent on this interface, in seconds. Values may range from 0 to 65535.
stub	Specifies the interface not to send any PIM packets through this interface, and to ignore received PIM packets.

Defaults

parameter	default
hello-interval *seconds*	30
triggered-hello *seconds*	5
joinprune-interval *seconds*	60
hello-holdtime *seconds*	105
joinprune-holdtime *seconds*	210
prune-delay *milliseconds*	500
override-interval *milliseconds*	2500
dr-priority *priority*	1
prune-limit-interval *seconds*	60
graft-retry-interval *seconds*	3
stub	Disabled.

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete a PIM interface.
- PIM must be enabled globally on the switch before it runs on the interface. To globally enable or disable PIM-SM on the switch, refer to the **ip pim sparse status** command on page 35-5. To enable or disable PIM-DM on the switch, refer to the **ip pim dense status** command on page 35-11.
- Specifying zero for the hello-interval represents an infinite time, in which case periodic PIM Hello messages are not sent.
- Specifying zero for the joinprune-interval represents an infinite time, in which case periodic PIM Join/Prune messages are not sent.
- Specifying the value of 65535 for hello-holdtime represents an infinite time. If a PIM router gets Hello packet from a neighbor with its hello-holdtime value as infinite time, then the PIM router will not time out the sender(neighbor). It is recommended that you should use a hello-holdtime interval that is 3.5 times the value of the hello-interval, or 65535 seconds if the hello-interval is set to zero.
- Specifying the value of 65535 for joinprune-holdtime represents an infinite time. The receipt of Join/Prune messages with its joinprune-holdtime value as infinite time, then this specifies an infinite hold-time for the particular join/prune message. It is recommended that you use a joinprune-holdtime interval that is 3.5 times the value of the Join/Prune interval defined for the interface, or 65535 seconds if the joinprune-interval is set to zero.
- The interface configured as a **stub** does not send any PIM packets through that interface, and any received PIM packets are also ignored. By default, a PIM interface is not set to be a stub one.
- The **graft-retry-interval** and **prune-limit-interval** options can be used only with the PIM-DM mode.

Examples

```
-> ip pim interface vlan-2 hello-interval 100 triggered-hello 10 joinprune-inter-
val 100 hello-holdtime 350 joinprune-holdtime 400
-> no ip pim interface vlan-2
```

Release History

Release 6.1.1; command introduced.

Related Command

show ip pim interface	Displays detailed PIM settings for a specific interface. In general, it displays PIM settings for all the interfaces if no argument is specified.

MIB Objects

```
alaPimInterfaceTable
   alaPimInterfaceIfIndex
   alaPimInterfaceStatus
   alaPimInterfaceHelloInterval
   alaPimInterfaceTrigHelloInterval
   alaPimInterfaceJoinPruneInterval
   alaPimInterfaceHelloHoldtime
   alaPimInterfaceJoinPruneHoldtime
   alaPimInterfacePropagationDelay
   alaPimInterfaceOverrideInterval
   alaPimInerfaceDRPriority
   alaPimInterfaceStubInterface
   alaPimInterfacePruneLimitInterval
   alaPimInterfaceGraftRetryInterval
```

ip pim neighbor-loss-notification-period

Specifies the minimum time that must elapse between PIM neighbor loss notifications originated by the router.

ip pim neighbor-loss-notification-period *seconds*

Syntax Definitions

seconds	Specifies the time value that must elapse between neighbor loss notifications, in seconds (0–65535).

Defaults

parameter	default
seconds	0

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- The maximum value of 65535 represents an infinite time. The PIM neighbor loss notifications are never sent in case of infinite time.
- This command is used with both IPv4 and IPv6 PIM.

Examples

```
-> ip pim neighbor-loss-notification-period 100
```

Release History

Release 6.3.1; command introduced.

Related Commands

show ip pim notifications	Displays the configuration of the configured notification periods as well as information on the events triggering the notifications.

MIB Objects

```
alaPim
   alaPimNeighborLossNotificationPeriod
```

ip pim invalid-register-notification-period

Specifies the minimum time that must elapse between the PIM invalid register notifications originated by the router.

ip pim invalid-register-notification-period *seconds*

Syntax Definitions

seconds	Specifies the minimum time value that must elapse between invalid register notifications, in seconds (10–65535).

Defaults

parameter	default
seconds	65535

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- The default value of 65535 represents an infinite time. The PIM invalid register notifications are never sent in case of infinite time.
- The non-zero minimum allowed value provides resilience against the propagation of denial-of-service attacks from the data and control planes to the network management plane.
- This value is used with both IPv4 and IPv6 PIM.
- This command is supported only in the sparse mode.

Examples

```
-> ip pim invalid-register-notification-period 100
```

Release History

Release 6.3.1; command introduced.

Related Commands

show ip pim notifications	Displays the configuration of the configured notification periods as well as information on the events triggering the notifications.

MIB Objects

```
alaPim
   alaPimInvalidRegisterNotificationPeriod
```

ip pim invalid-joinprune-notification-period

Specifies the minimum time that must elapse between the PIM invalid joinprune notifications originated by the router.

ip pim invalid-joinprune-notification-period *seconds*

Syntax Definitions

seconds	Specifies the minimum time value that must elapse between invalid joinprune notifications, in seconds (10–65535).

Defaults

parameter	default
seconds	65535

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- The default value of 65535 represents an infinite time. The PIM invalid joinprune notifications are never sent in case of infinite time.
- The non-zero minimum allowed value provides resilience against the propagation of denial-of-service attacks from the control plane to the network management plane.
- This value is used with both IPv4 and IPv6 PIM.

Examples

```
-> ip pim invalid-joinprune-notification-period 100
```

Release History

Release 6.3.1; command introduced.

Related Commands

show ip pim notifications	Displays the configuration of the configured notification periods as well as information on the events triggering the notifications.

MIB Objects

```
alaPim
   alaPimInvalidJoinPruneNotificationPeriod
```

ip pim rp-mapping-notification-period

Specifies the minimum time that must elapse between the PIM RP mapping notifications originated by the router.

ip pim rp-mapping-notification-period *seconds*

Syntax Definitions

seconds	Specifies the minimum time value that must elapse between RP mapping notifications, in seconds (0–65535).

Defaults

parameter	default
seconds	65535

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- The default value of 65535 represents an infinite time. The RP mapping notifications are never sent in case of infinite time.
- This value is used with both IPv4 and IPv6 PIM.
- This command is supported only in the sparse mode.

Examples

```
-> ip pim rp-mapping-notification-period 100
```

Release History

Release 6.3.1; command introduced.

Related Commands

show ip pim notifications	Displays the configuration of the configured notification periods as well as information on the events triggering the notifications.

MIB Objects

```
alaPim
   alaPimRPMappingNotificationPeriod
```

ip pim interface-election-notification-period

Specifies the minimum time that must elapse between the PIM interface election notifications originated by the router.

ip pim interface-election-notification-period *seconds*

Syntax Definitions

seconds	Specifies the minimum time value that must elapse between interface election notifications, in seconds (0–65535).

Defaults

parameter	default
seconds	65535

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- The default value of 65535 represents an infinite time. The interface election notifications are never sent in case of infinite time.
- This value is used with both IPv4 and IPv6 PIM.
- This command is supported only in the sparse mode.

Examples

```
-> ip pim interface-election-notification-period 100
```

Release History

Release 6.3.1; command introduced.

Related Commands

show ip pim notifications	Displays the configuration of the configured notification periods as well as information on the events triggering the notifications.

MIB Objects

```
alaPim
   alaPimInterfaceElectionNotificationPeriod
```

show ip pim sparse

Displays the status of the various global parameters for the PIM sparse mode.

show ip pim sparse

Syntax Definitions

N/A.

Defaults

N/A

Platforms Supported

OmniSwitch 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show ip pim sparse
Status                     = disabled,
Keepalive Period           = 210,
Max RPs                    = 32,
Probe Time                 = 5,
Register Checksum          = header,
Register Suppress Timeout  = 60,
RP Threshold               = 1,
SPT Status                 = enabled,
BIDIR Status               = disabled,
BIDIR Periodic Interval    = 60,
BFD Status                 = disabled
```

Release History

Release 6.1.1; command introduced.
Release 6.3.1; Keepalive Period field added.
Release 6.4.5; **BIDIR Status**, **BIDIR Periodic Interval,** and **BFD Status** included in output.

Related Commands

ip pim sparse status	Globally enables or disables PIM-SM protocol on the switch.
ip pim interface	Enables or disables the PIM protocol on a specific interface.
ip pim keepalive-period	Configures the period during which the (S,G) Join state is maintained in the absence of (S,G) Join messages or explicit (S,G) local membership.
ip pim max-rps	Configures the maximum number of C-RP routers allowed in the PIM-SM domain.
ip pim 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 resumes encapsulating packets from the source to the RP.
ip pim register checksum	Configures the application of the checksum function on sent and received register messages in the domain.
ip pim register-suppress-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 message.
ip pim rp-threshold	Specifies the data rate, in bits per second (bps), at which the Rendezvous Point (RP) attempts to switch to native forwarding by issuing a source-specific (S, G) Join message toward the source.
ip pim 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.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmAdminStatus
   alaPimKeepalivePeriod
   alaPimsmMaxRPS
   alaPimsmProbeTime
   alaPimsmOldRegisterMessageSupport
   alaPimRegisterSuppressionTime
   alaPimsmRPThreshold
   alaPimsmAdminSPTConfig
```

show ip pim dense

Displays the status of the various global parameters for the PIM dense mode.

show ip pim dense

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show ip pim dense
Status                       = disabled,
Source Lifetime              = 210,
State Refresh Interval       = 60,
State Refresh Limit Interval = 0,
State Refresh TTL            = 16,
BFD Status                   = disabled,
Redundant Path Status        = disabled
```

Release History

Release 6.1.1; command introduced.
Release 6.3.1; **join/prune** field was removed.
Release 6.4.5; **BFD status** and **Redundant Path Status** included in output.

Related Commands

ip pim dense status	Globally enables or disables PIM-DM protocol on the switch.
ip pim interface	Enables or disables the PIM protocol on a specific interface.
ip pim state-refresh-interval	Sets the interval between successive State Refresh messages originated by a router.
ip pim state-refresh-limit	Sets the limit at which a router does not forward successive State Refresh messages if they are received at less than the interval.
ip pim state-refresh-ttl	Sets the Time to Live to be used in a router's originated State Refresh messages if the data packet's Time to Live is not recorded.
ip pim keepalive-period	Configures the period during which the (S,G) Join state is maintained in the absence of (S,G) Join messages or explicit (S,G) local membership.

MIB Objects

```
alaPimdmGlobalConfig
   alaPimdmAdminStatus
   alaPimKeepalivePeriod
   alaPimRefreshInterval
   alaPimdmStateRefreshLimitInterval
   alaPimdmStateRefreshTimeToLive
```

show ip pim ssm group

Displays the static configuration of multicast group mappings for the PIM-Source Specific Multicast (SSM) mode.

show ip pim ssm group

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range.
- This command is supported only in the sparse mode.

Examples

```
-> show ip pim ssm group
Group Address/Pref Length   Mode  Override Precedence Status
--------------------------+-----+--------+----------+--------
224.0.0.0/4                 ssm   false    none       enabled
```

output definitions

Group Address/Pref Length	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 (/).
Mode	The PIM mode to be used for groups in this prefix. The possible values include asm, ssm, or dm.
Override	Specifies this static RP configuration to override the dynamically learned RP information for the specified group(s).
Precedence	Specifies the precedence value to be used for this static RP configuration.
Status	Displays whether this entry is currently enabled or disabled. Options include **enabled** and **disabled**.

Release History

Release 6.3.1; command introduced.

Related Commands

ip pim ssm group	Statically maps the specified IP multicast group(s) to the PIM Source Specific Multicast mode (SSM).
show ip pim group-map	Displays the PIM group mapping table.

MIB Objects

```
alaPimStaticRPTable
   alaPimStaticRPGrpAddress
   alaPimStaticRPGrpPrefixLength
   alaPimStaticRPPimMode
   alaPimStaticRPOverrideDynamic
   alaPimStaticRPPrecedence
   alaPimStaticRPRowStatus
```

show ip pim dense group

Displays the static configuration of multicast group mappings for PIM-Dense Mode (DM).

show ip pim dense group

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range.
- This command is supported only on PIM dense mode.

Examples

```
-> show ip pim dense group
Group Address/Pref Length   Mode  Override Precedence Status
---------------------------+-----+--------+----------+--------
224.0.0.0/4                 dm    false    none       enabled
```

output definitions

Group Address/Pref Length	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 (/).
Mode	The PIM mode to be used for groups in this prefix. The possible values include asm, ssm, or dm.
Override	Specifies this static RP configuration to override the dynamically learned RP information for the specified group(s).
Precedence	Specifies the precedence value to be used for this static RP configuration.
Status	Displays whether this entry is currently enabled or disabled. Options include **enabled** and **disabled**.

Release History

Release 6.3.1; command introduced.

Related Commands

ip pim dense group	Creates and manages the static configuration of dense mode (DM) group mappings.
show ip pim group-map	Displays the PIM group mapping table.

MIB Objects

```
alaPimStaticRPTable
   alaPimStaticRPGrpAddress
   alaPimStaticRPGrpPrefixLength
   alaPimStaticRPRowStatus
   alaPimStaticRPOverrideDynamic
   alaPimStaticRPPrecedence
   alaPimStaticRPPimMode
```

show ip pim neighbor

Displays a list of active PIM neighbors.

show ip pim neighbor [*ip_address***]**

Syntax Definitions

ip_address	The 32-bit IP address for the PIM neighbor.

Defaults

If a neighbor's IP address is not specified, the entire PIM neighbor table is displayed.

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

To view more detailed information about a particular neighbor, specify the neighbor's IP address in the command line. Additional information is displayed, which includes LAN Prune Delay, Override Interval, TBit field, State Refresh capable, and Designated Router option status.

Examples

```
-> show ip pim neighbor
Neighbor Address     Interface Name       Uptime      Expires    DR Priority
-----------------+-------------------+-----------+-----------+-------------
212.61.20.250          vlan-2            01h:07m:07s 00h:01m:38s 100
212.61.60.200          vlan-6            01h:07m:07s 00h:01m:38s 100
214.28.4.254           vlan-26           01h:07m:07s 00h:01m:38s 100
```

If a specific neighbor IP address is specified in the command line, *detailed information for the corresponding neighbor only* displays:

```
-> show ip pim neighbor 212.61.30.7
Neighbor IP Address        = 212.61.30.7,
Interface Name             = vlan-30,
Uptime                     = 00h:04m:14s,
Expires                    = 00h:01m:31s,
Lan Prune Delay Present    = true,
Propagation Delay          = 500,
Override Interval          = 2500,
TBit field                 = false,
Gen ID Present             = true,
Gen ID Value               = 0x79ca868e,
BiDir Capable              = false,
DR Priority Present        = true,
DR Priority                = 1,
State Refresh Capable      = true
```

output definitions

Neighbor (IP) Address	The 32-bit IP address of the active PIM neighbor.
Interface Name	The name of the interface used to reach this PIM neighbor.
Uptime	The amount of time since this PIM neighbor last became a neighbor of the local router, displayed in hours, minutes, and seconds.
Expiry time	The minimum amount of time remaining before the PIM neighbor is aged out, displayed in hours, minutes, and seconds.
Lan Prune Delay Present	Evaluates to TRUE if this neighbor is using the Lan Prune Delay option.
Propagation Delay	The expected propagation delay between PIM routers on this network.
DR Priority Present	Evaluates to TRUE if the neighbor is using the DR Priority option.
DR Priority	The value of the Designated Router Priority from the last PIM Hello message received from this neighbor. This object is always zero if the DR Priority Present value is FALSE.
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.
Generation ID Present	Evaluates to TRUE if this neighbor is using the Generation ID option.
Generation ID Value	The value of the Generation ID from the last PIM Hello message received from the neighbor.
BiDir Capable	Evaluates to TRUE if this neighbor is using the Bidirectional-PIM Capable option.
State Refresh Capable	Displays whether the neighbor is capable of receiving State Refresh messages. Options include **true** or **false**.
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 to 65535. The default value is 2500.

Release History

Release 6.1.1; command introduced.
Release 6.3.1; Interface name, LAN delay present, Propagation Delay, Generation ID present, Generation ID Value, BiDir Capable, DR Priority, Override Interval fields added.

Related Commands

N/A

MIB Objects

```
alaPimNeighborTable
   alaPimNeighborAddress
   alaPimNeighborIfIndex
   alaPimNeighborUpTime
```

```
alaPimNeighborExpiryTime
alaPimNeighborLanPruneDelayPresent
alaPimNeighborPropagationDelay
alaPimNeighborTBit
alaPimNeighborGenerationIDPresent
alaPimNeighborGenerationIDValue
alaPimNeighborBidirCapable
alaPimNeighborDRPriorityPresent
alaPimNeighborDRPriority
alaPimNeighborOverrideInterval
alaPimNeighborSRCapable
```

show ip pim candidate-rp

Displays the IP multicast groups for which the local router advertises itself as a Candidate-RP.

show ip pim candidate-rp

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show ip pim candidate-rp
RP Address         Group Address   Priority  Interval  Status
-----------------+---------------+---------+---------+--------
172.21.63.11       224.0.0.0/4     192       60        enabled
```

output definitions

RP Address	A 32-bit IP address that is advertised as the Candidate-Rendezvous Point (RP).
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 (/). This is the group for which the local router advertises itself as a C-RP.
Priority	The C-RP router's priority. The lower the value, the higher the priority.
Interval	The time interval at which the C-RP advertisements are sent to the BSR.
Status	The current status of this entry. The status is shown as enabled only if the PIM-SM is globally enabled and the PIM interface is enabled.

Release History

Release 6.3.1; command introduced.

Related Commands

ip pim candidate-rp	Configures the local router as the Candidate-Rendezvous Point (C-RP) for a specified IP multicast group(s).

MIB Objects

```
alaPimBsrCandidateRPTable
   alaPimBsrCandidateRPAddress
   alaPimBsrCandidateRPGroupAddress
   alaBsrCandidateRPGroupPrefixLength
   alaPimBsrCandidateRPPriority
   alaPimBsrCandidateRPInterval
   alaPimBsrCandidateRPStatus
```

show ip pim group-map

Displays the PIM group mapping table.

show ip pim group-map [bsr | static-rp | ssm | dense]

Syntax Definitions

N/A

Defaults

If the keywords **bsr**, **static-rp**, **ssm**, or **dense** are included in the command line, then only the entries that were created by the specified origin are displayed.

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- If static RP configuration is being used, this information is obtained from those static RP addresses that are defined through the **ip pim static-rp** command. As long as the RP addresses defined in the static RP set are reachable, they are added to the group mapping table.
- If the IP multicast groups are mapped to the mode SSM or DM, then the entries created by local SSM address range configuration using the **ip pim ssm group** command and local Dense Mode address range configuration using the **ip pim dense group** command are displayed.
- 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 Bootstrap messages).

Examples

```
-> show ip pim group-map
Origin    Group Address/Pref Length   RP Address    Mode  Precedence
---------+--------------------------+-------------+-----+-----------
BSR       224.0.0.0/4                172.21.63.11  asm   192
BSR       224.0.0.0/4                214.0.0.7     asm   192
Static    232.0.0.0/8                              ssm

-> show ip pim group-map bsr
Origin    Group Address/Pref Length   RP Address    Mode  Precedence
---------+--------------------------+-------------+-----+-----------
BSR       224.0.0.0/4                172.21.63.11  asm   192
BSR       224.0.0.0/4                214.0.0.7     asm   192

-> show ip pim group-map static
Origin    Group Address/Pref Length   RP Address    Mode  Precedence
---------+--------------------------+-------------+-----+-----------
Static    232.0.0.0/8                              ssm
```

output definitions

Origin	The mechanism by which the PIM mode and RP for the group were learned. The possible values include 'static RP' for local static RP configuration, 'static SSM' for both SSM group configuration and Dense Mode Group configuration, and 'BSR' for the PIM Bootstrap Router mechanism.
Group Address/Prefix Length	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	The IP address of the Rendezvous Point to be used for groups within the group prefix. There is no RP address if the PIM mode is either SSM or DM.
Mode	The PIM mode to be used for groups in this prefix.
Mapping Precedence	The precedence value of a particular row, which determines which row applies to a given group address. Numerically higher values for this object indicate lower precedences, with the value zero denoting the highest precedence.

Release History

Release 6.3.1; command introduced.

Related Commands

ip pim ssm group	Creates and manages the static configuration of a Source Specific Multicast mode group mappings.
ip pim dense group	Creates and manages the static configuration of dense mode (DM) group mappings.
ip pim static-rp	Adds, modifies, or deletes a static RP for a group (“modifies” applies only to the RP address, since the table is indexed from group address and mask parameters).

MIB Objects

```
alaPimGroupMappingTable
   alaPimGroupMappingOrigin
   alaPimGroupMappingGrpAddress
   alaPimGroupMappingPrecedence
   alaPimGroupMappingRPAddress
   alaPimGroupMappingPimMode
   alaPimGroupMappingGrpPrefixLength
```

show ip pim interface

Displays detailed PIM settings for a specific interface. In general, it displays PIM settings for all the interfaces if no argument is specified.

show ip pim interface [*if_name***]**

Syntax Definitions

if_name	The interface name.

Defaults

N/A

Platforms Supported

OmniSwitch 6855, 6850E, 9000E

Usage Guidelines

To view more detailed information about a particular interface, specify the interface name in the command line. Additional information includes Triggered Hello Interval, Hello Holdtime, Prune Delay status and value, Override Interval, LAN Delay status, Generation ID status, and Join/Prune Holdtime.

Examples

```
-> show ip pim interface
Total 1 Interfaces

Interface Name       IP Address      Designated      Hello    J/P      Oper
                                     Router          Interval Interval Status
--------------------+---------------+---------------+--------+--------+--------
tesvl                50.1.1.1        50.1.1.1        100      10       disabled


-> show ip pim interface tesvl
Interface Name              = vlan100,
IP Address                  = 100.100.100.2,
Designated Router           = 100.100.100.2,
Hello Interval              = 30,
Triggered Hello Interval    = 5,
Hello HoldTime              = 105,
Join/Prune Interval         = 60,
Join/Prune HoldTime         = 210,
Propagation (Prune) Delay   = 500,
Override Interval           = 2500,
Generation ID               = 0x4c8738d8,
DR Priority                 = 1,
DR Priority Enabled         = true,
Lan Delay Enabled           = true,
Effective Propagation Delay = 500,
Effective Override Interval = 2500,
Suppression Enabled         = true,
```

```
Stub Interface              = false,
Prune Limit Interval        = 60,
Graft Retry Interval        = 3,
State Refresh Enabled       = true,
Operational Status          = enabled
BFD Status   = Enabled
```

output definitions

Interface Name	The name of the interface on which PIM is enabled.
IP address	Specifies the IP address of the specified 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 acts as the DR.
Hello Interval	The frequency at which PIM Hello messages are transmitted on a specified interface. Values may range from 1 to 18000. The default value is 30.
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 to 18000.
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 to 60. The default value is 5.
Hello Holdtime	The current Hello Holdtime value. This value indicates the maximum amount of time, in seconds, Hello messages is held before they are considered invalid. Values may range from 0 to 65535. The default value is 105.
Join/Prune Holdtime	The current Join/Prune Holdtime value. This value indicates the maximum amount of time, in seconds, Join/Prune messages is held before they are considered invalid. Values may range from 0 to 65535. The default value is 210.
Propagation Delay	The expected propagation delay between PIM routers on this network.
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 to 65535. The default value is 2500.
Generation ID Option	The value of the Generation ID this router inserted in the last PIM Hello message it sent on this interface.
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 to 192. 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.
Lan Delay Enabled	Options include **true** and **false**. The value is true if all neighbors on the interface are using the LAN Prune Delay option. Otherwise, the setting is false.

output definitions (continued)

Effective Propagation Delay	The Effective Propagation Delay on this interface.
Effective Override Interval	The Effective Override Interval on this interface.
Suppression Enabled	Specifies whether the Join suppression is enabled on this interface.
DR Priority Enabled	Evaluates to TRUE if all routers on this interface are using the DR Priority option.
Stub Interface	Specifies whether this interface is a 'stub interface'. If this is TRUE, then no PIM packets are sent out on this interface, and any received PIM packets are ignored.
Prune Limit Interval	The minimum interval that must transpire between two successive Prunes sent by a router. This is used only with PIM-DM.
Graft Retry Interval	Displays the time-interval a router waits for a Graft acknowledgment before resending a Graft on the interface. This is used only with PIM-DM. Values may range from 1 to 65535. The default value is 3.
SR Priority Enabled	Evaluates to TRUE if all routers on this interface are using the State Refresh option. This is used only by PIM-DM.
Operational 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 is enabled on the interface, but the IP interface is currently down, this field displays as disabled. The default setting is **disabled**. To globally enable or disable PIM on the switch, refer to the **ip pim sparse status** command on page 35-5 and **ip pim dense status** command on page 35-11.
BFD Status	Displays the status of BFD protocol on PIM. Options are either **enabled** or **disabled**.

Release History

Release 6.1.1; command introduced.
Release 6.3.1; Propagation Delay, Effective Propagation Delay, Effective Override Interval, Suppression Enabled, DR Priority Enabled, and Stub Interface fields added.
Release 6.4.5; **BFD Status** included in output.

Related Commands

ip pim interface	Enables or disables the PIM protocol on a specific interface.

MIB Objects

```
alaPimInterfaceTable
   alaPimInterfaceIfIndex
   alaPimInterfaceDR
   alaPimInterfaceHelloInterval
   alaPimInterfaceJoinPruneInterval
   alaPimInterfaceStatus
   alaPimInterfaceAddress
   alaPimInterfaceTrigHelloInterval
   alaPimInterfaceHelloHoldtime
   alaPimInterfaceJoinPruneHoldtime
   alaPimInterfacePropagationDelay
```

```
alaPimInterfaceOverrideInterval
alaPimInterfaceGenerationIDValue
alaPimInterfaceDRPriority
alaPimInterfaceLanDelayEnabled
alaPimInterfaceEffectPropagDelay
alaPimInterfaceEffectOverrideIvl
alaPimInterfaceSuppressionEnabled
alaPimInterfaceDRPriorityEnabled
alaPimInterfaceStubInterface
AlaPimInterfacePruneLimitInterval
alaPimInterfaceGraftRetryInterval
alaPimInterfaceSRPriorityEnabled
```

show ip pim static-rp

Displays the PIM Static RP table for the ASM mode, which includes group address/prefix length, the static Rendezvous Point (RP) address, and the current status of the Static RP configuration (that is, enabled or disabled).

show ip pim static-rp

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range

Examples

```
-> show ip pim static-rp
Group Address/Pref Length   RP Address    Mode  Override Precedence Status
--------------------------+------------+-----+--------+----------+--------
224.0.0.0/4                 172.21.63.11  asm   false    none       enabled
```

output definitions

Group Address/Pref Length	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 pim static-rp** command on page 35-18.
RP Address	A 32-bit IP address of the Rendezvous Point (RP). To change the current RP address, refer to the **ip pim static-rp** command on page 35-18.
Mode	The PIM mode to be used for groups in this prefix. The possible values include asm, ssm, or dm.
Override	Specifies this static RP configuration to override the dynamically learned RP information for the specified group(s).
Precedence	Specifies the precedence value to be used for this static RP configuration.
Status	Displays whether static RP configuration is currently enabled or disabled. Options include **enabled** and **disabled**. To change the current status, refer to the **ip pim static-rp** command on page 35-18.

Release History

Release 6.1.1; command introduced.
Release 6.3.1; **Mode, Override,** and **Precedence** fields added.

Related Commands

ip pim static-rp	Adds, modifies, or deletes a static RP for a group (“modifies” applies only to the RP address, since the table is indexed from group address and mask parameters).

MIB Objects

```
alaPimStaticRPTable
   alaPimStaticRPGrpAddress
   alaPimStaticRPGrpPrefixLength
   alaPimStaticRPAddress
   alaPimStaticRPPimMode
   alaPimStaticRPOverrideDynamic
   alaPimStaticRPPrecedence
   alaPimStaticRPRowStatus
```

show ip pim cbsr

Displays the Candidate-BSR information that is used in the Bootstrap messages.

show ip pim cbsr

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show ip pim cbsr
CBSR Address             = 214.0.0.7,
Status                   = enabled,
CBSR Priority            = 0,
Hash Mask Length         = 30,
Elected BSR              = False,
Timer                    = 00h:00m:00s
```

output definitions

CBSR Address	The 32-bit address that the local router uses to advertise itself as a Candidate-BSR.
Status	The current status of this entry. The status is shown as enabled only if the PIM-SM is globally enabled and the PIM interface is enabled.
CBSR Priority	The value for the local router as a Candidate-BSR. The higher the value, the higher the priority.
Hash Mask Length	The 32-bit mask length that is advertised in the Bootstrap messages (the length of the mask is used in the hash function when computing the Rendezvous Point (RP) for a multicast group.
Elected BSR	Specifies whether the local router is the elected BSR.
Timer	The time value that is remaining before the local router originates the next Bootstrap message. This value is zero if this router is not the elected BSR.

Release History

Release 6.3.1; command introduced.

Related Commands

ip pim cbsr	Configures the Candidate-BSR information that is used in the Bootstrap messages.

MIB Objects

```
alaPimBSrCandidateBSRTable
   alaPimBsrCandidateBSRAddress
   alaPimBsrCandidateBSRPriority
   alaPimBsrCandidateBSRHashMaskLength
   alaPimBsrCandidateBSRElectedBSR
   alaPimBsrCandidateBSRBootstrapTimer
   alaPimBsrCandidateBSRStatus
```

show ip pim bsr

Displays information about the elected BSR.

show ip pim bsr

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show ip pim bsr
BSR Address              = 214.0.0.7
BSR Priority             = 192,
Hash Mask Length         = 30,
Expiry Time              = 00h:01m:35s
```

output definitions

BSR Address	The 32-bit address of the elected BSR.
BSR Priority	The priority value of the elected BSR. The higher the value, the higher the priority.
Hash Mask Length	The 32-bit mask length that is advertised in the Bootstrap messages by the elected BSR (the length of the mask is used in the hash function when computing the Rendezvous Point (RP) for a multicast group).
Expiry Time	The minimum time remaining before the elected BSR is declared down.

Release History

Release 6.3.1; command introduced.

Related Commands

ip pim cbsr	Configures the Candidate-BSR information that is used in the Bootstrap messages.

MIB Objects

```
alaPimBsrElectedBSRTable
   alaPimBsrElectedBSRAddress
   alaPimBsrElectedBSRPriority
   alaPimBsrElectedBSRHashMaskLength
   alaPimBsrElectedBSRExpiryTime
```

show ip pim notifications

Displays the configuration of the configured notification periods as well as information on the events triggering the notifications.

show ip pim notifications

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

The outputs from this command includes both IPv4 and IPv6 information.

Examples

```
-> show ip pim notifications
Neighbor Loss Notifications
  Period       = 0
  Count        = 0
Invalid Register Notifications
  Period       = 65535
  Msgs Rcvd    = 0
  Origin       = None
  Group        = None
  RP           = None
Invalid Join Prune Notifications
  Period       = 65535
  Msgs Rcvd    = 0
  Origin       = None
  Group        = None
  RP           = None
RP Mapping Notifications
  Period       = 65535
  Count        = 0
Interface Election Notifications
  Period       = 65535
  Count        = 0
```

output definitions

Neighbor Loss Notification	**Period:** Minimum time interval that must elapse between the PIM neighbor loss notification originated by the device. **Count:** The number of neighbor loss events that have occurred. This counter is incremented whenever a neighbor loss notification is generated.
Invalid Register Notification	**Period:** Minimum time interval that must elapse between the PIM invalid register notifications originated by the device. **Msgs Rcvd:** The number of invalid PIM register notification messages that have been received by the device. **Group:** The multicast group address to which the last unexpected Register message received by the device was addressed. **RP:** The RP address to which the last unexpected Register message received by the device was delivered. **Origin**: The source address of the last unexpected Register message received by the device.
Invalid Join/Prune Notification	**Period:** Minimum time that must elapse between PIM invalid join-prune notifications originated by the device. **Msgs Rcvd:** The number of invalid PIM join/prune messages that have been received by the device. **Origin**: The source address of the last unexpected join/prune message received by the device. **Group**: The multicast group address carried in the last unexpected join-prune message received by the device. **RP**: The RP address carried in the last unexpected join/prune message received by the device.
RP Mapping Notifications	**Period**: Minimum time that must elapse between PIM RP mapping change notifications originated by the device. **Count**: The number of changes to active RP mappings on this device.
Interface Election Notifications	**Period**: Minimum time that must elapse between PIM Interface Election traps originated by the router. **Count:** The number of times this device has been elected DR on any interface.

Release History

Release 6.3.1; command introduced.

Related Commands

ip pim neighbor-loss-notification-period	Specifies the minimum time that must elapse between PIM neighbor loss notifications originated by the router.
ip pim invalid-register-notification-period	Specifies the minimum time that must elapse between PIM invalid register notifications originated by the router.
ip pim invalid-joinprune-notification-period	Specifies the minimum time that must elapse between PIM invalid joinprune notifications originated by the router.
ip pim rp-mapping-notification-period	Specifies the minimum time that must elapse between PIM RP mapping notifications originated by this router.
ip pim interface-election-notification-period	Specifies the minimum time that must elapse between the PIM interface election notifications originated by the router.

MIB Objects

```
alaPim
   alaPimNeighborLossNotificationPeriod
   alaPimNeighborLossCount
   alaPimInvalidRegisterNotificationPeriod
   alaPimInvalidRegisterMsgsRcvd
   alaPimInvalidRegisterGroup
   alaPimInvalidRegisterRp
   alaPimInvalidJoinPruneNotificationPeriod
   alaPimInvalidJoinPruneMsgsRcvd
   alaPimInvalidJoinPruneOrigin
   alaPimInvalidJoinPruneGroup
   alaPimInvalidJoinPruneRP
   alaPimRPMappingNotificationPeriod
   alaPimRPMappingChangeCount
   alaPimInterfaceElectionNotificationPeriod
   alaPimInterfaceElectionWinCount
```

show ip pim groute

Displays all (*,G) state that the IPv4 PIM has.

show ip pim groute [*group_address***]**

Syntax Definitions

group_address	A 32-bit multicast address. If an IP address is not specified, the current PIM status for all multicast route entries are displayed.

Defaults

By default, entire (*,G) routing table is displayed. To view more detailed (*,G) state information about a particular group, specify the group address in the command line.

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

When the *group_address* is specified in the command line, the detailed information displayed also includes the detailed state of every outgoing interface.

Examples

```
-> show ip pim groute

Total 1 (*,G)

Group Address   RP Address     RPF Interface       Upstream Neighbor UpTime
---------------+--------------+-------------------+-----------------+-----------
225.0.0.0       212.61.60.8    vlan-30             212.61.30.7       00h:01m:43s
225.0.0.1       212.61.60.8    vlan-30             212.61.30.7       00h:01m:43s


-> show ip pim groute 225.0.0.0
(*,225.0.0.0)
  UpTime                  = 00h:01m:49s
  RP Address              = 212.61.60.8,
  PIM Mode                = ASM,
  PIM Mode Origin         = BSR,
  Upstream Join State     = Joined,
  Upstream Join Timer     = 00h:00m:11s,
  Upstream Neighbor       = 212.61.30.7,
  RPF Interface           = vlan-30,
  RPF Next Hop            = 212.61.30.7,
  RPF Route Protocol      = OSPF,
  RPF Route Address       = 212.61.60.0/24,
  RPF Route Metric Pref   = 110,
  RPF Route Metric        = 2,
  Interface Specific State:
    vlan-4
      UpTime                    = 00h:01m:49s,
```

```
    Local Membership          = True,
    Join/Prune State          = No Info,
    Prune Pending Timer       = 00h:00m:00s,
    Join Expiry Timer         = 00h:00m:00s,
    Assert State              = No Info,
    Assert Timer              = 00h:00m:00s,
  vlan-5
    UpTime                    = 00h:00m:00s,
    Local Membership          = False,
    Join/Prune State          = No Info,
    Prune Pending Timer       = 00h:00m:00s,
    Join Expiry Timer         = 00h:00m:00s,
    Assert State              = No Info,
    Assert Timer              = 00h:00m:00s,
  vlan-8
    UpTime                    = 00h:00m:00s,
    Local Membership          = False,
    Join/Prune State          = No Info,
    Prune Pending Timer       = 00h:00m:00s,
    Join Expiry Timer         = 00h:00m:00s,
    Assert State              = No Info,
    Assert Timer              = 00h:00m:00s,
  vlan-9
    UpTime                    = 00h:00m:00s,
    Local Membership          = False,
    Join/Prune State          = No Info,
    Prune Pending Timer       = 00h:00m:00s,
    Join Expiry Timer         = 00h:00m:00s,
    Assert State              = No Info,
    Assert Timer              = 00h:00m:00s,
  vlan-30
    UpTime                    = 00h:00m:00s,
    Local Membership          = False,
    Join/Prune State          = No Info,
    Prune Pending Timer       = 00h:00m:00s,
    Join Expiry Timer         = 00h:00m:00s,
    Assert State              = No Info,
    Assert Timer              = 00h:00m:00s,
```

output definitions

Group-address	The IPv4 Multicast Group Address.
RP Address	The address of the Rendezvous Point (RP) for the group.
RPF Interface	The RPF interface towards the RP. The ifIndex is converted to the if-name for the display.
Upstream Neighbor	The primary address of the neighbor on the RPF Interface that the local router is sending periodic (*,G) join messages to.
UpTime	The time since this entry was created.
Pim Mode Origin	The mechanism by which the PIM mode and RP for the group were learned.
Upstream Join State	Whether the local router should join the RP tree for the group.
Upstream Join Timer	The time remaining before the local router next sends a periodic (*,G) Join message on the RPF IfIndex.
RPF Next Hop	The address of the RPF next hop towards the RP.

output definitions (continued)

RPF Route Protocol	The routing mechanism through which the route used to find the RPF interface towards the RP was learned.
RPF Route Address/Prefix Length	The IPv6 address combined with the prefix length identifies the route used to find the RPF interface towards the RP.
Route Metric Pref	The metric preference of the route used to find the RPF interface towards the RP.
Route Metric	The routing metric of the route used to find the RPF interface towards the RP.
Interface Name	The interface name that corresponds to the ifIndex.
Local Membership	Whether the local router has (*,G) local membership on this interface.
Join Prune State	The state resulting from (*,G) Join/Prune messages received on this interface.
Prune Pending Timer	The time remaining before the local router acts on a (*,G) Prune message received on this interface, during which the router is waiting to see whether another downstream router overrides the Prune message.
Join Expiry Timer	The time remaining before (*,G) Join state for this interface expires.
Assert State	The (*,G) Assert state for this interface. The possible values are No Info, Winner or Loser.
Assert Timer	If Assert State is 'Winner', this is the time remaining before the local router next sends a (*,G) Assert message on this interface. If the Assert State is 'Loser', this is the time remaining before the (*,G) assert state expires.
Assert Winner Address	If the Assert State is 'Loser', this is the address of the assert winner.
Assert Winner Metric Pref	If the Assert State is 'Loser', this is the metric preference of the route to the RP advertised by the assert winner; otherwise, this is zero.
Assert Winner Metric	If the Assert State is 'Loser', this is the routing metric of the route to the RP advertised by the assert winner; otherwise, this is zero.

Release History

Release 6.3.1; command introduced.

Related Commands

N/A

MIB Objects

```
alaPimStarGTable
   alaPimStarGGrpAddress
   alaPimStarGRPAddress
   alaPimStarGRPFIfIndex
   alaPimStarGUpstreamNeighbor
   alaPimStarGUpTime
   alaPimStarGPimModeOrigin
   alaPimStarGUpstreamJoinState
   alaPimStarGUpstreamJoinTimer
   alaPimStarGRPFNextHop
```

```
   alaPimStarGRPFRouteProtocol
   alaPimStarGRPFRouteAddress
   alaPimStarGRPFRoutePrefixLength
   alaPimStarGRPFRouteMetricPref
   alaPimStarGRPFRouteMetric
alaPimStarGITable
   alaPimStarGIIfIndex
   alaPimStarGILocalMembership
   alaPimStarGIJoinPruneState
   alaPimStarGIPrunePendingTimer
   alaPimStarGIPrunePendingTimer
   alaPimStarGIAssertState
   alaPimStarGIAssertTimer
   alaPimStarGIAssertWinnerAddress
   alaPimStarGIAssertWinnerAddress
   alaPimStarGIAssertWinnerMetric
```

show ip pim sgroute

Displays all (S,G) state that the IPv4 PIM has.

show ip pim sgroute [*source_address group_address***]**

Syntax Definitions

source_address	The 32-bit IP address for a specific multicast source.
group_address	A 32-bit multicast address.

Defaults

By default, entire (S,G) routing table is displayed. To view the detailed information for a particular (S,G) entry, use the *source_address* and *group_address* associated with that entry.

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- When the *source_address* and *group_address* is specified in the command line, the detailed information displayed also includes the detailed state of every outgoing interface.
- If an IP address is not specified, the current PIM status for all multicast route entries are displayed.

Examples

```
-> show ip pim sgroute
Legend: Flags: D = Dense, S = Sparse, s = SSM Group,
               L = Local, R = RPT, T = SPT, F = Register,
               P = Pruned, O = Originator
Total 1 (S,G)

Source Address Group Address RPF Interface  Upstream Neighbor UpTime      Flags
--------------+-------------+--------------+-----------------+-----------+--------
172.21.63.2    225.0.0.0     vlan-30        212.61.30.7       00h:02m:09s ST
172.21.63.2    225.0.0.1     vlan-30        212.61.30.7       00h:02m:09s ST


-> show ip pim sgroute 172.21.63.2 225.0.0.0
(172.21.63.2,225.0.0.0)
  UpTime                  = 00h:02m:16s
  PIM Mode                = ASM,
  Upstream Join State     = Joined,
  Upstream RPT State      = Not Pruned,
  Upstream Join Timer     = 00h:00m:44s,
  Upstream Neighbor       = 212.61.30.7,
  RPF Interface           = vlan-30,
  RPF Next Hop            = 212.61.30.7,
  RPF Route Protocol      = OSPF,
  RPF Route Address       = 172.21.63.0/24,
  RPF Route Metric Pref   = 110,
  RPF Route Metric        = 2,
```

```
SPT Bit                 = True,
DR Register State       = No Info,
DR Register Stop Timer  = 00h:00m:00s,
Interface Specific State:
  vlan-4
    UpTime                    = 00h:02m:16s,
    Local Membership          = True,
    Join/Prune State          = No Info,
    RPT State                 = No Info,
    Prune Pending Timer       = 00h:00m:00s,
    Join Expiry Timer         = 00h:00m:00s,
    Assert State              = No Info,
    Assert Timer              = 00h:00m:00s,
  vlan-5
    UpTime                    = 00h:00m:00s,
    Local Membership          = False,
    Join/Prune State          = No Info,
    RPT State                 = No Info,
    Prune Pending Timer       = 00h:00m:00s,
    Join Expiry Timer         = 00h:00m:00s,
    Assert State              = No Info,
    Assert Timer              = 00h:00m:00s,
  vlan-8
    UpTime                    = 00h:00m:00s,
    Local Membership          = False,
    Join/Prune State          = No Info,
    RPT State                 = No Info,
    Prune Pending Timer       = 00h:00m:00s,
    Join Expiry Timer         = 00h:00m:00s,
    Assert State              = No Info,
    Assert Timer              = 00h:00m:00s,
  vlan-9
    UpTime                    = 00h:00m:00s,
    Local Membership          = False,
    Join/Prune State          = No Info,
    RPT State                 = No Info,
    Prune Pending Timer       = 00h:00m:00s,
    Join Expiry Timer         = 00h:00m:00s,
    Assert State              = No Info,
    Assert Timer              = 00h:00m:00s,
  vlan-30
    UpTime                    = 00h:00m:00s,
    Local Membership          = False,
    Join/Prune State          = No Info,
    RPT State                 = No Info,
    Prune Pending Timer       = 00h:00m:00s,
    Join Expiry Timer         = 00h:00m:00s,
    Assert State              = No Info,
    Assert Timer              = 00h:00m:00s,
```

output definitions

Source-address	The IPv4 Source address.
Group-address	The IPv4 Multicast Group Address.
RPF Interface	The RPF interface towards the RP. The ifIndex is converted to the if-name for the display.

output definitions (continued)

Upstream Neighbor	The primary address of the neighbor on the RPF Interface that the local router is sending periodic (S,G) join messages to.
UpTime	The time since this entry was created.
Flags	Flags indicating SPTBit, Prune State, Join State, and so on.
Pim Mode	Whether the Group Address is SSM, ASM or DM.
Upstream Join State	Whether the local router should join the SPT for the source and group represented by this entry.
Upstream Join Timer	The time remaining before the local router next sends a periodic (S,G) Join message.
RPF Next Hop	The address of the RPF next hop towards the source.
RPF Route Protocol	The routing mechanism through which the route used to find the RPF Interface towards the source was learned.
RPF Route Address/Prefix Length	The IP address which when combined with the Route Prefix length identifies the route used to find the RPF interface towards the source.
RPF Route Metric Pref	The metric preference of the route used to find the RPF interface towards the source.
RPF Route Metric	The metric preference of the route used to find the RPF interface towards the source.
DR Register State	Whether the local router should encapsulate (S,G) data packets in Register messages and send them to the RP. The possible values include No Info, Join, Join Pending, or Prune.
DR Register Stop Timer	The value of the Register Stop Timer. If the Register State is 'prune', this is the time remaining before the local router sends a Null-Register message to the RP. If the State is 'joinPending', this is the time remaining before the local router resumes encapsulating data packets and sending them to the RP.
Upstream Prune State	Whether the local router has pruned itself from the tree. This is only used by PIM-DM. The possible values include forwarding, Ack Pending, or Pruned.
Upstream Prune Limit Timer	The time remaining before the local router may send a (S,G) prune message on alaPimSGRPFIfIndex. This is only used by PIM-DM.
Originator State	Whether this router is an originator for the (S,G) message flow. This is only used by PIM-DM. The possible values include Not Originator or Originator.
Source Active Timer	If this router is the Originator, this is the time remaining before the local router reverts to notOriginator state. Otherwise, this is zero. This is only used by PIM-DM.
State Refresh Timer	If Originator state is 'originator', this is the time remaining before the local router sends a State Refresh Message. Otherwise, this is zero. This is only used by PIM-DM.
Interface Name	The interface name corresponding to the ifIndex that corresponds to this entry.
Uptime	The time since this entry was created.
Local Membership	Whether the local router has (S,G) local membership on this interface.

output definitions (continued)

Join Prune State	The state resulting from (S,G) Join/Prune messages received on this interface. The possible values include No Info, Join, or Prune Pending.
Prune Pending Timer	The time remaining before the local router acts on an (S,G) Prune message received on this interface, during which the router is waiting to see whether another downstream router overrides the Prune message.
Join Expiry Timer	The time remaining before (S,G) Join state for this interface expires.
Assert State	The (S,G) Assert state for this interface. The possible values include No Info, Winner, or Loser.
Assert Timer	If Assert State is Winner, this is the time remaining before the local router sends a (S,G) Assert message on this interface. If the Assert State is Loser, this is the time remaining before the (S,G) Assert state expires.
Assert Winner	If the Assert State is Loser, this is the address of the assert winner.
Assert Winner Metric Pref	If the Assert State is Loser, this is the metric preference of the route to the source advertised by the assert winner.
Assert Winner Metric Metric	If the Assert State is Loser, this is the routing metric of the route to the source advertised by the assert winner.

Release History

Release 6.3.1; command introduced.

Related Commands

N/A

MIB Objects

```
alaPimSGTable
   alaPimSGSrcAddress
   alaPimSGGrpAddress
   alaPimSGRPFIfIndex
   alaPimSGUpstreamNeighbor
   alaPimSGUpTime
   alaPimSGSPTBit
   alaPimSGUpstreamPruneState
   alaPimSGUpstreamJoinState
   alaPimSGPimMode
   alaPimSGUpstreamJoinState
   alaPimSGUpstreamJoinTimer
   alaPimSGRPFNextHop
   alaPimSGRPFRouteProtocol
   alaPimSGRPFRouteAddress
   alaPimSGRPFRoutePrefixLength
   alaPimSGRPFRouteMetricPref
   alaPimSGRPFRouteMetric
   alaPimSGDRRegisterState
   alaPimSGDRRegisterStopTimer
   alaPimSGUpstreamPruneState
   alaPimSGUpstreamPruneLimitTimer
   alaPimSGOriginatorState
   alaPimSGSourceActiveTimer
```

```
   alaPimSGStateRefreshTimer
alaPimSGITable
   alaPimSGIIfIndex
   alaPimSGIUpTime
   alaPimSGILocalMembership
   alaPimSGIJoinPruneState
   alaPimSGIPrunePendingTimer
   alaPimSGIJoinExpiryTimer
   alaPimSGIAssertState
   alaPimSGIAssertTimer
   alaPimSGIAssertWinnerAddress
   alaPimSGIAssertWinnerMetricPref
   alaPimSGIAssertWinnerMetric
```

ipv6 pim sparse status

Enables or disables the IPv6 PIM-SM (sparse mode) globally for IPv6.

ipv6 pim sparse status {enable | disable}

Syntax Definitions

enable	Enables PIM-SM globally for IPv6.
disable	Disables PIM-SM globally for IPv6.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

This command must be set to **enable** before PIM-SM can run on the switch. In addition, the **ip load pim** command must be executed. Refer to page 35-3 for more information.

Examples

```
-> ipv6 pim sparse status enable
-> ipv6 pim sparse status disable
```

Release History

Release 6.3.1; command introduced.

Related Commands

ipv6 pim interface	Enables or disables the PIM protocol on a specific interface.
ip load pim	Dynamically loads PIM to memory.
show ipv6 pim sparse	Displays the status of the various global parameters for the IPv6 PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmV6AdminStatus
```

ipv6 pim dense status

Enables or disables the IPv6 PIM-DM (dense mode) globally for IPv6.

ipv6 pim dense status {enable | disable}

Syntax Definitions

enable	Enables PIM-DM globally for IPv6.
disable	Disables PIM-DM globally for IPv6.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

This command must be set to **enable** before PIM-DM can run on the switch. In addition, the **ip load pim** command must be executed. Refer to page 35-3 for more information.

Examples

```
-> ipv6 pim dense-status enable
-> ipv6 pim dense-status disable
```

Release History

Release 6.3.1; command introduced.

Related Commands

ipv6 pim interface	Enables or disables the PIM protocol on a specific interface.
ip load pim	Dynamically loads PIM to memory.
show ipv6 pim dense	Displays the status of the various global parameters for the IPv6 PIM dense mode.

MIB Objects

```
alaPimdmGlobalConfig
   alaPimdmV6AdminStatus
```

ipv6 pim ssm group

Statically maps the specified IPv6 multicast group(s) to the PIM Source Specific Multicast mode (SSM).

ipv6 pim ssm group *group_address/prefix_length* **[[no] override] [priority** *priority***]**

no ipv6 pim ssm group *group_address/prefix_length*

Syntax Definitions

group_address	Specifies the IPv6 multicast group address.
/prefix_length	Specifies the prefix length of the IPv6 multicast group. Values may range from 4 to 128.
override	Specifies the static SSM mode mapping configuration to override the dynamically learned group mapping information for the specified group(s).
priority	Specifies the preference value to be used for this static SSM mode configuration and provides fine control over which configuration is overridden by this static configuration. Values may range from 0 to 128.

Defaults

By default, the priority option is not set and the override option is set to false.

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a static configuration of a Source Specific Multicast mode group mapping.
- The IPv6 PIM Source-Specific Multicast (SSM) mode for the default SSM address range (FF3x::/32) reserved by the Internet Assigned Numbers Authority is not enabled automatically and must be configured manually to support SSM.
- You can also map additional IPv6 multicast address ranges for the SSM group using this command. However, the IPv6 multicast groups in the reserved address range can be mapped only to the SSM mode.
- If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range
- Specifying the priority value obsoletes the **override** option and once the priority option has been defined, a value of 65535 can be used to change the priority.

Examples

```
-> ipv6 pim ssm group ff30::1234:abcd/128 priority 50
-> no ipv6 pim ssm group ff30::1234:abcd/128
```

Release History

Release 6.3.1; command introduced.

Related Commands

show ipv6 pim group-map	Displays the IPv6 PIM group mapping table.
show ipv6 pim ssm group	Displays the static configuration of IPv6 multicast group mappings for PIM-Source Specific Multicast (SSM).

MIB Objects

```
alaPimStaticRPTable
   alaPimStaticRPGrpAddress
   alaPimStaticRPGrpPrefixLength
   alaPimStaticRPOverrideDynamic
   alaPimStaticRPPrecedence
   alaPimStaticRPRowStatus
```

ipv6 pim dense group

Statically maps the specified IPv6 multicast group(s) to the PIM Dense mode (DM).

ipv6 pim dense group *group_address/prefix_length* **[[no] override] [priority** *priority***]**

no ipv6 pim dense group *group_address/prefix_length*

Syntax Definitions

group_address	Specifies the IPv6 multicast group address.
/prefix_length	Specifies the prefix length of the IPv6 multicast group.
override	Specifies the static dense mode mapping configuration to override the dynamically learned group mapping information for the specified group(s).
priority	Specifies the preference value to be used for this static configuration and provides fine control over which configuration is overridden by this static configuration. Values may range from 0 to 128.

Defaults

By default, the priority option is not set and the override option is set to false.

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a static configuration of a dense mode group mapping.
- This command specifies the mode as Dense (PIM-DM) for the specified IPv6 multicast group addresses.
- If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range.
- Specifying the priority value obsoletes the **override** option and once the priority option has been defined, a value of 65535 can be used to un-set the priority.

Examples

```
-> ipv6 pim dense group ff0e::1234/128 priority 50
-> no ipv6 pim dense group ff0e::1234/128
```

Release History

Release 6.3.1; command introduced.

Related Commands

show ipv6 pim group-map	Displays the IPv6 PIM group mapping table.
show ipv6 pim dense group	Displays the static configuration of IPv6 multicast group mappings for PIM Dense Mode (DM).

MIB Objects

```
alaPimStaticRPTable
   alaPimStaticRPGrpAddress
   alaPimStaticRPGrpPrefixLength
   alaPimStaticRPOverrideDynamic
   alaPimStaticRPPrecedence
   alaPimStaticRPRowStatus
```

ipv6 pim cbsr

Configures the local router as the candidate Bootstrap router (C-BSR) for the PIM IPv6 domain of the specified scope zone.

ipv6 pim cbsr *bsr_address* **[priority** *bsr_priority***] [mask-length** *masklen***] [scope** *scope_value***]**

no ipv6 pim cbsr *bsr_address* **[priority** *bsr_priority***] [mask-length** *masklen***] [scope** *scope_value***]**

Syntax Definitions

bsr_address	The IPv6 unicast address that the local router uses to advertise itself as a Candidate-BSR for PIM IPv6. The specified address must be a domain-wide reachable address.
bsr_priority	The priority value of the local router as a Candidate-BSR. Values may range from 0 to 255. A numerically higher value indicates higher priority
masklen	The hash mask length that is advertised in the Bootstrap messages for IPv6 PIM (the length of the mask is used in the hash function when computing the Rendezvous Point (RP) for a multicast group). Values may range from 1 to 128.
scope_value	The scope value to which this entry applies. The values 3-15 are used to indicate the particular scope to which this BSR applies. If scope value is not used then the C-BSR will be a global (non-scoped) BSR.

Defaults

parameter	default
bsr-priority	64
masklen	126

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove the association of the device as a Candidate-BSR for a PIM domain.
- This command is supported only if PIM is loaded in the system.
- This command is supported only in the sparse mode.
- The information configured using this command is used in the Bootstrap messages.
- Candidate-BSRs also avoid a single point of failure in a PIM domain.

Examples

```
-> ipv6 pim cbsr 2000::1 priority 100 mask-length 4 scope 6
-> no ipv6 pim cbsr 2000::1 scope 6
-> no ipv6 pim cbsr 2000::1
```

Release History

Release 6.3.1; command introduced.
Release 6.3.4; **scope** parameter was added.

Related Commands

show ipv6 pim cbsr	Displays the IPv6 Candidate-BSR information that is used in the Bootstrap messages.

MIB Objects

```
pimBsrCandidateBSRTable
   pimBsrCandidateBSRAddress
   pimBsrCandidateBSRPriority
   pimBsrCandidateBSRHashMaskLength
   pimBsrCandidateBSRZoneIndex
```

ipv6 pim static-rp

Adds, modifies, or deletes a static RP for an IPv6 multicast group (“modifies” applies only to the RP address, since the table is indexed from group address and prefix length parameters).

ipv6 pim static-rp *group_address/prefix_length rp_address* **[[no] override] [priority** *priority***]**

no ipv6 pim static-rp *group_address/prefix_length rp_address*

Syntax Definitions

group_address	Specifies the IPv6 multicast group address.
/prefix_length	Specifies the prefix length of the IPv6 multicast group.
rp_address	Specifies the IPv6 unicast address of the Rendezvous Point (RP). This must be a domain-wide reachable address.
override	Specifies the static RP configuration to override the dynamically learned RP information for the specified group(s).
priority	Specifies the preference value to be used for this static RP configuration and provides fine control over which configuration is overridden by this static configuration. Values may range from 0 to 128.

Defaults

By default, the priority option is not set and the override option is set to false.

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete a static RP configuration.
- Specifying the priority value obsoletes the **override** option.
- The IPv6 PIM Source-Specific Multicast (SSM) mode for the default SSM address range (FF3x::/32) reserved by the Internet Assigned Numbers Authority is not enabled automatically and must be configured manually to support SSM. You can also map additional IPv6 multicast address ranges for the SSM group. However, the IPv6 multicast groups in the reserved address range can be mapped only to the SSM mode.
- If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range
- Note that once the priority option has been defined, a value of 65535 can be used to un-set the priority
- This command is supported only in the sparse mode.

Examples

```
-> ipv6 pim static-rp ff0e::1234/128 2000::1 priority 10
-> no ipv6 pim static-rp ff0e::1234/128 2000::1
```

Release History

Release 6.3.1; command introduced.

Related Commands

show ipv6 pim group-map	Displays the IPv6 PIM group mapping table.
show ipv6 pim static-rp	Displays the IPv6 PIM Static RP table, which includes IPv6 multicast group address/prefix length, the static Rendezvous Point (RP) address, and the current status of the Static RP configuration (that is, enabled or disabled).

MIB Objects

```
alaPimStaticRPTable
   alaPimStaticRPGrpAddress
   alaPimStaticRPGrpPrefixLength
   alaPimStaticRPRPAddress
   alaPimStaticRPOverrideDynamic
   alaPimStaticRPPrecedence
   alaPimStaticRPRowStatus
```

ipv6 pim candidate-rp

Configures the local router as the Candidate-Rendezvous Point (C-RP) for a specified IPv6 multicast group(s).

ipv6 pim candidate-rp *rp_address group_address/prefix_length* **[priority** *priority***] [interval** *seconds***]**

no ipv6 pim candidate-rp *rp_address group_address/prefix_length*

Syntax Definitions

rp_address	Specifies the IPv6 unicast address that will be advertised as a Candidate-RP. This must be a domain-wide reachable address.
group_address	Specifies the IPv6 multicast group address for which the local router advertises itself as a Candidate-RP.
/prefix_length	Specifies the prefix length of the specified IPv6 multicast group address.
priority	Specifies the priority value of the Candidate-RP. Values may range from 0 to 192. The lower the value, the higher the priority.
seconds	Specifies the interval at which the C-RP advertisements are sent to the Bootstrap router, in seconds. Values may range from 1 to 300.

Defaults

parameter	default
priority	192
seconds	60

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove the association of the device as a C-RP for a particular multicast group.
- Only one RP address is supported per switch. If multiple candidate-RP entries are defined, they must specify the same *rp-address.*
- This command is supported only in the sparse mode.

Examples

```
-> ipv6 pim candidate-rp 2000::1 ff0e::1234/128 priority 100 interval 100
-> no ipv6 pim candidate-rp 2000::1 ff0e::1234/128
```

Release History

Release 6.3.1; command introduced.

Related Commands

show ipv6 pim candidate-rp	Displays the IPv6 multicast groups for which the local router advertises itself as a Candidate-RP.

MIB Objects

```
alaPimBsrCandidateRPTable
   alaPimBsrCandidateRPAddress
   alaPimBsrCandidateRPGroupAddress
   alaPimBsrCandidateRPGroupPrefixLength
   alaPimBSrCandidateRPPriority
   alaPimBsrCandidateRPAdvInterval
   alaPimBsrCandidateRPRowStatus
```

ipv6 pim rp-switchover

Enables or disables an RP to attempt switching to native forwarding upon receiving the first register-encapsulated packet in the IPv6 PIM domain.

ipv6 pim rp-switchover {enable | disable}

Syntax Definitions

enable	Enables the RP to switch to native forwarding.
disable	Disables the RP from switching to native forwarding.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- You cannot specify a pre-configured threshold, such as the RP threshold, as you would do for IPv4 PIM.
- This command is supported only in the sparse mode.

Examples

```
-> ipv6 pim rp-switchover enable
-> ipv6 pim rp-switchover disable
```

Release History

Release 6.3.1; command introduced.

Related Commands

show ipv6 pim sparse	Displays the status of the various global parameters for the IPv6 PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmV6RPSwitchover
```

ipv6 pim spt status

Enables or disables last hop Designated Router (DR) switching to the Shortest Path Tree (SPT).

ipv6 pim 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 6850E, 6855, 9000E

Usage Guidelines

- This command is supported only in the sparse mode.
- If the SPT status is enabled, last hop DR switching to the SPT begins once the first data packet is received.

Examples

```
-> ipv6 pim spt status enable
-> ipv6 pim spt status disable
```

Release History

Release 6.3.1; command introduced.

Related Commands

show ipv6 pim sparse	Displays the status of the various global parameters for the IPv6 PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmV6SPTConfig
```

ipv6 pim interface

Enables IPv6 PIM and configures the statistics such as hello-interval, triggered-hello, hello-holdtime, joinprune, prune-delay, override-interval, dr-priority, stub interface, prune limit interval, and graft retry interval on the IPv6 interface.

ipv6 pim interface *if_name* **[hello-interval** *seconds***] [triggered-hello** *seconds***] [joinprune-interval** *seconds***] [hello-holdtime** *seconds***] [joinprune-holdtime** *seconds***] [prune-delay** *milliseconds***] [override-interval** *milliseconds***] [dr-priority** *priority***] [[no] stub] [prune-limit-interval** *seconds***] [graft-retry-interval** *seconds***]**

no ipv6 pim interface *if_name*

Syntax Definitions

if_name	The interface name on which the IPv6 PIM is being enabled or disabled.
hello-interval *seconds*	The frequency at which IPv6 PIM Hello messages are transmitted on this interface, in seconds. Values may range from 0 to 18000.
triggered-hello *seconds*	Specifies the maximum time, in seconds, before a triggered IPv6 PIM Hello message is sent on this interface. Values may range from 0 to 60.
joinprune-interval *seconds*	The frequency at which periodic IPv6 PIM Join/Prune messages are sent on this interface, in seconds. Values may range from 0 to 18000.
hello-holdtime *seconds*	Specifies the value of the IPv6 PIM hello-holdtime for this interface. This value is set in the Holdtime field of IPv6 PIM Hello messages sent on this interface, in seconds. Values may range from 0 to 65535.
joinprune-holdtime *seconds*	Specifies the value that is set in the Holdtime field of the IPv6 PIM Joinprune messages sent on this interface, in seconds.Values may range from 0 to 65535.
prune-delay *milliseconds*	Specifies the value of the expected propagation delay between IPv6 PIM routers on this network, inserted into the LAN prune-delay option of the IPv6 PIM Hello messages sent on this interface, in milliseconds. Values may range from 0 to 32767.
override-interval *milliseconds*	Specifies the value set in the Override Interval field of the LAN prune-delay option of the IPv6 PIM Hello messages sent on this interface, if the prune-delay status is enabled, in *milliseconds.* Values may range from 0 to 65535.
dr-priority *priority*	Specifies the Designated Router priority set in the DR priority option on this interface. The DR priority option value (1–192). A higher numeric value denotes a higher priority.
prune-limit-interval *seconds*	Specifies the minimum interval that must elapse between two successive IPv6 PIM prune messages sent on this interface, in seconds. Values may range from 0 to 65535.
graft-retry-interval *seconds*	Specifies the minimum interval that must elapse between two successive IPv6 PIM graft messages sent on this interface, in seconds. Values may range from 0 to 65535.

stub Specifies the interface not to send any IPv6 PIM packets through this interface, and to ignore received IPv6 PIM packets.

Defaults

parameter	default
hello-interval *seconds*	30
triggered-hello *seconds*	5
joinprune-interval *seconds*	60
hello-holdtime *seconds*	105
joinprune-holdtime *seconds*	210
prune-delay *milliseconds*	500
override-interval *milliseconds*	2500
dr-priority *priority*	1
prune-limit-interval *seconds*	60
graft-retry-interval *seconds*	3
stub	Disabled

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete an IPv6 PIM interface.
- IPv6 PIM must be enabled globally on the switch before IPv6 PIM begins running on the interface. To globally enable or disable IPv6 PIM-SM on the switch, refer to the **ipv6 pim sparse status** command on page 35-79. To enable or disable IPv6 PIM-DM on the switch, refer to the **ipv6 pim dense status** command on page 35-80.
- Specifying zero for IPv6 PIM hello-interval represents an infinite time, in which case the periodic IPv6 PIM hello messages are not sent.
- Specifying zero for IPv6 PIM joinprune-interval represents an infinite time, in which case the periodic IPv6 PIM joinprune messages are not sent.
- Specifying the value of 65535 for IPv6 PIM hello-holdtime represents an infinite time. If an IPv6 PIM router gets IPv6 PIM Hello packet from a neighbor with its hello-holdtime value as infinite time, then the router does not time out the sender(neighbor). It is recommended that you use an IPv6 PIM hello-holdtime interval that is 3.5 times the value of the IPv6 PIM hello-interval, or 65535 seconds if the IPv6 PIM hello-interval is set to zero
- Specifying the value of 65535 for IPv6 PIM joinprune-holdtime represents an infinite time. The receipt of IPv6 Join/Prune messages with its joinprune-holdtime value as infinite time, then this specifies an infinite holdtime for the particular IPv6 join/prune message. It is recommended that you use a join-prune- holdtime interval that is 3.5 times the value of the IPv6 PIM Join/Prune interval defined for the interface, or 65535 seconds if the IPv6 PIM joinprune-interval is set to zero.

- The interface configured as a **stub** does not send any IPv6 PIM packets through that interface, and any received IPv6 PIM packets are also ignored. By default, an IPv6 PIM interface is not set to be a stub one.
- The IPv6 PIM **graft-retry-interval** and **prune-limit-interval** options can be used only with the IPv6 PIM-DM mode.

Examples

```
-> ipv6 pim interface vlan-2 hello-interval 100 triggered-hello 10 joinprune-inter-
val 100 hello-holdtime 350 joinprune-holdtime 400
-> no ipv6 pim interface vlan-2
```

Release History

Release 6.3.1; command introduced.

Related Command

show ipv6 pim interface	Displays detailed IPv6 PIM settings for a specific interface.

MIB Objects

alaPimInterfaceTable

```
alaPimInterfaceIfIndex
alaPimInterfaceStatus
alaPimInterfaceHelloInterval
alaPimInterfaceTrigHelloInterval
alaPimInterfaceJoinPruneInterval
alaPimInterfaceHelloHoldtime
alaPimInterfaceJoinPruneHoldtime
alaPimInterfacePropagationDelay
alaPimInterfaceOverrideInterval
alaPimInerfaceDRPriority
alaPimInterfaceStubInterface
alaPimInterfacePruneLimitInterval
alaPimInterfaceGraftRetryInterval
```

show ipv6 pim sparse

Displays the status of the various global parameters for the IPv6 PIM sparse mode.

show ipv6 pim sparse

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show ipv6 pim sparse
Status                      = enabled,
Keepalive Period            = 210,
Max RPs                     = 32,
Probe Time                  = 5,
Register Suppress Timeout   = 60,
RP Switchover               = enabled,
SPT Status                  = enabled,
```

output definitions

Status	The current global (that is, switch-wide) status of the IPv6 PIM sparse mode. Options include **enabled** and **disabled**.
Keepalive Period	The duration of the Keepalive timer. The default value is 210.
Max RPs	The maximum number of Rendezvous Points (RPs) allowed in the IPv6 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 resumes encapsulating packets from the source to the RP. Values may range from 1 to 300. The default value is 5.
Register Suppress Timeout	The amount of time, in seconds, the Designated Router (DR) stops sending registers to the Rendezvous Point (RP) once a Register-Stop is received (1–300). The default value is 60.

output definitions

RP switchover	The current status of the RP Switchover capability. RP switchover enables or disables an RP to attempt switching to native forwarding upon receiving the first register-encapsulated data packet. Options include **enabled** and **disabled**. The default setting is **enabled**.
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**.

Release History

Release 6.3.1; command introduced.

Related Commands

ipv6 pim rp-switchover	Enables or disables an RP to attempt switching to native forwarding upon receiving the first register-encapsulated packet in the IPv6 PIM domain.
ipv6 pim 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 multicast data packet is received.
ipv6 pim sparse status	Enables or disables the IPv6 PIM-SM (sparse mode) globally for IPv6.
ipv6 pim interface	Enables IPv6 PIM and configures statistics such as hello-interval, triggered-hello, hello-holdtime, joinprune, prune-delay, override-interval, dr-priority, stub interface, prune limit interval, and graft retry interval on the interface.
ip pim max-rps	Configures the maximum number of C-RP routers allowed in the PIM-SM domain.
ip pim 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 resumes encapsulating packets from the source to the RP.
ip pim register-suppress-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 message.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmV6AdminStatus
   alaPimKeepalivePeriod
   alaPimsmMaxRPS
   alaPimsmProbeTime
   alaPimRegisterSuppressionTime
   alaPimsmV6RPSwitchover
   alaPimsmV6AdminSPTConfig
```

show ipv6 pim dense

Displays the status of the various global parameters for the IPv6 PIM dense mode.

show ipv6 pim dense

Syntax Definitions

N/A.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show ipv6 pim dense
Status                       = enabled,
Source Lifetime              = 210,
State Refresh Interval       = 60,
State Refresh Limit Interval = 0,
State Refresh TTL            = 16
```

output definitions

Status	The current global (that is, switch-wide) status of the IPv6 PIM dense mode. Options include **enabled** and **disabled**.
Source Lifetime	The duration of the Keepalive or Source Lifetime timer. The default value is 210.
State Refresh Interval	The time-interval, in seconds, between successive State Refresh messages originated by the router. The default value is 60.
State Refresh Limit Interval	Displays the limit at which a router does not forward the State Refresh messages, if they are received at less than the interval. The default value is 0.
State Refresh TTL	Displays the TTL to be used in the router's originated State Refresh messages. The default value is 16.

Release History

Release 6.3.1; command introduced.

Related Commands

ipv6 pim dense status	Enables or disables IPv6 PIM-DM (dense mode) globally on the switch.
ip pim keepalive-period	Configures the period during which the (S,G) Join state is maintained in the absence of (S,G) Join messages or explicit (S,G) local membership.
ip pim state-refresh-interval	Sets the interval between successive State Refresh messages originated by a router.
ip pim state-refresh-limit	Sets the limit at which a router does not forward successive State Refresh messages if they are received at less than the interval.
ip pim state-refresh-ttl	Sets the Time to Live to be used in a router's originated State Refresh messages if the data packet's Time to Live is not recorded.

MIB Objects

```
alaPimdmGlobalConfig
   alaPimdmV6AdminStatus
   alaPimKeepalivePeriod
   alaPimRefreshInterval
   alaPimdmStateRefreshLimitInterval
   alaPimdmStateRefreshTimeToLive
```

show ipv6 pim ssm group

Displays the static configuration of IPv6 multicast group mappings for PIM-Source Specific Multicast (SSM).

show ipv6 pim ssm group

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range.

Examples

```
-> show ipv6 pim ssm group

Group Address/Pref Length   Mode  Override Precedence Status
--------------------------+-----+--------+----------+--------
ff00::/8                   ssm    false    none       enabled
ff34::/32                  ssm    false    none       enabled
```

output definitions

Group Address/Pref Length	The IPv6 multicast group address along with the prefix length.
Mode	The IPv6 PIM mode that is used for the groups in this prefix.
Override	Specifies this static RP configuration to override the dynamically learned RP information for the specified group(s).
Precedence	The precedence value that can be used for this static RP configuration.
Status	Displays whether this entry is currently enabled or disabled. Options include **enabled** and **disabled**.

Release History

Release 6.3.1; command introduced.

Related Commands

ipv6 pim ssm group	Statically maps the specified IPv6 multicast group(s) to the PIM Source Specific Multicast mode (SSM).

MIB Objects

```
alaPimStaticRPTable
   alaPimStaticRPGrpAddress
   alaPimStaticRPGrpPrefixLength
   alaPimStaticRPPimMode
   alaPimStaticRPOverrideDynamic
   alaPimStaticRPPrecedence
   alaPimStaticRPRowStatus
```

show ipv6 pim dense group

Displays the static configuration of IPv6 multicast group mappings for PIM Dense Mode (DM).

show ipv6 pim dense group

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range.

Examples

```
-> show ipv6 pim dense group
Group Address/Pref Length   Mode  Override Precedence Status
---------------------------+-----+--------+----------+--------
ff00::/8                    dm    false    none       enabled
ff34::/32                   dm    false    none       enabled
```

output definitions

Group Address/Pref Length	The IPv6 multicast group address along with the prefix length.
Mode	The IPv6 PIM mode that is used for the groups in this prefix.
Override	Specifies this static RP configuration to override the dynamically learned RP information for the specified group(s).
Precedence	The precedence value that can be used for this static RP configuration.
Status	Displays whether this entry is currently enabled or disabled. Options include **enabled** and **disabled**.

Release History

Release 6.3.1; command introduced.

Related Commands

ipv6 pim dense group	Statically maps the specified IPv6 multicast group(s) to the PIM Dense mode (DM).

MIB Objects

```
alaPimStaticRPTable
   alaPimStaticRPRowStatus
   alaPimStaticRPGrpPrefixLength
   alaPimStaticRPPimMode
   alaPimStaticRPOverrideDynamic
   alaPimStaticRPPrecedence
   alaPimStaticRPGrpAddress
```

show ipv6 pim interface

Displays detailed IPv6 PIM settings for a specific interface. In general, it displays IPv6 PIM settings for all the interfaces if no argument is specified.

show ipv6 pim interface [*if_name***]**

Syntax Definitions

if_name	The name of the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

To view more detailed information about a particular interface, specify the interface name in the command line. Additional information includes Triggered Hello Interval, Hello Holdtime, Prune Delay status and value, Override Interval, LAN Delay status, Generation ID status, and Join/Prune Holdtime.

Examples

```
-> show ipv6 pim interface

Interface Name       Designated                Hello    Join/Prune Oper
                     Router                    Interval Interval   Status
--------------------+-------------------------+--------+----------+---------
vlan-5               fe80::2d0:95ff:feac:a537   30       60         enabled
vlan-30              fe80::2d0:95ff:feac:a537   30       60         disabled
vlan-40              fe80::2d0:95ff:fee2:6eec   30       60         enabled

-> show ipv6 pim interface vlan-5
Interface Name              = vlan-5,
IP Address                  = fe80::2d0:95ff:fee2:6eec,
Designated Router           = fe80::2d0:95ff:fee2:a537,
Hello Interval              = 30,
Triggered Hello Interval    = 5,
Hello HoldTime              = 105,
Join/Prune Interval         = 60,
Join/Prune HoldTime         = 210,
Propagation (Prune) Delay   = 500,
Override Interval           = 2500,
Generation ID               = 0x4717be4d,
DR Priority                 = 1,
DR Priority Enabled         = true,
Lan Delay Enabled           = true,
Effective Propagation Delay = 500,
Effective Override Interval = 2500,
Suppression Enabled         = true,
Stub Interface              = false,
```

```
Prune Limit Interval        = 60,
Graft Retry Interval        = 3,
State Refresh Enabled       = true,
Operational Status          = enabled
```

output definitions

Interface Name	The name of the IPv6 PIM interface.
IPv6 address	Specifies the IPv6 address of the specified interface.
Designated Router	The primary 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 acts as the DR.
Hello Interval	The frequency at which PIM Hello messages are transmitted on a specified interface. Values may range from 1 to 18000. The default value is 30.
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 0 to 18000. The default value is 60.
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 0 to 60. The default value is 5.
Hello Holdtime	The current Hello Holdtime value. This value indicates the maximum amount of time, in seconds, Hello messages is held before they are considered invalid. Values may range from 0 to 65535. The default value is 105.
Join/Prune Holdtime	The current Join/Prune Holdtime value. This value indicates the maximum amount of time, in seconds, Join/Prune messages is held before they are considered invalid. Values may range from 0 to 65535. The default value is 210.
Propagation Delay	The expected propagation delay between PIM routers on the network. Values may range from 0 to 32767. The default value is 500.
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 to 65535. The default value is 2500.
Generation ID Option	The value of the Generation ID this router inserted in the last PIM Hello message it sent on this interface.
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 to 192. 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.
Lan Delay Enabled	Options include **true** and **false**. The value is true if all neighbors on the interface are using the LAN Prune Delay option. Otherwise, the setting is false.
Effective Propagation Delay	The Effective Propagation Delay on this interface.

output definitions (continued)

Effective Override Interval	The Effective Override Interval on this interface.
Suppression Enabled	Specifies whether the Join suppression is enabled on this interface.
DR Priority Enabled	Evaluates to TRUE if all routers on this interface are using the DR Priority option.
Stub Interface	Specifies whether this interface is a 'stub interface'. If this is TRUE, then no PIM packets are sent out on this interface, and any received PIM packets are ignored.
Prune Limit Interval	The minimum interval that must transpire between two successive Prunes sent by a router. This is used only with PIM-DM. Values may range from 0 to 65535. The default value is 60.
Graft Retry Interval	Displays the time-interval a router waits for a Graft acknowledgment before resending a Graft on the interface. This is only used with PIM-DM. Values may range from 0 to 65535. The default value is 3.
SR Priority Enabled	Evaluates to TRUE if all routers on this interface are using the State Refresh option. This is used only by PIM-DM.
Operational Status	The current operational status of the corresponding interface. Options include **enabled** and **disabled**. This value indicates whether the IPv6 interface is operationally up. For example, if PIM is enabled on the interface, but the interface is currently down, this field displays as disabled. The default setting is **disabled**. To enable or disable PIM on an interface, refer to the **ipv6 pim interface** command on page 35-93. To globally enable or disable PIM on the switch, refer to the **ipv6 pim sparse status** command on page 35-79 and **ipv6 pim dense status** command on page 35-80.

Release History

Release 6.3.1; command introduced.

Related Commands

ipv6 pim interface	Enables IPv6 PIM and configures statistics such as hello-interval, triggered-hello, hello-holdtime, joinprune, prune-delay, override-interval, dr-priority, stub interface, prune limit interval, and graft retry interval on the interface.

MIB Objects

```
alaPimInterfaceTable
   alaPimInterfaceIfIndex
   alaPimInterfaceDR
   alaPimInterfaceHelloInterval
   alaPimInterfaceJoinPruneInterval
   alaPimInterfaceStatus
   alaPimInterfaceAddress
   alaPimInterfaceTrigHelloInterval
   alaPimInterfaceHelloHoldtime
   alaPimInterfaceJoinPruneHoldtime
   alaPimInterfacePropagationDelay
   alaPimInterfaceOverrideInterval
   alaPimInterfaceGenerationIDValue
```

```
alaPimInterfaceDRPriority
alaPimInterfaceLanDelayEnabled
alaPimInterfaceEffectPropagDelay
alaPimInterfaceEffectOverrideIvl
alaPimInterfaceSuppressionEnabled
alaPimInterfaceDRPriorityEnabled
alaPimInterfaceStubInterface
AlaPimInterfacePruneLimitInterval
alaPimInterfaceGraftRetryInterval
alaPimInterfaceSRPriorityEnabled
```

show ipv6 pim neighbor

Displays a list of active IPv6 PIM neighbors.

show ipv6 pim neighbor [*ipv6_address***] [***if_name***]**

Syntax Definitions

ipv6_address	The IPv6 address for the PIM neighbor.
if_name	The name of the interface.

Defaults

If the neighbor's IPv6 address or interface name is not specified, the entire IPv6 PIM neighbor table is displayed.

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

To view more detailed information about a particular neighbor, specify the neighbor's IPv6 address or the associated interface name in the command line. Additional information is displayed, which includes LAN Prune Delay, Override Interval, TBit field, State Refresh capable, and Designated Router option status.

Examples

```
-> show ipv6 pim neighbor
Neighbor Address               Interface Name       Uptime      Expires     DR Pri
------------------------------+--------------------+-----------+-----------+------
fe80::2d0:95ff:feac:a537       vlan-30               02h:56m:51s 00h:01m:28s 1
```

If a specific neighbor address is specified in the command line, *detailed information for the corresponding neighbor only* displays:

```
-> show ipv6 pim neighbor fe80::2d0:95ff:feac:a537
vlan-30
  Neighbor IPv6 Address        = fe80::2d0:95ff:feac:a537,
  Uptime                       = 02h:57m:09s,
  Expires                      = 00h:01m:40s,
  Lan Prune Delay Present      = True,
  Propagation Delay            = 500,
  Override Interval            = 2500,
  TBit Field                   = True,
  Gen ID Present               = True,
  Gen ID Value                 = 0x7720c123,
  BiDir Capable                = False,
  DR Priority Present          = True,
  DR Priority                  = 1,
  State Refresh Capable        = True,
  Secondary Addresses:
```

```
    3000::11

vlan-40
  Neighbor IPv6 Address        = fe80::2d0:95ff:feac:a537,
  Uptime                       = 03h:57m:03s,
  Expires                      = 00h:01m:20s,
  Lan Prune Delay Present            = True,
  Propagation Delay            = 500,
  Override Interval            = 2500,
  TBit Field                   = True,
  Gen ID Present               = True,
  Gen ID Value                 = 0x7720c123,
  BiDir Capable                = False,
  DR Priority Present          = True,
  DR Priority                  = 1,
  State Refresh Capable        = True,
  Secondary Addresses:
    4000::11
```

If a specific interface name is specified in the command line, *detailed information corresponding to all neighbors on the specified interface only* displays:

```
-> show IPv6 pim neighbor vlan-30
vlan-30
  Neighbor IPv6 Address        = fe80::2d0:95ff:feac:a537,
  Uptime                       = 02h:57m:09s,
  Expires                      = 00h:01m:40s,
  Lan Prune Delay Present            = True,
  Propagation Delay            = 500,
  Override Interval            = 2500,
  TBit Field                   = True,
  Gen ID Present               = True,
  Gen ID Value                 = 0x7720c123,
  BiDir Capable                = False,
  DR Priority Present          = True,
  DR Priority                  = 1,
  State Refresh Capable        = True,
  Secondary Addresses:
    3000::11
```

output definitions

Neighbor IPv6 Address	The IPv6 address of the active PIM neighbor.
Interface Name	The name of the IPv6 PIM interface that is used to reach the neighbor.
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 is aged out, displayed in hours, minutes, and seconds.
LAN Prune Delay present	Specifies whether this neighbor is using the LAN Prune Delay option. Options include **true** or **false**.
Propagation Delay	The value of the propagation-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.

output definitions (continued)

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 to 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.
Gen ID present	Specifies whether this neighbor is using Generation ID option. Options include **true** or **false**.
Gen ID Value	The value of the Generation ID in the last PIM Hello message received from this neighbor.
BiDir Capable	Specifies whether this neighbor is using the Bidirectional-PIM Capable option.
DR Priority Present	Displays whether the neighbor is using the Designated Router option. Options include **true** or **false**.
DR priority	The value of the Designated Router Priority in the last PIM Hello message received from this neighbor.
State Refresh Capable	Displays whether the neighbor is capable of receiving State Refresh messages. Options include **true** or **false**.
Secondary Addresses	The secondary IPv6 address of this PIM neighbor.

Release History

Release 6.3.1; command introduced.

Related Commands

N/A

MIB Objects

```
alaPimNeighborTable
   alaPimNeighborAddress
   alaPimNeighborIfIndex
   alaPimNeighborUpTime
   alaPimNeighborExpiryTime
   alaPimNeighborLanPruneDelayPresent
   alaPimNeighborPropagationDelay
   alaPimNeighborTBit
   alaPimNeighborGenerationIDPresent
   alaPimNeighborGenerationIDValue
   alaPimNeighborBidirCapable
   alaPimNeighborDRPriorityPresent
   alaPimNeighborDRPriority
   alaPimNeighborSRCapable
```

```
alaPimNbrSecAddressTable
   alaPimNbrSecAddress
```

show ipv6 pim static-rp

Displays the IPv6 PIM Static RP table, which includes IPv6 multicast group address/prefix length, the static Rendezvous Point (RP) address, and the current status of the static RP configuration (that is, enabled or disabled).

show ipv6 pim static-rp

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range.

Examples

```
-> show ipv6 pim static-rp

Group Address/Pref Length   RP Address    Mode  Override Precedence Status
---------------------------+-------------+-----+--------+----------+--------
ff00::/8                    3000::11      asm   false    none       enabled
ff34::/32                   3000::11      asm   false    none       enabled
```

output definitions

Group Address/Pref Length	The IPv6 multicast group address along with the prefix length.
RP Address	The IPv6 address of the RP that is mapped for the groups within the group prefix. This field is set to zero, if the specified IPv6 PIM mode is SSM or DM.
Mode	The IPv6 PIM mode that is used for the groups in this prefix. The possible values include ASM, SSM, or DM.
Override	Specifies that this static RP configuration can override the dynamically learned RP information for the specified group(s).
Precedence	The precedence value that is used for this static RP configuration.
Status	Displays whether the static RP configuration is currently enabled or disabled. Options include **enabled** and **disabled**.

Release History

Release 6.3.1; command introduced.

Related Commands

ipv6 pim static-rp	Adds, modifies, or deletes a static RP for an IPv6 multicast group (“modifies” applies only to the RP address, since the table is indexed from group address and prefix length parameters).

MIB Objects

```
alaPimStaticRPTable
   alaPimStaticRPGrpAddress
   alaPimStaticRPGrpPrefixLength
   alaPimStaticRPAddress
   alaPimStaticRPPimMode
   alaPimStaticRPOverrideDynamic
   alaPimStaticRPRowStatus
   alaPimStaticRPPrecedence
```

show ipv6 pim group-map

Displays the IPv6 PIM group mapping table.

show ipv6 pim group-map [bsr | static-rp | ssm | dense]

Syntax Definitions

N/A

Defaults

If the keywords **bsr**, **static-rp**, **ssm**, or **dense** are included in the command line, then only the entries that were created by the specified origin are displayed.

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- If static RP configuration is being used, this information is obtained from those static RP addresses that are defined through the **ipv6 pim static-rp** command. As long as the RP addresses defined in the static RP set are reachable, they are added to the group mapping table.
- If the IPv6 multicast groups are mapped to the mode DM or SSM, then the entries created by local SSM address range configuration using the **ipv6 pim ssm group** command and local Dense Mode address range configuration using the **ipv6 pim dense group** command are displayed.
- 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 Bootstrap messages).

Examples

```
-> show ipv6 pim group-map
Origin    Group Address/Pref Length   RP Address    Mode  Precedence
---------+--------------------------+-------------+-----+-----------
BSR       ff00::/8                   3000::11      asm   192
BSR       ff00::/8                   4000::7       asm   192
SSM       ff33::/32                                ssm

-> show ipv6 pim group-map bsr
Origin    Group Address/Pref Length   RP Address    Mode  Precedence
---------+--------------------------+-------------+-----+-----------
BSR       ff00::/8                   3000::11      asm   192
BSR       ff00::/8                   4000::7       asm   192

-> show ipv6 pim group-map ssm
Origin     Group Address/Pref Length   RP Address    Mode  Precedence
---------+--------------------------+-------------+-----+-----------
```

```
SSM       ff33::/32                                ssm
```

output definitions

Origin	The mechanism by which the PIM mode and RP for the group were learned. The possible values include 'static RP' for local static RP configuration, 'static SSM' for both static SSM group configuration and Dense Mode Group configuration, and 'BSR' for the PIM Bootstrap Router mechanism.
Group Address/Prefix Length	The IPv6 multicast group address along with the prefix length.
RP Address	The IPv6 address of the Rendezvous Point to be used for groups within the group prefix.
Mode	The IPv6 PIM mode to be used for groups in this prefix.
Mapping Precedence	The precedence value of a particular row, that determines which row applies to a given group address. Numerically higher values for this object indicate lower precedences, with the value zero denoting the highest precedence.

Release History

Release 6.3.1; command introduced.

Related Commands

ipv6 pim static-rp	Adds, modifies, or deletes a static RP for an IPv6 multicast group (“modifies” applies only to the RP address, since the table is indexed from group address and prefix length parameters).
ipv6 pim ssm group	Statically maps the specified IPv6 multicast group(s) to the PIM Source Specific Multicast mode (SSM).
ipv6 pim dense group	Statically maps the specified IPv6 multicast group(s) to the PIM Dense mode (DM).

MIB Objects

```
alaPimGroupMappingTable
   alaPimGroupMappingOrigin
   alaPimGroupMappingGrpAddress
   alaPimGroupMappingGrpPrefixLength
   alaPimGroupMappingRPAddress
   alaPimGroupMappingPimMode
   alaPimGroupMappingPrecedence
```

show ipv6 pim candidate-rp

Displays the IPv6 multicast groups for which the local router advertises itself as a Candidate-RP.

show ipv6 pim candidate-rp

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show ipv6 pim candidate-rp
RP Address         Group Address   Priority  Interval  Status
-----------------+---------------+---------+---------+--------
3000::11           FF00::/8        192       60        enabled
```

output definitions

RP Address	An IPv6 unicast address that is advertised as the Candidate-Rendezvous Point (RP).
Group Address	The IPv6 multicast group address along with the prefix length. This is the group for which the local router advertises itself as a C-RP.
Priority	The C-RP router's priority. The lower the value, the higher the priority.
Interval	The time interval at which the C-RP advertisements are sent to the BSR.
Status	The current status of this entry. The status is shown as enabled only if the IPv6 PIM-SM is globally enabled and the IPv6 PIM interface is enabled.

Release History

Release 6.3.1; command introduced.

Related Commands

ipv6 pim candidate-rp	Configures the local router as the Candidate-Rendezvous Point (C-RP) for a specified IPv6 multicast group(s).

MIB Objects

```
alaPimBsrCandidateRPTable
   alaPimBsrCandidateRPAddress
   alaPimBsrCandidateRPGroupAddress
   alaPimBsrCandidateRPGroupPrefixLength
   alaPimBsrCandidateRPPriority
   alaPimBsrCandidateRPInterval
   alaPimBsrCandidateRPStatus
```

show ipv6 pim cbsr

Displays the IPv6 Candidate-BSR information that is used in the Bootstrap messages. If the scope argument is not included in the command line, then this command displays C-BSR information for all known scope zones.

show ipv6 pim cbsr [scope *scope_value***]**

Syntax Definitions

scope_value	This is an optional argument used to display the C-BSR information associated with a particular scope zone.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show ipv6 pim cbsr

CBSR Global Scope
 CBSR Address             = 8000::7,
 Status                   = enabled,
 CBSR Priority            = 0,
 Hash Mask Length         = 126,
 Elected BSR              = False,
 Timer                    = 00h:00m:00s

CBSR Scope Zone:6
 CBSR Address             = 3000::7,
 Status                   = enabled,
 CBSR Priority            = 0,
 Hash Mask Length         = 126,
 Elected BSR              = False,
 Timer                    = 00h:00m:00s

-> show ipv6 pim cbsr scope 6

CBSR Scope Zone:6
 CBSR Address             = 3000::7,
 Status                   = enabled,
 CBSR Priority            = 0,
 Hash Mask Length         = 126,
```

```
Elected BSR              = False,
Timer                    = 00h:00m:00s
```

output definitions

Scope	IPv6 scope value that ranges from 3-15. It is used to define Candidate BSR information associated with a particular scope zone.
CBSR Address	An IPv6 unicast address that the local router uses to advertise itself as a Candidate-BSR for PIM IPv6.
Status	The current status of this entry. The status is shown as enabled only if the IPv6 PIM-SM is globally enabled and the IPv6 PIM interface is enabled.
CBSR Priority	The priority value for the local router as a Candidate-BSR. The higher the value, the higher the priority.
Hash Mask Length	The hash mask length that is advertised in the Bootstrap messages (the length of the mask is used in the hash function when computing the Rendezvous Point (RP) for an IPv6 multicast group).
Elected BSR	Specifies whether the local router is the elected BSR for PIM IPv6.
Timer	The time that is remaining before the local router originates the next Bootstrap message. This value is zero if this router is not the elected BSR.

Release History

Release 6.3.1; command introduced.
Release 6.3.4; **scope** parameter was added.

Related Commands

ipv6 pim cbsr	Configures the Candidate-BSR information that is used in the Bootstrap messages.

MIB Objects

```
pimBsrCandidateBSRTable
   pimBsrCandidateBSRZoneIndex
   pimBsrCandidateBSRAddress
   pimBsrCandidateBSRPriority
   pimBsrCandidateBSRHashMaskLength
   pimBsrCandidateBSRElectedBSR
   pimBsrCandidateBSRBootstrapTimer
   pimBsrCandidateBSRStatus
```

show ipv6 pim bsr

Displays information about the elected BSR for PIM IPv6. If the scope argument is included in the command line, then this command displays BSR information of the specified scope zone. If the scope argument is not included in the command line then BSR information for all the known scope zones is displayed.

show ipv6 pim bsr [scope *scope_value***]**

Syntax Definitions

scope_value	This is an optional argument used to display BSR information of a particular scope zone.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show ipv6 pim bsr

BSR Global Scope
 BSR Address              = 8000::7,
 BSR Priority             = 192,
 Hash Mask Length         = 126,
 Expiry Time              = 00h:01m:35s

BSR Scope Zone:6
 BSR Address              = 3000::7,
 BSR Priority             = 192,
 Hash Mask Length         = 126,
 Expiry Time              = 00h:01m:32s

->show ipv6 pim bsr scope 6

BSR Scope Zone:3
 BSR Address              = 3000::7,
 BSR Priority             = 192,
 Hash Mask Length         = 126,
 Expiry Time              = 00h:01m:32s
```

output definitions

Scope	IPv6 scope value that ranges from 3-15. It is used to define BSR information associated with a particular scope zone.
BSR Address	The IPv6 unicast address of the elected BSR.
BSR Priority	The priority value of the elected BSR. The higher the value, the higher the priority.
Hash Mask Length	The hash mask length that is advertised in the Bootstrap messages by the elected BSR (the length of the mask is used in the hash function when computing the Rendezvous Point (RP) for a multicast group.
Expiry Time	The minimum time remaining before the elected BSR for PIM IPv6 is declared down.

Release History

Release 6.3.1; command introduced.
Release 6.3.4; **scope** parameter was added.

Related Commands

ipv6 pim cbsr	Configures the Candidate-BSR information that is used in the Bootstrap messages.

MIB Objects

```
pimBsrElectedBSRTable
   pimBsrElectedBSRZoneIndex
   pimBsrElectedBSRAddress
   pimBsrElectedBSRPriority
   pimBsrElectedBSRHashMaskLength
   pimBsrElectedBSRExpiryTime
```

show ipv6 pim groute

Displays all (*,G) state that the IPv6 PIM has.

show ipv6 pim groute [*group_address***]**

Syntax Definitions

group_address	The IPv6 address of the Multicast Group.

Defaults

By default, entire (*,G) routing table is displayed. To view more detailed (*,G) state information about a particular group, specify the group address in the command line.

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

When the *group_address* is specified in the command line, the detailed information displayed also includes the detailed state of every outgoing interface.

Examples

```
-> show ipv6 pim groute
Total 1 (*,G)

Group Address          RP Address          RPF Interface                UpTime
----------------------+-------------------+----------------------------+-----------
ff0e::7                5ffe::3             vlan-4                       00h:01m:23s


-> show ipv6 pim groute ff0e::7
(*,ff0e::7)
  UpTime                  = 00h:01m:28s
  RP Address              = 5ffe::3,
  PIM Mode                = ASM,
  PIM Mode Origin         = BSR,
  Upstream Join State     = Not Joined,
  Upstream Join Timer     = 00h:00m:00s,
  Upstream Neighbor       = fe80::220:fcff:fe1e:2455,
  RPF Interface           = vlan-4,
  RPF Next Hop            = fe80::220:fcff:fe1e:2455,
  RPF Route Protocol      = Static,
  RPF Route Address       = 5ffe::3/128,
  RPF Route Metric Pref   = 10,
  RPF Route Metric        = 10,
  Interface Specific State:
    vlan-3
      UpTime                    = 00h:01m:28s,
      Local Membership          = False,
      Join/Prune State          = Joined,
      Prune Pending Timer       = 00h:00m:00s,
```

```
    Join Expiry Timer         = 00h:02m:02s,
    Assert State              = Loser,
    Assert Timer              = 00h:01m:32s,
    Assert Winner Address     = fe80::220:fcff:fe1e:2454,
    Assert Winner Metric Pref = 9 (rpt),
    Assert Winner Metric      = 10,
  vlan-4
    UpTime                    = 00h:00m:00s,
    Local Membership          = False,
    Join/Prune State          = No Info,
    Prune Pending Timer       = 00h:00m:00s,
    Join Expiry Timer         = 00h:00m:00s,
    Assert State              = No Info,
    Assert Timer              = 00h:00m:00s,
  vlan-5
    UpTime                    = 00h:00m:00s,
    Local Membership          = False,
    Join/Prune State          = No Info,
    Prune Pending Timer       = 00h:00m:00s,
    Join Expiry Timer         = 00h:00m:00s,
    Assert State              = No Info,
    Assert Timer              = 00h:00m:00s,
```

output definitions

Group-address	The IPv6 Multicast Group Address.
RP Address	The address of the Rendezvous Point (RP) for the group.
RPF Interface	The RPF interface towards the RP. The ifIndex is converted to the if-name for the display.
Upstream Neighbor	The primary address of the neighbor on the RPF Interface that the local router is sending periodic (*,G) join messages to.
UpTime	The time since this entry was created.
Pim Mode Origin	The mechanism by which the PIM mode and RP for the group were learned.
Upstream Join State	Whether the local router should join the RP tree for the group.
Upstream Join Timer	The time remaining before the local router next sends a periodic (*,G) Join message on the RPF IfIndex.
RPF Next Hop	The address of the RPF next hop towards the RP.
RPF Route Protocol	The routing mechanism through which the route used to find the RPF interface towards the RP was learned.
RPF Route Address/Prefix Length	The IPv6 address combined with the prefix length identifies the route used to find the RPF interface towards the RP.
Route Metric Pref	The metric preference of the route used to find the RPF interface towards the RP.
Route Metric	The routing metric of the route used to find the RPF interface towards the RP.
Interface Name	The interface name that corresponds to the ifIndex.
Local Membership	Whether the local router has (*,G) local membership on this interface.
Join Prune State	The state resulting from (*,G) Join/Prune messages received on this interface.

output definitions (continued)

Prune Pending Timer	The time remaining before the local router acts on a (*,G) Prune message received on this interface, during which the router is waiting to see whether another downstream router overrides the Prune message.
Join Expiry Timer	The time remaining before (*,G) Join state for this interface expires.
Assert State	The (*,G) Assert state for this interface. The possible values are No Info, Winner or Loser.
Assert Timer	If Assert State is 'Winner', this is the time remaining before the local router next sends a (*,G) Assert message on this interface. If the Assert State is 'Loser', this is the time remaining before the (*,G) assert state expires.
Assert Winner Address	If the Assert State is 'Loser', this is the address of the assert winner.
Assert Winner Metric Pref	If the Assert State is 'Loser', this is the metric preference of the route to the RP advertised by the assert winner; otherwise, this is zero.
Assert Winner Metric	If the Assert State is 'Loser', this is the routing metric of the route to the RP advertised by the assert winner; otherwise, this is zero.

Release History

Release 6.3.1; command introduced.

Related Commands

N/A

MIB Objects

```
alaPimStarGTable
   alaPimStarGGrpAddress
   alaPimStarGRPAddress
   alaPimStarGRPFIfIndex
   alaPimStarGUpstreamNeighbor
   alaPimStarGUpTime
   alaPimStarGPimModeOrigin
   alaPimStarGUpstreamJoinState
   alaPimStarGUpstreamJoinTimer
   alaPimStarGRPFNextHop
   alaPimStarGRPFRouteProtocol
   alaPimStarGRPFRouteAddress
   alaPimStarGRPFRoutePrefixLength
   alaPimStarGRPFRouteMetricPref
   alaPimStarGRPFRouteMetric
alaPimStarGITable
   alaPimStarGIIfIndex
   alaPimStarGILocalMembership
   alaPimStarGIJoinPruneState
   alaPimStarGIPrunePendingTimer
   alaPimStarGIPrunePendingTimer
   alaPimStarGIAssertState
   alaPimStarGIAssertTimer
   alaPimStarGIAssertWinnerAddress
   alaPimStarGIAssertWinnerAddress
```

```
alaPimStarGIAssertWinnerMetric
```

show ipv6 pim sgroute

Displays all (S,G) state that the IPv6 PIM has.

show ipv6 pim sgroute [*source_address group_address***]**

Syntax Definitions

source_address	The IPv6 address for a specific multicast source.
group_address	A IPv6 multicast address.

Defaults

By default, entire (S,G) routing table is displayed. To view the detailed information for a particular (S,G) entry, use the *source_address* and *group_address* associated with that entry.

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- When the *source_address* and *group_address* is specified in the command line, the detailed information displayed also includes the detailed state of every outgoing interface.
- If an IPv6 address is not specified, the current PIM status for all multicast route entries are displayed.

Examples

```
-> show ipv6 pim sgroute

Legend: Flags: D = Dense, S = Sparse, s = SSM Group,
               L = Local, R = RPT, T = SPT, F = Register,
               P = Pruned, O = Originator

Total 1 (S,G)

Source Address        Group Address         RPF Interface    UpTime      Flags
---------------------+---------------------+----------------+-----------+------
8ffe::3               ff0e::7                                00h:01m:34s  SR


-> show ipv6 pim sgroute 8ffe::3 ff0e::7
(8ffe::3,ff0e::7)
  UpTime                  = 00h:01m:40s
  PIM Mode                = ASM,
  Upstream Join State     = Not Joined,
  Upstream RPT State      = Not Pruned,
  Upstream Join Timer     = 00h:00m:00s,
  Upstream Neighbor       = none,
  SPT Bit                 = False,
  DR Register State       = No Info,
  DR Register Stop Timer  = 00h:00m:00s,
  Interface Specific State:
```

```
vlan-3
  UpTime                    = 00h:01m:40s,
  Local Membership          = False,
  Join/Prune State          = No Info,
  RPT State                 = No Info,
  Prune Pending Timer       = 00h:00m:00s,
  Join Expiry Timer         = 00h:00m:00s,
  Assert State              = No Info,
  Assert Timer              = 00h:00m:00s,
vlan-4
  UpTime                    = 00h:00m:00s,
  Local Membership          = False,
  Join/Prune State          = No Info,
  RPT State                 = No Info,
  Prune Pending Timer       = 00h:00m:00s,
  Join Expiry Timer         = 00h:00m:00s,
  Assert State              = No Info,
  Assert Timer              = 00h:00m:00s,
vlan-5
  UpTime                    = 00h:00m:00s,
  Local Membership          = False,
  Join/Prune State          = No Info,
  RPT State                 = No Info,
  Prune Pending Timer       = 00h:00m:00s,
  Join Expiry Timer         = 00h:00m:00s,
  Assert State              = No Info,
  Assert Timer              = 00h:00m:00s,
```

output definitions

Source-address	The IPv6 Source address.
Group-address	The IPv6 Multicast Group Address.
RPF Interface	The RPF interface towards the RP. The ifIndex is converted to the if-name for the display.
Upstream Neighbor	The primary address of the neighbor on the RPF Interface that the local router is sending periodic (S,G) join messages to.
UpTime	The time since this entry was created.
Flags	Flags indicating SPTBit, Prune State, Join State, and so on.
Pim Mode	Whether the Group Address is SSM, ASM or DM.
Upstream Join State	Whether the local router should join the SPT for the source and group represented by this entry.
Upstream Join Timer	The time remaining before the local router next sends a periodic (S,G) Join message.
RPF Next Hop	The address of the RPF next hop towards the source.
RPF Route Protocol	The routing mechanism through which the route used to find the RPF Interface towards the source was learned.
RPF Route Address/Prefix Length	The IP address which when combined with the Route Prefix length identifies the route used to find the RPF interface towards the source.
RPF Route Metric Pref	The metric preference of the route used to find the RPF interface towards the source.

output definitions (continued)

RPF Route Metric	The metric preference of the route used to find the RPF interface towards the source.
DR Register State	Whether the local router should encapsulate (S,G) data packets in Register messages and send them to the RP. The possible values include No Info, Join, Join Pending, or Prune.
DR Register Stop Timer	The value of the Register Stop Timer. If the Register State is 'prune', this is the time remaining before the local router sends a Null-Register message to the RP. If the State is 'joinPending', this is the time remaining before the local router resumes encapsulating data packets and sending them to the RP.
Upstream Prune State	Whether the local router has pruned itself from the tree. This is only used by PIM-DM. The possible values include forwarding, Ack Pending, or Pruned.
Upstream Prune Limit Timer	The time remaining before the local router may send a (S,G) prune message on alaPimSGRPFIfIndex. This is only used by PIM-DM.
Originator State	Whether this router is an originator for the (S,G) message flow. This is only used by PIM-DM. The possible values include Not Originator or Originator.
Source Active Timer	If this router is the Originator, this is the time remaining before the local router reverts to notOriginator state. Otherwise, this is zero. This is only used by PIM-DM.
State Refresh Timer	If Originator state is 'originator', this is the time remaining before the local router sends a State Refresh Message. Otherwise, this is zero. This is only used by PIM-DM.
Interface Name	The interface name corresponding to the ifIndex that corresponds to this entry.
Uptime	The time since this entry was created.
Local Membership	Whether the local router has (S,G) local membership on this interface.
Join Prune State	The state resulting from (S,G) Join/Prune messages received on this interface. The possible values include No Info, Join, or Prune Pending.
Prune Pending Timer	The time remaining before the local router acts on an (S,G) Prune message received on this interface, during which the router is waiting to see whether another downstream router overrides the Prune message.
Join Expiry Timer	The time remaining before (S,G) Join state for this interface expires.
Assert State	The (S,G) Assert state for this interface. The possible values include No Info, Winner, or Loser.
Assert Timer	If Assert State is Winner, this is the time remaining before the local router sends a (S,G) Assert message on this interface. If the Assert State is Loser, this is the time remaining before the (S,G) Assert state expires.
Assert Winner	If the Assert State is Loser, this is the address of the assert winner.
Assert Winner Metric Pref	If the Assert State is Loser, this is the metric preference of the route to the source advertised by the assert winner.
Assert Winner Metric Metric	If the Assert State is Loser, this is the routing metric of the route to the source advertised by the assert winner.

Release History

Release 6.3.1; command introduced.

Related Commands

N/A

MIB Objects

alaPimSGTable

- alaPimSGSrcAddress
- alaPimSGGrpAddress
- alaPimSGRPFIfIndex
- alaPimSGUpstreamNeighbor
- alaPimSGUpTime
- alaPimSGSPTBit
- alaPimSGUpstreamPruneState
- alaPimSGUpstreamJoinState
- alaPimSGPimMode
- alaPimSGUpstreamJoinState
- alaPimSGUpstreamJoinTimer
- alaPimSGRPFNextHop
- alaPimSGRPFRouteProtocol
- alaPimSGRPFRouteAddress
- alaPimSGRPFRoutePrefixLength
- alaPimSGRPFRouteMetricPref
- alaPimSGRPFRouteMetric
- alaPimSGDRRegisterState
- alaPimSGDRRegisterStopTimer
- alaPimSGUpstreamPruneState
- alaPimSGUpstreamPruneLimitTimer
- alaPimSGOriginatorState
- alaPimSGSourceActiveTimer
- alaPimSGStateRefreshTimer

alaPimSGITable

- alaPimSGIIfIndex
- alaPimSGIUpTime
- alaPimSGILocalMembership
- alaPimSGIJoinPruneState
- alaPimSGIPrunePendingTimer
- alaPimSGIJoinExpiryTimer
- alaPimSGIAssertState
- alaPimSGIAssertTimer
- alaPimSGIAssertWinnerAddress
- alaPimSGIAssertWinnerMetricPref
- alaPimSGIAssertWinnerMetric

36 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.

The current release also provides support for IPv6 multicast addresses. In the IPv6 addressing scheme, multicast addresses begin with the prefix ff00::/8. Similar to IPv6 unicast addresses, IPv6 multicast addresses also have different scopes depending on their prefix, though the range of possible scopes is different.

Multicast Listener Discovery (MLD) is the protocol used by an IPv6 router to discover the nodes which request multicast packets on its directly attached links and the multicast addresses that are of interest to those neighboring nodes. MLD is derived from version 2 of IPv4's Internet Group Management Protocol, IGMPv2. MLD uses ICMPv6 message types, rather than IGMP message types.

MIB information for the multicast routing commands is as follows:

Filename: AlcatelIND1Ipmrm.mib
Module: ALCATEL-IND1-IPMRM-MIB

Filename: IETF_IPMCAST.mib
Module: IPMCAST-MIB

A summary of the available commands is listed here:

ip mroute-boundary
ip mroute interface ttl
ipv6 mroute-boundary
ipv6 mroute interface ttl
show ip mroute-boundary
show ipv6 mroute-boundary
show ip mroute
show ipv6 mroute
show ip mroute interface
show ipv6 mroute interface
show ip mroute-nexthop
show ipv6 mroute-nexthop

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 *OmniSwitch AOS Release 6 Advanced Routing Configuration Guide* for detailed information.

ip mroute-boundary *if_name scoped_address mask*

no ip mroute-boundary *if_name scoped_address mask*

Syntax Definitions

if_name	The interface name 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 (for example, 255.0.0.0).

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete the scoped multicast address boundaries for a router interface.
- IPMRM must be configured on the switch

Examples

```
-> ip mroute-boundary vlan-2 239.0.0.0 255.0.0.0
```

Release History

Release 6.1; 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
```

ipv6 mroute-boundary

Configures or deletes an IPv6 multicast boundary on the interface for a specified scope zone. Packets with a destination address in the associated address/mask range will not be forwarded over the boundary interface.

ipv6 mroute-boundary *if_name* **scope** *scope_value*

no ipv6 mroute-boundary *if_name* **scope** *scope_value*

Syntax Definitions

if_name	The interface name on which the boundary is being assigned.
scope_value	The scope value indicates the scope of the IPv6 internetwork for which the multicast traffic is intended. Range of scope value is 3-15.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete the configured IPv6 scoped multicast address boundaries for a router interface.
- IPMRM must be configured on the switch.

Examples

```
-> ipv6 mroute-boundary vlan-2 scope 6
```

Release History

Release 6.3.4; command was introduced.

Related commands

show ipv6 mroute-boundary	Displays information about the IPv6 scoped multicast boundaries that have been defined on the system.

MIB Objects

```
ipMcastBoundaryTable
   ipMcastBoundaryIfIndex
   ipMcastBoundaryAddressType
   ipMcastBoundaryAddress
   ipMcastBoundaryAddressPrefixLength
```

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 of the interface.

ip mroute interface *if_ name* **ttl** *threshold*

Syntax Definitions

if_name	The interface name that has one of the Multicast routing protocols running (either DVMRP or PIM).
threshold	The TTL threshold value. Values may range from 0–255. The default value of 0 allows all multicast packets to be forwarded out of the interface.

Defaults

parameter	default
threshold	0

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> ip mroute interface vlan-1 ttl 255
```

Release History

Release 6.1; command was introduced.

Related Commands

show ip mroute interface	Displays IP multicast interface information.

MIB Objects

```
alaIpMcastInterfaceTable
   alaIpMcastInterfaceIfIndex
   alaIpMcastInterfaceTtl
```

ipv6 mroute interface ttl

Specifies a multicast datagram Time to Live (TTL) threshold for an existing IPv6 interface. Any IP multicast datagrams with a TTL value lower than the specified TTL threshold value will not be forwarded out of the interface.

ipv6 mroute interface *if_name* **ttl** *threshold*

Syntax Definitions

if_name	The name of the IPv6 interface.
threshold	The TTL threshold value. Values may range from 0–255. The default value of 0 allows all multicast packets to be forwarded out of the interface.

Defaults

parameter	default
threshold	0

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> ipv6 mroute interface vlan-1 ttl 255
```

Release History

Release 6.3.1; command was introduced.

Related Commands

show ipv6 mroute interface	Displays IPv6 multicast interface information.

MIB Objects

```
alaIpMcastInterfaceTable
   alaIpMcastInterfaceIfIndex
   alaIpMcastInterfaceTtl
```

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 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show ip mroute-boundary

Interface Name  Interface Address  Boundary Address
--------------+------------------+------------------
vlan-4           214.0.0.7          239.1.1.1/32
```

output definitions

Interface Name	The name of the interface on which the boundary is assigned. Packets with a destination address in the associated address/mask range will not be forwarded from this interface.
Interface Address	The IP address of this interface where the boundary is assigned.
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 6.1; 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 ipv6 mroute-boundary

Displays IPv6 scoped multicast boundaries which are configured on the system.

show ipv6 mroute-boundary

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show ipv6 mroute-boundary

Interface Name                   Boundary Address/Prefix Length
---------------------------------+------------------------------
vlan-5                           ff06::/16
vlan-8                           ff08::/16
```

output definitions

Interface Name	The name of the interface on which the boundary is assigned. Packets with a destination address in the associated address/mask range will not be forwarded from this interface.
Boundary Address	The IPv6 group address which when combined with the prefix length identifies the group range for which the scoped boundary exists.

Release History

Release 6.3.4; command was introduced.

Related Commands

ipv6 mroute-boundary	Configures or deletes an IPv6 multicast boundary on the interface for a specified scope zone.

MIB Objects

```
ipMcastBoundaryTable
   ipMcastBoundaryIfIndex
   ipMcastBoundaryAddressType
   ipMcastBoundaryAddress
   ipMcastBoundaryAddressPrefixLength
```

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 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show ip mroute

Total 2 Mroutes
Group Address   Src Address      Upstream Nbr    Route Address       Proto
--------------+---------------+---------------+----------------+----------
225.0.0.0       214.0.0.2/32      0.0.0.0       214.0.0.0/24         PIM-SM
225.0.0.1       214.0.0.2/32      0.0.0.0       214.0.0.0/24         PIM-DM
```

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 Address	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 (that is, DVMRP, PIM-SM or PIM-DM).

Release History

Release 6.1; command was introduced.

Related Commands

N/A

MIB Objects

```
alaIpMcastRouteTable
   alaIpMcastRouteGroup
   alaIpMcastRouteSource
   alaIpMcastRouteInIfIndex
   alaIpMcastRouteUpstreamNeighbor
   alaIpMcastRouteRtAddress
   alaIpMcastRouteRtPrefixLength
   alaIpMcastRouteProtocol
```

show ipv6 mroute

Displays multicast routing information for IPv6 datagrams sent by particular sources to the IPv6 multicast groups known to this router.

show ipv6 mroute

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show ipv6 mroute
Total 2 Mroutes
Group Address Source Address Interface Upstream Neighbor Route Addr/Prefix Len
 Proto
-------------+--------------+---------+-----------------------+-----------------
+------+
ff06:7777::1  2600::7       vlan-30   fe80::2d0:95ff:feac:a537 2600::/64
 PIM-SM
ff06:7777::2  2600::7        vlan-30   fe80::2d0:95ff:feac:a537 2600::/64
 PIM-SM
```

output definitions

Group Address	The IPv6 multicast group address for this entry.
Source Address	The IPv6 multicast address, which identifies the source for this entry.
Interface	The name of the IPv6 interface on which the datagrams sent by these sources to this IPv6 multicast address are received.
Upstream Neighbor	The IPv6 address of the upstream neighbor from which the datagrams from these sources to this multicast address are received.
Route Addr/Prefix len	The IPv6 address portion of the route used to find the upstream or parent interface for this IPv6 multicast forwarding entry.
Proto	The IPv6 multicast routing protocol through which this IPv6 multicast forwarding entry was learned.

Release History

Release 6.3.1; command was introduced.

Related Commands

N/A

MIB Objects

```
alaIpMcastRouteTable
   alaIpMcastRouteGroup
   alaIpMcastRouteSource
   alaIpMcastRouteInIfIndex
   alaIpMcastRouteUpstreamNeighbor
   alaIpMcastRouteRtAddress
   alaIpMcastRouteRtPrefixLength
   alaIpMcastRouteProtocol
```

show ip mroute interface

Displays IP multicast interface information.

show ip mroute interface {*interface_name***}**

Syntax Definitions

interface_name	The name of the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

Not specifying an interface name displays all known IP multicast interfaces information.

Examples

```
-> show ip mroute interface

Interface Name     IP Address     TTL   Multicast Protocol
---------------+---------------+------+--------------------
vlan-4             214.0.0.7       0        PIM
vlan-26            172.21.63.7     0        PIM
vlan-11            212.61.11.7     0        PIM
```

output definitions

Interface Name	The name configured for the interface.
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 of the interface. The default value, 0, specifies that *all* multicast packets are forwarded out of the interface.
Multicast Protocol	The multicast routing protocol currently running on this interface. Options include DVMRP and PIM.

Release History

Release 6.1; command was introduced.

Related Commands

N/A

MIB Objects

```
alaIpMcastInterfaceTable
   alaIpMcastInterfaceIfIndex
   alaIpMcastInterfaceTtl
   alaIpMcastInterfaceProtocol
```

show ipv6 mroute interface

Displays IPv6 multicast interface information.

show ipv6 mroute interface {*interface_name***}**

Syntax Definitions

interface_name	The name of the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

Not specifying an interface name displays all known IPv6 multicast interfaces information.

Examples

```
-> show ipv6 mroute interface

Interface Name     IP Address     TTL   Multicast Protocol
---------------+---------------+------+--------------------
vlan-4             2000::1      0        PIM
vlan-26            2000::2      0        PIM
vlan-11            2000::3      0        PIM
```

output definitions

Interface Name	The name configured for the IPv6 interface.
IP Address	The IPv6 address of this interface entry.
TTL	The datagram TTL threshold for the interface. Any IPv6 multicast datagrams with a TTL less than the threshold displayed in the table will not be forwarded out of the interface. The default value, 0, specifies that *all* multicast packets are forwarded out of the interface.
Multicast Protocol	The multicast routing protocol currently running on this interface. Options include DVMRP and PIM.

Release History

Release 6.3.1; command was introduced.

Related Commands

N/A

MIB Objects

```
alaIpMcastInterfaceTable
   alaIpMcastInterfaceIfIndex
   alaIpMcastInterfaceTtl
   alaIpMcastInterfaceProtocol
```

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 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show ip mroute-nexthop

Total 10 Nexthops

Group Address  Src Address   Interface Name    Next Hop     Protocol
                                               Address
-------------+-------------+----------------+-------------+----------
225.0.0.0     214.0.0.2/32      vlan-26        225.0.0.0    PIM-SM
225.0.0.1     214.0.0.2/32      vlan-26        225.0.0.1    PIM-SM
225.0.0.2     214.0.0.2/32      vlan-26        225.0.0.2    PIM-SM
225.0.0.3     214.0.0.2/32      vlan-26        225.0.0.3    PIM-SM
225.0.0.4     214.0.0.2/32      vlan-26        225.0.0.4    PIM-SM
225.0.0.5     214.0.0.2/32      vlan-26        225.0.0.5    PIM-SM
225.0.0.6     214.0.0.2/32      vlan-26        225.0.0.6    PIM-SM
225.0.0.7     214.0.0.2/32      vlan-26        225.0.0.7    PIM-SM
225.0.0.8     214.0.0.2/32      vlan-26        225.0.0.8    PIM-SM
225.0.0.9     214.0.0.2/32      vlan-26        225.0.0.9    PIM-SM
```

output definitions

Group Address	The IP multicast group address for this entry.
Src Address	The network address, which identifies the source for this entry.
Interface Name	Generally, this is the name configured for the interface.
Next Hop Address	The address of the next-hop that is specific to this entry.
Protocol	The routing protocol by which this next-hop was learned (that is, DVMRP or PIM-SM).

Release History

Release 6.1; command was introduced.

Related Commands

show ipv6 mroute-boundary	Displays multicast routing information for IP datagrams sent by particular sources to the IP multicast groups known to this router.

MIB Objects

```
alaIpMcastRouteNextHopTable
   alaIpMcastRouteNextHopGroup
   alaIpMcastRouteNextHopSource
   alaIpMcastRouteNextHopIfIndex
   alaIpMcastRouteNextHopAddress
   alaIpMcastRouteNextHopProtocol
```

show ipv6 mroute-nexthop

Displays IPv6 next-hop information on outgoing interfaces for routing IP multicast datagrams.

show ipv6 mroute-nexthop

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show ipv6 mroute-nexthop
Total 2 Nexthops
Group Address   Source Address    Interface    Next Hop Address        Protocol
---------------+-----------------+------------+-----------------------+---------
ff06:7777::1    2600::7           vlan-40      ff06:7777::1            PIM-SM
ff06:7777::2    2600::7           vlan-40      ff06:7777::2            PIM-SM
```

output definitions

Group Address	The IPv6 multicast group address for this entry.
Src Address	The IPv6 multicast address, which identifies the source for this entry.
Interface Name	The name of the IPv6 interface on which the datagrams sent by these sources to this IPv6 multicast address are received.
Next Hop Address	The IPv6 address of the next-hop that is specific to this entry.
Protocol	The IPv6 multicast routing protocol by which this IPv6 multicast forwarding entry was learned.

Release History

Release 6.3.1; command was introduced.

Related Commands

N/A

MIB Objects

```
alaIpMcastRouteNextHopTable
   alaIpMcastRouteNextHopGroup
   alaIpMcastRouteNextHopSource
   alaIpMcastRouteNextHopIfIndex
   alaIpMcastRouteNextHopAddress
   alaIpMcastRouteNextHopProtocol
```

37 QoS Commands

Alcatel-Lucent's QoS software provides a way to manipulate flows coming through the switch based on user-configured policies. The flow manipulation (generally referred to as *Quality of Service* or *QoS*) may be as simple as allowing/denying traffic, or as complicated as remapping 802.1p bits from a Layer 2 network to ToS values in a Layer 3 network.

This chapter provides information about configuring QoS global and port parameters through the Command Line Interface (CLI). Refer to Chapter 38, "QoS Policy Commands," for information about commands used to configure QoS policy rules.

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 on one or more platforms. See command descriptions in this chapter and check release notes for information about commands that are not supported.

The QoS commands are listed here:

Global commands	**qos** **qos trust ports** **qos default servicing mode** **qos forward log** **qos log console** **qos log lines** **qos log level** **qos default bridged disposition** **qos default routed disposition** **qos default multicast disposition** **qos user-port** **qos dei** **qos stats interval** **qos nms priority** **qos phones** **qos quarantine mac-group** **qos quarantine path** **qos quarantine page** **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 trusted** **qos port servicing mode** **qos port q minbw maxbw** **qos port maximum egress-bandwidth** **qos port maximum ingress-bandwidth** **qos port default 802.1p** **qos port default dscp** **qos port default classification** **qos port dei** **qos port monitor** **show qos port** **show qos port monitor**

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 servicing mode]
[forward log]
[log console]
[log lines *lines***]**
[log level *level***]**
[clear log]
[default bridged disposition {accept | deny | drop}]
[default routed disposition {accept | deny | drop}
[default multicast disposition {accept | deny | drop}]
[user-port {filter | shutdown} {spoof | bgp | bpdu | rip | ospf}]
[stats interval *seconds***]**
[nms priority]
[phones [priority *priority_value* **| trusted]]**
[quarantine mac-group *mac_group***]**
[quarantine path *url***]**
[qos quarantine page]
[dei {ingress | egress}]

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 6400, 6850E, 6855, 9000E

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 default disposition deny
-> qos disable
-> qos enable
```

Release History

Release 6.1; 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
   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/DSCP values in incoming packets; untrusted ports will set any 802.1p or ToS/DSCP values to zero in incoming packets, unless a default 802.1p or ToS/DSCP value is configured.

Any port configured through the **qos port** command will automatically be added in the trust mode specified by this command. See page 37-44 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **qos port 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 tagging is always trusted regardless of the global setting.
- Mobile ports are always trusted regardless of the global setting.
- Use the **qos port default 802.1p** or **qos port default dscp** commands to specify that a value other than zero should be applied to the incoming packets. Note that this value is overridden if a policy exists that specifies a different value for such packets.

Examples

```
-> qos trust ports
-> qos no trust ports
```

Release History

Release 6.1; 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 servicing mode

Configures the default queuing scheme for destination (egress) ports.

qos default servicing mode {strict-priority | wrr [*w0 w1 w2 w3 w4 w5 w6 w7***] | priority-wrr [***w0 w1 w2 w3 w4 w5 w6 w7***] | drr] [***w0 w1 w2 w3 w4 w5 w6 w7***]}**

Syntax Definitions

strict-priority	Selects the strict priority queuing scheme as the default servicing mode. All eight available queues on a port are serviced strictly by priority.
wrr	Selects the weighted round robin (WRR) queuing scheme as the default servicing mode. Traffic is serviced based on the weight of each queue.
priority-wrr	Parameter not supported.
drr	Selects the deficit round robin (DRR) queuing scheme as the default servicing mode. Traffic is serviced based on the weight of each queue.
w0 w1 w2 w3 w4 w5 w6 w7	The value of the desired weight for each of the queues when WRR or DRR is the active queuing scheme. The range is 0 to 15.

Defaults

parameter	default
strict-priority | wrr | drr	**strict-priority**
w0 w1 w2 w3 w4 w5 w6 w7	1 (best effort)

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Each queue can have a different weight value and configuring these values in ascending or descending order is not required. When a queue is given a weight of 0, it is configured as a Strict-Priority queue.
- Use the **wrr** parameter to configure a Priority-WRR queuing scheme, which consists of a combination of Strict-Priority queues (zero weight) and WRR queues (non-zero weight).
- Using the **qos default servicing mode** command does not override configuration values that were set on a per port basis with the **qos port servicing mode** command.
- The servicing mode only applies to destination (egress) ports because this is where traffic shaping occurs. Even though the **qos port servicing mode** and **qos default servicing mode** commands are allowed on source (ingress) ports, they do not affect traffic on these ports.

Examples

```
-> qos default servicing mode strict-priority
-> qos default servicing mode wrr 1 2 3 4 5 6 7 8
-> qos default servicing mode drr 10 0 12 14 0 0 8 1
```

Release History

Release 6.1; command was introduced.
Release 6.1.1; **wrr** and **drr** parameters added.
Release 6.3.1; **priority-wrr** parameter deprecated.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
qos port servicing mode	Configures the servicing mode (SPQ or priority WRR) for a port.
show qos queue	Displays information for all QoS queues.

MIB Objects

```
alaQoSConfig
   alaQoSConfigServicingMode
   alaQoSConfigLowPriorityWeight
   alaQoSConfigMediumPriorityWeight
   alaQoSConfigHighPriorityWeight
   alaQoSConfigUrgentPriorityWeight
```

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 policy server software in the switch.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 6.1; 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 switch logging utility, which is an event logging application available on the OmniSwitch. The configuration of the switch logging utility determines if QoS messages are sent to a log file in the switch's flash file system, displayed on the switch console, or sent to a remote syslog server.

qos log console

qos no log console

Syntax Definitions

N/A

Defaults

QoS log messages are not sent to the switch logging utility by default.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- To display QoS log events as they happen on an output console attached to the switch, configure the switch logging utility to output events to the console. This is done using the **swlog output** command.
- 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 6.1; command was introduced.

Related Commands

qos log lines	Configures the number of lines in the QoS log.
swlog output	Enables or disables switch logging output to the console, file, or data socket (remote session).
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 6400, 6850E, 6855, 9000E

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 6.1; 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 2 (least detail) to 9 (most detail).

Defaults

parameter	default
level	6

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 6.1; 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 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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.
- This command applies only to IGMP messages. It does not apply to other types of multicast traffic.

Examples

```
-> qos default multicast disposition deny
```

Release History

Release 6.1; command was introduced.

Related Commands

policy action disposition	Configures a disposition for a policy action.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigDefaultMulticastDisposition
   alaQoSConfigAppliedDefaultMulticastDisposition
```

qos user-port

Configures the option to filter packets or administratively disable a port when the specified type of traffic is received on a port that is a member of the pre-defined UserPorts group.

qos user-port {filter | shutdown} {spoof | bgp | bpdu | rip | ospf | vrrp | dvmrp | pim | isis | dhcp-server | dns-reply}

qos no user-port {filter | shutdown}

Syntax Definitions

filter	Filters the specified type of traffic when it is received on UserPort ports.
shutdown	Administratively disables UserPort ports that receive the specified type of traffic.
spoof	Detects IP spoofing. The source IP address of a packet ingressing on a user port is compared to the subnet of the VLAN for the user port; the packet is dropped if these two items do not match. Also applies to ARP packets.
bgp	Filters only BGP protocol packets from a TCP session that was not originated by the same switch that has this filter configured.
bpdu	Filters conventional Spanning Tree BPDU (destination MAC address 0x0180c2:000000) packets and GVRP (destination MAC address 0x0180c2:000021) packets.
rip	Filters RIP protocol packets.
ospf	Filters OSPF protocol packets.
vrrp	Filters VRRP protocol packets.
dvmrp	Filters IGMP packets with a type of 0x13. This applies only to IP packets with no options.
pim	Filters PIMv1, PIM-DM, and PIM-SM packets. The PIMv1 filter applies only to IP packets with no options.
isis	Filters IS-IS protocol packets.
dhcp-server	Filters response packets originating from a DHCP or BOOTP server that is configured on the known UDP port 67.
dns-reply	Filters all packets (both TCP and UDP) that originate from the known DNS port 53.

Defaults

parameter	default
filter	spoof
shutdown	none

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to disable the filter or shutdown function. This form of the command effects the overall operation of the feature.
- To specify more than one traffic type in the same command line, enter each type separated by a space (e.g., **spoof bgp ospf**).
- Note that existing traffic types to filter or shutdown are removed each time the **filter** or **shutdown** option is configured. Specify all desired traffic types each time the **qos user-port** command is performed to retain previously configured traffic types.
- No changes to the **filtering** and **shutdown** options are applied to the switch until the **qos apply** command is performed.
- This command only applies to ports that are members of the UserPorts group. Use the **policy port group** command to create and assign members to the UserPorts group.
- An SNMP trap is sent when a port is administratively disabled through a UserPorts shutdown function or a port disable action.
- To enable a port disabled by a user port shutdown operation, use the **interfaces admin** command to administratively enable the port or disconnect and reconnect the port cable.
- Up to 126 IP interfaces are supported with spoof detection on user ports. If the number of interfaces exceeds this amount, user port packets ingressing on those interfaces that exceed the 126 limit are dropped.

Examples

```
-> qos user-port filter spoof bpdu
-> qos user-port shutdown spoof bgp ospf
-> qos no user-port shutdown
```

Release History

Release 6.1.1; command was introduced.
Release 6.3.1; **dvmrp**, **pim**, **isis**, and **dns-reply** parameters added.

Related Commands

policy port group	Configures a port group and its associated slot and port numbers.
show qos config	Displays QoS configuration information.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigUserportFilter
   alaQoSConfigAppliedUserportFilter
   alaQoSConfigUserportShutdown
   alaQoSConfigAppliedUserportShutdown
```

qos dei

Configures the global Drop Eligible Indicator (DEI) bit mapping and marking setting for all QoS ports.The DEI setting applies to packets marked yellow (non-conforming) as the result of Tri-Color Marking (TCM) rate limiting.

qos dei {ingress | egress}

qos no dei {ingress | egress}

Syntax Definitions

ingress	Maps the DEI/CFI bit to yellow (non-conforming) if this bit is set for ingress traffic.
egress	Marks the DEI/CFI bit for egress packets if TCM marked the packets yellow.

Defaults

By default, no DEI/CFI bit marking or mapping is done.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to disable the global DEI bit mapping (ingress) or marking (egress) configuration for the switch.
- Use the **qos port dei** command to set the DEI bit mapping and marking configuration for a specific port. Note that the port setting takes precedence over the global DEI setting.
- Packets marked yellow by TCM rate limiting are still transmitted when there is no congestion on the egress port queues. Setting the DEI/CFI bit for yellow egress packets (**qos dei egress**) ensures that an upstream switch is made aware that the packet was marked yellow.
- When a switch receives a yellow packet with the DEI/CFI bit set and ingress DEI/CFI bit mapping is enabled (**qos dei ingress**), the packet is mapped to an internal drop precedence or yellow color marking for the switch.

Examples

```
-> qos dei ingress
-> qos dei egress
-> qos no dei ingress
-> qos no dei egress
```

Release History

Release 6.4.3; command was introduced.

Related Commands

qos port	Configures a physical port for QoS.
qos port dei	Configures the Drop Eligible Indicator (DEI) bit mapping and marking setting for the specified QoS port.
policy action cir	Configures a Tri-Color Marking policy action.
show qos config	Displays global information about the QoS configuration.
show qos port	Displays information about QoS ports.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigDEIMapping
   alaQoSConfigDEIMarking
```

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 6400, 6850E, 6855, 9000E

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 6.1; command was introduced.

Related Commands

show qos statistics	Displays statistics about the QoS configuration.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigStatsInterval
```

qos nms priority

Enables or disables the automatic prioritization of NMS traffic—SSH (TCP Port 22), Telnet (TCP Port 23), WebView (HTTP Port 80) and SNMP (UDP port 161)—that is destined for the switch. Prioritization maximizes access for NMS traffic and helps to reduce the potential for DoS attacks.

qos nms priority

qos no nms priority

Syntax Definitions

N/A

Defaults

By default, NMS traffic prioritization is enabled.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to disable automatic prioritization of NMS traffic.
- The NMS traffic from the first eight *active* IP interfaces is prioritized; any such traffic from additional interfaces is not prioritized.
- The precedence of an active IP interface is determined by the value of the SNMP interface index (ifindex), which was assigned to the interface when it was created. The lower the ifindex value the higher the precedence; the higher the ifindex value the lower the precedence. Note that the precedence is only determined for active IP interfaces.
- To change the precedence of an IP interface, use the **ip interface ifindex** command and specify a higher (lower precedence) or lower (higher precedence) ifindex value.
- When automatic NMS prioritization is enabled, QoS policies that specify priority are not applied to the NMS traffic. Other QoS policies, however, are applied to this type of traffic as usual. If a policy specifies rate limiting, then the policy with the lowest rate limiting value is applied.

Examples

```
-> qos nms priority
-> qos no nms priority
```

Release History

Release 6.3.1; command was introduced.

Related Commands

show qos config	Displays the QoS configuration for the switch.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigAutoNms
```

qos phones

Enables or disables the automatic prioritization of IP phone traffic.

qos phones [priority *priority_value* **| trusted]**

qos no phones

Syntax Definitions

priority_value	The priority given to scheduling traffic on the output port. Values range from 0 (lowest) to 7 (highest).
trusted	Trusts IP phone traffic; priority value of the IP phone packet is used.

Defaults

parameter	default
priority_value **| trusted**	trusted

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to disable automatic prioritization of IP phone traffic.
- IP phone traffic is identified by examining the source MAC address of the packet received on the port. If the source MAC falls within one of the following ranges, the QoS IP phone priority is automatically assigned to the MAC:

  00-80-9F-54-xx-xx to 00-80-9F-64-xx-xx
  00-80-9F-66-xx-xx to 00-80-9F-6F-xx-xx.

- To automatically apply the QoS IP phone priority to other, non-IP phone traffic, add the source MAC addresses of such traffic to the QoS “alaPhone” group.
- When automatic prioritization of IP phone traffic is enabled, QoS policies that specify priority are not applied to the IP phone traffic. Other QoS policies, however, are applied to this type of traffic as usual.

Examples

```
-> qos phones priority 7
-> qos phones trusted
-> qos no phones
```

Release History

Release 6.3.1; command was introduced.

Related Commands

show qos config	Displays the QoS configuration for the switch.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigAutoPhones
```

qos quarantine mac-group

Configures the name of the Quarantine MAC address group. The OmniVista Quarantine Manager application identifies source MAC addresses to quarantine and adds these addresses to the Quarantine MAC group.

qos quarantine mac-group *mac_group*

qos no quarantine mac-group

Syntax Definitions

mac_group	The name of the Quarantine MAC group (up to 31 alphanumeric characters).

Defaults

parameter	default
mac-group	Quarantined

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- Use the **no** form of the command to reset the default MAC group name back to “Quarantined”.
- The *mac-group* name specified with this command must match the group name specified with the OmniVista Quarantine Manager application.
- Each switch can have a different Quarantine MAC group name as long as each switch matches the OmniVista Quarantine Manager MAC group name for that switch. Note that there is only one such MAC group per switch.
- Do not use the Quarantine MAC group name in regular QoS policies.
- This group is also used by the switch Quarantine Manager and Remediation (QMR) application to restrict or restore network access to quarantined MACs.
- Note that QMR is not available if VLAN Stacking services or QoS VLAN Stacking inner VLAN and 802.1p policies are configured on the switch.
- QMR is considered active when there are MAC addresses in the Quarantine MAC address group. Use the **show policy mac group** command to display the contents of this group. In addition, the **show mac-address-table** command output display identifies quarantined MAC addresses.

Examples

```
-> qos quarantine mac-group mac_group1
-> no quarantine mac-group
```

Release History

Release 6.3.1; command was introduced.

Related Commands

qos quarantine path	Specifies the URL for a remediation server.
qos quarantine page	Configures the Quarantine Manager and Remediation (QMR) application to send a Quarantined page to a client if a remediation server is not configured.
show policy mac group	Displays information about policy MAC groups.
show qos config	Displays QoS configuration information.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigQuarantineMacGroupName
```

qos quarantine path

Specifies the URL for a remediation server. This information is used by the Quarantine Manager and Remediation (QMR) application.

qos quarantine path *url*

qos no quarantine path

Syntax Definitions

url	The URL for the QMR remediation server.

Defaults

By default, no URL is configured.

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- Use the **no** form of the command to remove the remediation server URL from the configuration.
- Add the corresponding IP address for the remediation server to the “alaExceptionSubnet” network group. Specifying both the URL and IP address is required to redirect quarantined MACs to the remediation server.

Examples

```
-> qos quarantine path www.remediate.com
-> no quarantine path
```

Release History

Release 6.3.1; command was introduced.

Related Commands

qos quarantine mac-group	Configures the name of the Quarantine MAC address group.
qos quarantine page	Configures the Quarantine Manager and Remediation (QMR) application to send a Quarantined page to a client if a remediation server is not configured.
policy network group	Configures a network group name and its associated IP addresses.
show qos config	Displays QoS configuration information.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigQMPath
```

qos quarantine page

Configures the Quarantine Manager and Remediation (QMR) application to send a Quarantined page to a client if a remediation server is not configured. This page is used to notify the client that QMR has quarantined the client.

qos quarantine page

qos no quarantine page

Syntax Definitions

N/A

Defaults

By default, no Quarantined page is sent to the client.

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- Use the **no** form of the command to disable the Quarantined page notification.
- A Quarantined page is only sent if a remediation server path was not configured. Note that even if the remediation server is not active, a page is not sent as long as the server is configured for QMR.

Examples

```
-> qos quarantine page
-> no quarantine page
```

Release History

Release 6.3.1; command was introduced.

Related Commands

qos quarantine mac-group	Configures the name of the Quarantine MAC address group.
qos quarantine path	Specifies the URL for a remediation server.
show qos config	Displays QoS configuration information.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigQMPage
```

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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to change the type of messages that will be logged or to return debugging to its default state.
- Use this command to troubleshoot QoS events on the switch.

Examples

```
-> debug qos flows queue
-> qos debug no flows no queue
-> debug no qos
```

Release History

Release 6.1; 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.
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	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 6400, 6850E, 6855

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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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 [egress]

Syntax Definitions

N/A

Defaults

All QoS statistic counters are reset to zero.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use this command to reset global QoS statistics to zero. Statistics may be displayed with the **show qos statistics** command.
- Use the **egress** parameter to reset only the egress CoS queue statistics to zero. Statistics may be displayed with the **show qos queue** command.

Examples

```
-> qos stats reset
-> qos stats reset egress
```

Release History

Release 6.1; command was introduced.
Release 6.4.3; **egress** parameter added.

Related Commands

show qos statistics	Displays statistics about the QoS configuration.
show qos queue	Displays QoS egress CoS queue statistics.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigStatsReset
```

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 6400, 6850E, 6855, 9000E

Usage Guidelines

The QoS port configuration parameters that are reset include:

parameter	default
default queues	8
trusted	not trusted

Examples

```
-> qos port 3/1 reset
```

Release History

Release 6.1; command was introduced.

MIB Objects

```
alaQoSPortTable
   alaQoSPortSlot
   alaQoSPortPort
   alaQoSPortReset
```

qos port

Configures QoS parameters for a physical port. This section describes the base command with a single required option (*slot/port*).

In lieu of these options, the base command (**qos port**) may be used with other keywords to set up a QoS configuration on a per port basis. 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 port *slot/port*
[trusted]
[servicing mode]
[q*n* **{minbw | maxbw}** *kbps***]**
[maximum egress-bandwidth]
[maximum ingress-bandwidth]
[default 802.1p *value***]**
[default dscp *value***]**
[default classification {802.1p | tos | dscp}]
[dei {ingress | egress}]

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.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 6.1; 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
   alaQoSPortMaximumDefaultBandwidth
   alaQoSPortAppliedMaximumDefaultBandwidth
   alaQoSPortDefaultClassification
   alaQoSPortAppliedDefaultClassification
   alaQoSPortLowPriorityWeight
   alaQoSPortAppliedLowPriorityWeight
   alaQoSPortMediumPriorityWeight
   alaQoSPortAppliedMediumPriorityWeight
   alaQoSPortHighPriorityWeight
   alaQoSPortAppliedHighPriorityWeight
   alaQoSPortUrgentPriorityWeight
   alaQoSPortAppliedUrgentPriorityWeight
```

qos port trusted

Configures whether an individual port is trusted or untrusted. Trusted ports can accept the 802.1p and ToS/DSCP values in incoming packets; untrusted ports will set any 802.1p or ToS/DSCP values to zero in incoming packets, unless a default 802.1p or ToS/DSCP value is configured.

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 6400, 6850E, 6855, 9000E

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.
- Use the **qos port default 802.1p** or **qos port default dscp** commands to specify that a value other than zero should be applied to the incoming packets. Note that this value is overridden if a policy exists that specifies a different 802.1p or ToS/DSCP value for such packets.
- 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 6.1; 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 servicing mode

Configures a queuing scheme for an individual destination (egress) port.

qos port *slot/port* **servicing mode {strict-priority | wrr [***w0 w1 w2 w3 w4 w5 w6 w7***] | priority-wrr [***w0 w1 w2 w3 w4 w5 w6 w7***] | drr [***w0 w1 w2 w3 w4 w5 w6 w7***] | default}**

Syntax Definitions

slot/port	The slot and port number to which this servicing mode applies.
strict-priority	Selects the strict priority queuing scheme as the servicing mode for the specified port. All eight available queues on a port are serviced strictly by priority.
wrr	Selects the weighted round robin (WRR) queuing scheme as the servicing mode for the specified port. Traffic is serviced based on the weight of each queue.
priority-wrr	Parameter not supported.
drr	Selects the deficit round robin (DRR) queuing scheme as the servicing mode for the specified port. Traffic is serviced based on the weight of each queue.
w0 w1 w2 w3 w4 w5 w6 w7	The value of the desired weight for each of the queues when WRR or DRR is the active queuing scheme. The range is 0 to 15.
default	Selects the switch default servicing mode for the port. The default mode is configured using the **qos default servicing mode** command.

Defaults

parameter	default
strict-priority | wrr | drr	**strict-priority**
w0 w1 w2 w3 w4 w5 w6 w7	1 (best effort)

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Each queue can have a different weight value and configuring these values in ascending or descending order is *not* required. When a queue is given a weight of 0, it is configured as a Strict-Priority queue.
- Use the **wrr** parameter to configure a Priority-WRR queuing scheme, which consists of a combination of Strict-Priority queues (zero weight) and WRR queues (non-zero weight).
- The **qos port servicing mode** command overrides the servicing mode configured with the **qos default servicing mode** command.

- The servicing mode only applies to destination (egress) ports because this is where traffic shaping occurs. Even though the **qos port servicing mode** and **qos default servicing mode** commands are allowed on source (ingress) ports, they do not affect traffic on these ports.
- Once the **qos port servicing mode** command is used on a port, this same command is required to make any additional mode changes for that port. If the port is changed back to the default servicing mode, however, this restriction is removed and the **qos default servicing mode** command is also allowed on the port.

Examples

```
-> qos port 3/1 servicing mode strict-priority
-> qos port 3/3 servicing mode wrr 1 2 3 4 5 6 7 8
-> qos port 3/4 servicing mode drr 10 11 12 13 14 15 16 17
-> qos port 3/2 servicing mode default
```

Release History

Release 6.1; command was introduced.
Release 6.1.1; **wrr** and **drr** parameters added.
Release 6.3.1; priority-wrr parameter deprecated.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
qos default servicing mode	Configures the default servicing mode for all switch ports.
show qos queue	Displays information for all QoS queues.

MIB Objects

```
alaQoSPortTable
   alaQoSPortServicingMode
   alaQosPortQ0PriorityWeight
   alaQosPortQ1PriorityWeight
   alaQosPortQ2PriorityWeight
   alaQosPortQ3PriorityWeight
   alaQosPortQ4PriorityWeight
   alaQosPortQ5PriorityWeight
   alaQosPortQ6PriorityWeight
   alaQosPortQ7PriorityWeight
```

qos port q minbw maxbw

Configures a minimum and maximum bandwidth for each of the 8 COS egress queues on the specified port.

qos port *slot/port* **q***n* **{minbw | maxbw}** *kbps*

qos port *slot/port* **no q***n* **{minbw | maxbw}** *kbps*

Syntax Definitions

slot/port	The slot/port on which the COS min/max bandwidth is configured.
n	The number of the queue for the specified port. Range is 1 to 8.
kbps	The minimum or maximum bandwidth value (in Kbits per second). The value may be entered as an integer (for example, **10000**) or with abbreviated units (for example, **10k**, **10m**, **10g,** or **10t**). If the value is entered in bits per second, the switch rounds the value up to the nearest thousand.

Defaults

By default the minimum bandwidth value for each queue is set to zero (best effort), and the maximum bandwidth value for each queue is set to zero (port speed).

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to return the minimum or maximum bandwidth value for the specified queue to the default value (zero).
- Note that configuring the minimum and maximum bandwidth for the same queue is allowed on the same command line (see the “Examples” section).
- Configuring the bandwidth values for different queues requires a separate command for each queue.

Examples

```
-> qos port 1/3 q0 minbw 10 q0 maxbw 100
-> qos port 1/3 q1 minbw 100
-> qos port 1/3 q1 maxbw 10g
-> qos port 2/1 q7 minbw 5k q7 maxbw 50k
-> qos port 1/3 no q1 minbw
-> qos port 1/3 no q1 maxbw
```

Release History

Release 6.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
qos default servicing mode	Configures the default servicing mode for all switch ports.
show qos queue	Displays information for all QoS queues.

MIB Objects

```
alaQoSPortTable
   alaQoSPortSlot
   alaQoSPortPort
   alaQoSPortCOS0MaximumBandwidth
   alaQoSPortCOS1MaximumBandwidth
   alaQoSPortCOS2MaximumBandwidth
   alaQoSPortCOS3MaximumBandwidth
   alaQoSPortCOS4MaximumBandwidth
   alaQoSPortCOS5MaximumBandwidth
   alaQoSPortCOS6MaximumBandwidth
   alaQoSPortCOS7MaximumBandwidth
   alaQoSPortCOS0MinimumBandwidth
   alaQoSPortCOS1MinimumBandwidth
   alaQoSPortCOS2MinimumBandwidth
   alaQoSPortCOS3MinimumBandwidth
   alaQoSPortCOS4MinimumBandwidth
   alaQoSPortCOS5MinimumBandwidth
   alaQoSPortCOS6MinimumBandwidth
   alaQoSPortCOS7MinimumBandwidth
```

qos port maximum egress-bandwidth

Configures the maximum rate at which to send traffic on the specified QoS port.

qos port *slot/port* **maximum egress-bandwidth** *bps*

qos port *slot/port* **no maximum egress-bandwidth**

Syntax Definitions

slot/port	The slot number and port number of the physical port.
bps	The maximum amount of bandwidth that may be used for all traffic egressing on the QoS port.

Defaults

By default, the maximum bandwidth is the maximum allowed for the interface type on which the port resides.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a configured maximum egress bandwidth value from a port.
- The maximum egress bandwidth value cannot exceed the maximum bandwidth of the interface type associated with the port.
- Modifying the maximum egress bandwidth is most useful for low-bandwidth links.

Examples

```
-> qos port 3/1 maximum egress-bandwidth 1000
-> qos port 3/1 no maximum egress-bandwidth
```

Release History

Release 6.1; command was introduced.
Release 6.3.1; **bandwidth** parameter changed to **egress-bandwidth**.

Related Commands

qos port maximum ingress-bandwidth	Configures the rate at which traffic is received on a QoS port.
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
   alaQoSPortMaximumBandwidth
   alaQoSPortMaximumBandwidthStatus
```

qos port maximum ingress-bandwidth

Configures the maximum rate at which traffic is received on a QoS port.

qos port *slot/port* **maximum ingress-bandwidth** *bps*

qos port *slot/port* **no maximum ingress-bandwidth**

Syntax Definitions

slot/port	The slot number and port number of the physical port.
bps	The maximum amount of bandwidth that may be used for all traffic ingressing on the QoS port.

Defaults

By default, the maximum bandwidth is the maximum allowed for the interface type on which the port resides.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a configured maximum ingress bandwidth value from a port.
- The maximum ingress bandwidth value cannot exceed the maximum bandwidth of the interface type associated with the port.
- Modifying the maximum ingress bandwidth is most useful for low-bandwidth links.

Examples

```
-> qos port 3/1 maximum ingress-bandwidth 1000
-> qos port 3/1 no maximum ingress-bandwidth
```

Release History

Release 6.3.1; command introduced.

Related Commands

qos port maximum egress-bandwidth	Configures the rate at which traffic is sent on a QoS port.
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
   alaQoSPortMaximumIngBandwidth
   alaQoSPortMaximumIngBandwidthStatus
```

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 6400, 6850E, 6855, 9000E

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.
- The default 802.1p value is not used if there is a matching QoS policy rule that sets the priority.
- Note that on the 802.1p bit for tagged packets received on untrusted ports is set with the default 802.1p value, which is configured using the **qos port default 802.1p** command. If the packet is untagged, however, then the DSCP bit is set with the default DSCP value, which is configured using the **qos port default dscp** command.

Examples

```
-> qos port 3/1 default 802.1p 5
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- The value configured by this command sets the upper byte (precedence) and therefore configures the ToS/DSCP value for the port.
- The default DSCP value is not used if there is a matching QoS policy rule that sets the priority.
- Note that on the 802.1p bit for tagged packets received on untrusted ports is set with the default 802.1p value, which is configured using the **qos port default 802.1p** command. If the packet is untagged, however, then the DSCP bit is set with the default DSCP value, which is configured using the **qos port default dscp** command.

Examples

```
-> qos port 3/1 default dscp 63
```

Release History

Release 6.1; 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 the default egress priority value to use for IP traffic ingressing on trusted ports.

qos port *slot/port* **default classification {802.1p | dscp}**

Syntax Definitions

slot/port	The slot number and port number of the physical port.
802.1p	Specifies that the 802.1p value of the flow will be used to prioritize flows coming in on the port.
dscp	Specifies that DSCP of the flow will be used to prioritize flows coming in on the port.

Defaults

parameter	default
802.1p | dscp	DSCP

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The egress priority assigned to an IP packet received on a trusted port is based on the DSCP value of the packet unless 802.1p is specified as the default priority value.
- Note that when the default priority value is set to DSCP (using the default DSCP value of 0), the DSCP value of a tagged IP packet is mapped to the 802.1p value for that same packet. In other words, the 802.1p priority is overwritten with the DSCP value. This does not apply to Layer 2 packets.
- The default classification priority is not used if there is a matching QoS policy rule that sets the egress priority value.
- This command does not affect Layer 2 traffic, which is always classified with 802.1p.
- In some network situations, some IP traffic may be dropped before any QoS rules can take effect for the traffic.

Examples

```
-> qos port 3/1 default classification tos
-> qos port 8/24 default classification dscp
-> qos port 7/1 default classification 802.1p
```

Release History

Release 6.1; 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
```

qos port dei

Configures the Drop Eligible Indicator (DEI) bit mapping and marking setting for the specified QoS port. The DEI setting applies to packets marked yellow (non-conforming) as the result of Tri-Color Marking (TCM) rate limiting.

qos port *slot/port* **dei {ingress | egress}**

qos port *slot/port* **no dei {ingress | egress}**

Syntax Definitions

slot/port	The slot number and port number of the physical port.
ingress	Maps the DEI/CFI bit to yellow (non-conforming) if this bit is set for ingress packets.
egress	Sets the DEI/CFI bit for egress packets if TCM marked the packets yellow.

Defaults

By default, no DEI/CFI bit mapping or marking is done.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to disable the DEI bit mapping (ingress) or marking (egress) configuration for the specified port
- Use the **qos dei** command to set the global DEI bit mapping and marking configuration for all QoS switch ports. Note that the port-level setting takes precedence over the global DEI setting.
- Packets marked yellow by TCM rate limiting are still transmitted when there is no congestion on the egress port queues. Setting the DEI/CFI bit for yellow egress packets (**qos port dei egress**) ensures that an upstream switch is made aware that the packet was marked yellow.
- When a switch receives a yellow packet with the DEI/CFI bit set and ingress DEI/CFI bit mapping is enabled (**qos port dei ingress**), the packet is mapped to an internal drop precedence or yellow color marking for the switch.

Examples

```
-> qos port 1/10 dei ingress
-> qos port 1/20 dei egress
-> qos port 1/10 no dei ingress
-> qos port 1/20 no dei egress
```

Release History

Release 6.4.3; command was introduced.

Related Commands

qos port	Configures a physical port for QoS.
qos dei	Configures the global Drop Eligible Indicator (DEI) bit mapping and marking setting for all QoS ports.
policy action cir	Configures a Tri-Color Marking policy action.
show qos config	Displays global information about the QoS configuration.
show qos port	Displays information about QoS ports.

MIB Objects

```
alaQoSPortTable
   alaQoSPortDEIMapping
   alaQoSPortDEIMarking
```

qos port monitor

Enables or disables the gathering of transmit and drop packet statistics for the egress queues of the specified port.

qos port *slot/port* **monitor**

qos port *slot/port* **no monitor**

Syntax Definitions

slot/port	The slot number and port number of the physical port.

Defaults

By default, monitoring is disabled for the port.

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- Use the **no** form of this command to disable QoS statistics monitoring for the specified port.
- Enabling QoS statistics monitoring resets all statistics counters for the port. At such point in time, statistics gathering is started and continues until the monitoring is disabled and enabled again or statistics are reset using the **qos stats reset** command.
- QoS statistics monitoring is allowed only on one port per slot at any given time.
- Use the **show qos queue** command to display statistics for QoS monitored ports.
- Enabling QoS port monitoring is required to capture statistics on a per port basis. Note that this command is not required on the OmniSwitch 9000E, as QoS monitoring is automatically active on all ports for these switches.

Examples

```
-> qos port 1/10 monitor
-> qos port 2/2 monitor
-> qos port 1/10 no monitor
-> qos port 2/2 no dei egress
```

Release History

Release 6.4.3; command was introduced.

Related Commands

qos port	Configures a physical port for QoS.
show qos port monitor	Displays ports that QoS is monitoring to gather egress CoS statistics.
show qos queue	Displays information and statistics for QoS priority queues.

MIB Objects

```
alaQoSPortTable
   alaQoSPortMonitor
```

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 6400, 6850E, 6855, 9000E

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/             Default    Default       Queues          Bandwidth          DEI
Port Active Trust P/DSCP Classification Deflt Total Physical Ingress Egress Map/Mark Type
-----+-----+-----+------+--------------+-----+-----+--------+-------+------+--------+--------
1/1   Yes     No  0/ 0        DSCP        8     0     100M      -       -     No /Yes ethernet
1/2    No     No  0/ 0        DSCP        8     0       0K      -       -     No /No  ethernet
1/3    No     No  0/ 0        DSCP        8     0       0K      -       -     No /No  ethernet
1/4    No     No  0/ 0        DSCP        8     0       0K      -       -     No /No  ethernet
1/5    No     No  0/ 0        DSCP        8     0       0K      -       -     No /No  ethernet
1/6    No     No  0/ 0        DSCP        8     0       0K      -       -     No /No  ethernet
1/7    No     No  0/ 0        DSCP        8     0       0K      -       -     No /No  ethernet
1/8    No     No  0/ 0        DSCP        8     0       0K      -       -     No /No  ethernet
1/9    No     No  0/ 0        DSCP        8     0       0K      -       -     No /No  ethernet
1/10   No     No  0/ 0        DSCP        8     0       0K      -       -    Yes /Yes ethernet
1/11   No     No  0/ 0        DSCP        8     0       0K      -       -     No /No  ethernet
1/12   No     No  0/ 0        DSCP        8     0       0K      -       -     No /No  ethernet
```

```
-> show qos port 1/1
Slot/             Default    Default       Queues          Bandwidth          DEI
Port Active Trust P/DSCP Classification Deflt Total Physical Ingress Egress Map/Mark Type
-----+-----+-----+------+--------------+-----+-----+--------+-------+------+--------+--------
1/1   Yes     No  0/ 0        DSCP        8     0     100M      -       -     No /Yes ethernet
```

output definitions

Slot/Port	The slot and physical port number.
Active	Whether or not the port is sending/receiving QoS traffic.
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 Classification	The default classification setting for the port (**802.1p** or **DSCP**).
Default Queues	The number of default queues.
Total Queues	The total number of queues.
Physical Bandwidth	The amount of physical bandwidth available on the port.
Ingress	The amount of ingress bandwidth for the port.
Egress	The amount of egress bandwidth for the port.
DEI Map	Whether or not the port maps the DEI bit for yellow (non-conforming) ingress packets.
DEI Mark	Whether or not the port sets the DEI bit for yellow (non-conforming) egress packets.
Type	The interface type, **ethernet** or **wan**.

Release History

Release 6.1; command was introduced.
Release 6.4.3; **DEI Map** and **Mark** fields added.

Related Commands

qos port	Configures a physical port for QoS.

MIB Objects

```
alaQoSPortTable
   alaQoSPortSlot
   alaQoSPortPort
   alaQoSPortEnabled
   alaQoSPortDefault8021p
   alaQoSPortDefaultDSCP
   alaQoSPortDefaultQueues
   alaQoSPortMaximumReservedBandwidth
   alaQoSPortMaximumDefaultBandwidth
   alaQoSPortDefaultClassification
alaQoSClassify
   alaQoSClassifySourceInterfaceType
```

show qos port monitor

Displays ports that are enabled to monitor egress CoS transmit and drop statistics.

show qos port monitor

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- This command displays ports that were configured to enable statistics monitoring using the **qos port monitor** command.
- Note that this command is not required on the OmniSwitch 9000E, as QoS monitoring is automatically active on all ports for these switches.

Examples

```
-> show qos port monitor

   NI     Port
--------+---------
   1      1/10
   2      2/5
   3      3/16
   4      4/26
   5      5/25
```

output definitions

NI	The slot number.
Port	The slot/port number for the switch port.

Release History

Release 6.4.3; command was introduced.

Related Commands

qos port monitor	Enables or disables statistics monitoring for a specific port.

MIB Objects

show qos queue

Displays information and statistics for all QoS queues or only for those queues associated with a specific port.

show qos queue [*slot/port***]**

Syntax Definitions

slot/port The physical slot and port number. For example: 3/1.

Defaults

By default, statistics are displayed for all queues.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the *slot/port* parameter to display queue statistics for a specific port.

Examples

```
-> show qos queue
Slot/     Q          Bandwidth Max  Max         Packets
Port  VPN No Pri Wt  Min   Max Bufs Depth      Xmit/Drop      Type
----+----+--+---+--+----------+----------+----------+----------------+---------
4/7  102  0  0   -   *     *     *     *         */*          PRI
4/7  102  1  1   -   *     *     *     *         */*          PRI
4/7  102  2  2   -   *     *     *     *         */*          PRI
4/7  102  3  3   -   *     *     *     *         */*          PRI
4/7  102  4  4   -   *     *     *     *         */*          PRI
4/7  102  5  5   -   *     *     *     *         */*          PRI
4/7  102  6  6   -   *     *     *     *         */*          PRI
4/7  102  7  7   -   *     *     *     *         */*          PRI

-> show qos queue  2/10
Slot/     Q          Bandwidth Max  Max         Packets
Port  VPN No Pri Wt  Min   Max Bufs Depth      Xmit/Drop      Type
----+----+--+---+--+----------+----------+----------+----------------+---------
2/10 102  0  0   -   *     *     *     *      1000/20         PRI
2/10 102  1  0   -   *     *     *     *      1000/20         PRI
2/10 102  2  0   -   *     *     *     *      1000/20         PRI
2/10 102  3  0   -   *     *     *     *      1000/20         PRI
2/10 102  4  0   -   *     *     *     *      1000/20         PRI
2/10 102  5  0   -   *     *     *     *      1000/20         PRI
2/10 102  6  0   -   *     *     *     *      1000/20         PRI
2/10 102  7  0   -   *     *     *     *      1000/20         PRI
```

output definitions

Slot/Port	The physical slot/port numbers associated with the queue.
VPN	The virtual port number associated with the queue.
Q No	The queue number (**0** through **7**).
Pri	The priority associated with the queue (**0** through **7)**, configured through the **policy action priority** command.
Wt	The weight value assigned to each queue. Configured through the **qos default servicing mode** and **qos port servicing mode** commands.
Bandwidth Min	The minimum bandwidth requirement for 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.
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	The type of queuing performed on this queue (**pri**, **wrr**, **drr**).

Release History

Release 6.1; command was introduced.
Release 6.1.1; **Q No** field was added.
Release 6.4.3; *slot/port* parameter 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).
qos port monitor	Enables QoS statistics monitoring for a specific port.

MIB Objects

```
alaQoSQueueTable
   alaQoSQueueId
   alaQoSQueueSlot
   alaQoSQueuePort
   alaQoSQueuePortId
   alaQoSQueueType
   alaQoSQueuePriority
   alaQoSQueueMinimumBandwidth
   alaQoSQueueMaximumBandwidth
   alaQoSQueueAverageBandwidth
   alaQoSQueueMaximumDepth
   alaQoSQueueMaximumBuffers
   alaQoSQueue8021p
   alaQoSQueuePacketsSent
   alaQoSQueuePacketsDropped
   alaQoSQueueMaxLength
   alaQoSQueueAverageLength
   alaQoSQueueCurrentLength
```

show qos slice

Displays rule availability and usage information for QoS slices of QoS slots. A *slice* is a logical section of hardware and corresponds to particular ports on the interface.

show qos slice {ingress | egress} [*slot/slice***]**

Syntax Definitions

ingress	Displays information for ingress rules.
egress	Displays information for egress rules.
slot/slice	The slot number and slice for which you want to view information. The number of slices per module varies depending on the type of module.

Defaults

By default, information is displayed for all slots/slices.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E
OmniSwitch 6400, 6855-U24X, 9000E; **egress** parameter supported.

Usage Guidelines

- Use the **ingress** parameter to display information for rules applied to ingress traffic.
- Use the **egress** parameter to display information for rules applied to egress traffic.
- Use the *slot/slice* parameter to display information for a specific slot or slice on the switch.
- This command is useful for monitoring switch resources required for policy rules.

Examples

```
-> show qos slice
Slot/            Ranges          Rules          Counters         Meters
Slice     Type Total/Free  CAM Total/Free      Total/Free      Total/Free
 3/0  Firebolt    16/16      0   128/101         128/101          64/64
                             1   128/125         128/125          64/64
                             2   128/0           128/0            64/64
                             3   128/0           128/0            64/64
                             4   128/0           128/0            64/64
                             5   128/0           128/0            64/64
                             6   128/0           128/0            64/64
                             7   128/0           128/0            64/64
                             8   128/0           128/0            64/64
                             9   128/0           128/0            64/64
                            10   128/0           128/0            64/64
                            11   128/0           128/0            64/64
                            12   128/0 (127)     128/0  (126)     64/64
                            13   128/0           128/24 (127)     64/64
                            14   128/0           128/62           64/64
                            15   128/124         128/123          64/63
```

output definitions

Slot/Slice	The slot and slice number.
Type	The type of slice.
Ranges Total	The total number of TCP/UDP port ranges supported per slot/slice.
Ranges Free	The number of TCP/UDP port ranges that are still available for use.
CAM	The CAM number.
Rules Total	The total number of rules supported per CAM.
Rules Free	The number of rules that are still available for use. On startup, the switch uses 27 rules.
Counters Total	The total number of counters supported per CAM.
Counter Free	The number of counters that are still available for use.
Meters Total	The total number of meters supported per CAM.
Meters Free	The number of meters that are still available for use.

Release History

Release 6.1; command was introduced.
Release 6.1.1: command modified to show policy rule usage and available resources.
Release 6.4.3: **ingress** and **egress** parameters 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

N/A

show qos log

Displays the log of QoS events.

show qos log

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use this command to display the current QoS log. To clear the log, use the **qos clear log** command.
- Logging of ARP packets is not supported.

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 6.1; 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 6400, 6850E, 6855, 9000E

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    : None
DEI:
 Mapping    : Enabled
 Marking    : Enabled
Classifier:
 Default queues          : 8
 Default queue service   : strict-priority
 Trusted ports           :  No
 NMS Priority            : Yes
 Phones             : trusted
 Default bridged disposition : accept
 Default routed disposition  : accept
 Default IGMP/MLD disposition    : accept
Logging:
 Log lines      : 256
 Log level      : 6
 Log to console :  No
 Forward log    :  No
Stats interval  : 60 seconds
Userports:
 Filter  : spoof
 Shutdown: none
Quarantine Manager:
  Quarantine MAC Group   : Quarantined
  Quarantined Page       :  No
  Remediation URL        :
Debug           : info
```

output definitions

QoS Configuration	Whether or not QoS is enabled or disabled. Configured through the **qos** command.
Mapping	Whether or not DEI mapping for ingress packets is enabled or disabled. Configured through the **qos dei** command.
Marking	Whether or not DEI marking for egress packets is enabled or disabled. Configured through the **qos dei** command
Default queues	The number of default queues for QoS ports. There are eight queues for each QoS port; this value is not configurable.
Default queue service	The default servicing mode for the switch (**strict-priority**, **WRR**, or **DRR**). Configured through the **qos default servicing mode** command.
Trusted Ports	The default trusted mode for switch ports. Configured through the **qos trust ports** command.
NMS Priority	Whether or not the automatic prioritization of NMS traffic is enabled or disabled. Configured through the **qos nms priority** command.
Phones	Whether or not IP Phone traffic is automatically trusted or assigned a priority value. Configured through the **qos phones** 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/MLD 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.
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.
Filter	The type of traffic that is filtered on ports that are members of the User-Ports group. Configured through the **qos user-port** command.
Shutdown	The type of traffic that will trigger an administrative shutdown of the port if the port is a member of the UserPorts group. Configured through the **qos user-port** command.
Quarantine MAC Group	The name of the Quarantine Manager and Remediation (QMR) MAC address group. Configured through the **qos quarantine mac-group** command. Note that this field only displays on an OmniSwitch 6855.

output definitions (continued)

Quarantined Page	Indicates whether or not QMR sends a Quarantined page to a client. Configured through the **qos quarantine page** command. Note that this field only displays on an OmniSwitch 6855.
Remediation URL	The URL for the QMR remediation server. Configured through the **qos quarantine path** command. Note that this field only displays on an OmniSwitch 6855.
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 6.1; command was introduced.
Release 6.1.1; **Filter** and **Shutdown** fields added.
Release 6.3.1; **NMS Priority**, **Phones**, and **Quarantine Manager** fields added.
Release 6.4.3; **DEI Mapping** and **Marking** fields 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
   alaQoSConfigDEIMapping
   alaQoSConfigDEIMarking
   alaQosConfigServicingMode
   alaQosConfigTrustPorts
   alaQoSConfigAutoNms
   alaQoSConfigAutoPhones
   alaQoSConfigDefaultBridgedDisposition
   alaQoSConfigDefaultRoutedDisposition
   alaQoSConfigDefaultMulticastDisposition
   alaQoSConfigLogLines
   alaQoSConfigLogLevel
   alaQoSConfigLogConsole
   alaQoSConfigStatsInterval
   alaQosConfigUserportFilter
   alaQosConfigUserportShutdown
   alaQoSConfigQMMacGroup
   alaQoSConfigQMPage
   alaQoSConfigQMPath
   alaQoSConfigDebug
```

show qos statistics

Displays statistics about the QoS configuration.

show qos statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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
  Spoofed Events        : 0
  NonSpoofed Events     : 0
  DropServices          : 0

Software resources
                     Applied                    Pending
         Table  CLI LDAP ACLM  Blt Total     CLI LDAP ACLM  Blt Total     Max
         rules    0    0    0    0     0       4    0    0    0     4    2048
       actions    0    0    0    0     0       1    0    0    0     1    2048
    conditions    0    0    0    0     0       1    0    0    0     1    2048
```

```
      services    0    0    0    0     0       0    0    0    0     0     256
service groups    1    0    0    0     1       1    0    0    0     1    1024
network groups    0    0    0    1     1       0    0    0    1     1    1024
   port groups    2    0    0   16    18       2    0    0   16    18    1024
    mac groups    0    0    0    0     0       0    0    0    0     0    1024
    map groups    0    0    0    0     0       0    0    0    0     0    1024
   vlan groups    0    0    0    0     0       0    0    0    0     0    1024

Hardware resources          TCAM                Ranges
   Slot Slice Unit   Used  Free   Max    Used  Free   Max
      1     0    0      0  1664  1664       0    16    16
      2     0    0      0  1664  1664       0    16    16
```

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.
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 classifier tree.
Max Ptree depth	The length of the longest path in the classifier tree.
Spoofed Events	The number of spoofed events.
Nonspoofed Events	The number of nonspoofed events.
DropServices	The number of TCP/UDP flows dropped.
Software Resources	The current usage and availability of software resources for the QoS configuration.
Hardware Resources	The current usage and availability of hardware resources for the QoS configuration.

Release History

Release 6.1; command was introduced.
Release 6.1.1; **Spoofed Events**, **Nonspoofed Events**, and **DropServices** fields added.
Release 6.3.4: **vlan groups** field added to Software Resources display.

Related Commands

qos stats reset	Resets QoS statistic counters to zero.

MIB Objects

```
alaQoSStats
   alaQoSStatsL2Events
   alaQoSStatsL2matches
   alaQoSStatsL2Drops
   alaQoSStatsL3IngressEvents
   alaQoSStatsL3IngressMatches
   alaQoSStatsL3IngressDrops
   alaQoSStatsL3EgressEvents
   alaQoSStatsL3EgressMatches
   alaQoSStatsL3EgressDrops
   alaQoSStatsFragments
   alaQoSStatsBadFragments
   alaQoSStatsUnknownFragments
   alaQoSStatsSpoofedEvents
   alaQoSStatsNonspoofedEvents
```

38 QoS Policy Commands

This chapter describes CLI commands used for policy management in the switch. The Quality of Service (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 can be created on the switch through CLI or SNMP commands, or they can 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.

Refer to Chapter 43, "QoS Commands," for information about commands used to configure QoS software.

MIB information for the QoS policy commands is as follows:

Filename: alcatelIND1Qos.mib
Module ALCATEL-IND1-QoS-MIB

Important Note. Some of the commands listed here are not currently supported on one or more platforms. See command descriptions in this chapter and check release notes for information about commands that are not supported.

The QoS Policy commands are listed here:

Policy commands	**policy rule** **policy validity period** **policy condition** **policy action** **policy list** **show policy action** **show policy condition** **show active policy rule** **show active policy rule meter-statistics** **show policy rule** **show policy validity period** **show active policy list** **show policy list**

Group commands	**policy network group** **policy service group** **policy mac group** **policy port group** **policy vlan group** **policy map group** **show policy network group** **show policy mac group** **show policy port group** **show policy vlan group** **show policy map group** **show policy service group**
Service commands	**policy service** **policy service protocol** **policy service source tcp port** **policy service destination tcp port** **policy service source udp port** **policy service destination udp port** **show policy service**

Condition commands	**policy condition** **policy condition source ip** **policy condition source ipv6** **policy condition destination ipv6** **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 established** **policy condition tcpflags** **policy condition service** **policy condition service group** **policy condition icmptype** **policy condition icmpcode** **policy condition ip protocol** **policy condition ipv6** **policy condition nh** **policy condition flow-label** **policy condition tos** **policy condition dscp** **policy condition source mac** **policy condition source mac group** **policy condition destination mac** **policy condition destination mac group** **policy condition source vlan** **policy condition source vlan group** **policy condition inner source vlan** **policy condition inner source vlan group** **policy condition destination vlan** **policy condition 802.1p** **policy condition inner 802.1p** **policy condition source port** **policy condition destination port** **policy condition source port group** **policy condition destination port group** **policy condition vrf**
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 depth** **policy action cir** **policy action tos** **policy action 802.1p** **policy action dscp** **policy action map** **policy action permanent gateway ip** **policy action port-disable** **policy action redirect port** **policy action redirect linkagg** **policy action no-cache** **policy action mirror**

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 AOS Release 6 Network Configuration Guide* for more information about creating these types of policies and information about valid condition/action combinations.

Access Control Lists	**policy condition** **policy action disposition** **policy rule**
ACLMAN interactive shell	**aclman**
Traffic prioritization/shaping	**policy action shared** **policy action priority** **policy action maximum bandwidth** **policy action maximum depth** **policy action cir** **policy rule**
802.1p/ToS/DSCP tagging or mapping	**policy condition tos** **policy condition dscp** **policy condition 802.1p** **policy action tos** **policy action 802.1p** **policy action dscp** **policy action map** **policy rule**
Policy based port mirroring	**policy action mirror**
VLAN Stacking (Ethernet Services)	**policy condition inner source vlan** **policy condition inner 802.1p**

aclman

Invokes the Access Control List Manager (ACLMAN) interactive shell for using common industry syntax to create ACLs.

aclman

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Invoking multiple, concurrent ACLMAN shells is supported.
- Once the shell is active, Alcatel-Lucent CLI commands are no longer accepted. Refer to the *OmniSwitch AOS Release 6 Network Configuration Guide* for more information about ACLMAN commands and usage.
- Commands entered using the ACLMAN shell are interpreted and converted to Alcatel-Lucent CLI syntax that is used for creating QoS filtering policies.
- Note that a user with read-only access to the Alcatel-Lucent CLI policy domain is restricted to using only the ACLMAN **clear**, **exit**, and **show** commands when the shell is active.

Examples

```
-> aclman
```

Release History

Release 6.1.2; command was introduced.

Related Commands

N/A

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***] [validity period** *name* **| no validity period] [save] [log [log-interval** *seconds***]] [count {packets | bytes}] [trap | no trap] [default-list | no default-list]**

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.
name	The name of a user-defined validity period that is associated with this rule. Validity periods are configured through the **policy validity period** command.
save	Marks the policy rule so that it can 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.
seconds	Configures how often to look for packets that match this policy rule when rule logging is applied (in the range from 0–3600 seconds). A value of 0 specifies to log as often as possible.
packets	Counts the number of packets that match the rule.
bytes	Counts the number of bytes that match the rule.
trap	Enables or disables traps for the rule.
default-list	Adds or removes the policy rule from the default policy list.

Defaults

By default, rules are not reflexive, but they are saved to the configuration.

parameter	default
enable | disable	enable
precedence	0
log	no
log-interval	30 seconds
packets | bytes	packets
trap	enable
default-list	add to default list

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 can 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.
- Only one validity period is associated with a policy rule. Each time this command is entered with a validity period name specified, the existing period name is overwritten with the new one.
- Software and hardware resources are allocated for rules associated with a validity period even if the validity period is not active. Pre-allocating the resources makes sure the rule can be enforced when the validity period becomes active.
- 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 **reload issu** 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.
- The **log** option is useful for determining the source of attacks on the switch firewall.
- Logging of ARP packets is not supported.

- If traps are enabled for the rule, a trap is only sent when a port disable action or UserPort shutdown operation is triggered.
- The **default-list** option adds the rule to the default policy list. Rules are added to this list by default when the rule is created. A rule can belong to multiple policy lists. As a result, the rule remains a member of the default list even when it is subsequently assigned to additional lists.
- Note that each time a rule is assigned to a policy list, an instance of that rule is created and each instance is allocated system resources. Use the **no default-list** option with this command to exclude the rule from the default policy list.
- 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 can 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.

Examples

```
-> policy rule rule2 condition c2 action a2
-> policy rule rule2 precedence 65535
-> policy rule rule2 validity period vp01
-> no policy rule rule2
-> policy rule rule2 no precedence
-> policy rule rule2 no validity period
-> policy rule rule2 no default-list
```

Release History

Release 6.1; command was introduced.
Release 6.1.1; **count** parameter added.
Release 6.3.4; **default-list** parameter added.

Related Commands

policy validity period	Configures a validity period that specifies days, times, and/or months during which an associated policy rule is in effect.
policy condition	Configures condition parameters.
policy action	Configures action parameters.
policy list	Adds or removes a policy rule from a policy list.
qos apply	Applies configured QoS and policy settings to the current configuration.
show active policy rule	Displays only those policy rules that are currently being enforced on the switch.
show policy rule	Displays information for policy rules configured on the switch.

MIB Objects

alaQoSRuleTable

- alaQoSRuleName
- alaQoSRuleEnabled
- alaQoSRuleSource
- alaQoSRulePrecedence
- alaQoSRuleCondition
- alaQoSRuleAction
- alaQoSRuleReflexive
- alaQoSRuleSave
- alaQoSRuleLog
- alaQoSRuleLogInterval
- alaQoSRuleCountType
- alaQoSRulePacketCount
- alaQoSRuleByteCount
- alaQoSRuleExcessPacketCount
- alaQoSRuleExcessByteCount
- alaQoSRuleTrapEvents
- alaQosRuleDefaultList

alaQoSAppliedRuleTable

- alaQoSAppliedRuleName
- alaQoSAppliedRuleEnabled
- alaQoSAppliedRuleSource
- alaQoSAppliedRulePrecedence
- alaQoSAppliedRuleCondition
- alaQoSAppliedRuleAction
- alaQoSAppliedRuleReflexive
- alaQoSAppliedRuleSave
- alaQoSAppliedRuleLog
- alaQoSAppliedRuleLogInterval
- alaQoSAppliedCountType
- alaQoSAppliedPacketCount
- alaQoSAppliedByteCount
- alaQoSAppliedExcessPacketCount
- alaQoSAppliedExcessByteCount
- alaQosAppliedDefaultList

policy validity period

Configures a validity period that specifies the days and times in which a policy rule is in effect.

policy validity period *name* **[[no] days** *days***] [[no] months** *months***] [[no] hours** *hh:mm* **to** *hh:mm* **| no hours] [interval** *mm:dd:yyyy hh:mm* **to** *mm:dd:yyyy hh:mm* **| no interval]**

no policy validity period *name*

Syntax Definitions

name	The name of the validity period (up to 31 alphanumeric characters).
days	The day(s) of the week this validity period is active. Enter the actual day of the week (for example, monday, tuesday, wednesday, and so on.).
months	The month(s) in which the validity period is active. Enter the actual month (for example, january, february, march, and so on.).
hh:mm	The time of day, specified in hours and minutes, the validity period starts and the time of day the validity period ends for example, 10:30 to 11:30).
mm:dd:yyyy hh:mm	An interval of time in which a rule is in effect. Specify a start and end to the interval period by entering a beginning date and time followed by an end date and time (for example, 11:01:2005 12:01 to 11:02:2005 12:01).

Defaults

By default, no validity period is in effect for a policy rule.

parameter	default
days	no restriction
months	no restriction
hh:mm	no specific time
mm:dd:yyyy hh:mm	no interval

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of the command to remove a validity period from the configuration, or to remove parameters from a particular validity period. Note that at least one parameter must be associated with a validity period.
- Any combination of days, months, hours, and interval parameters is allowed. The validity period is only in effect when all specified parameters are true.
- Use the **policy rule** command to associate a validity period with a rule.

- Software and hardware resources are allocated for rules associated with a validity period even if the validity period is not active. Pre-allocating the resources makes sure the rule can be enforced when the validity period becomes active.
- If the **snapshot** command is entered after the **policy validity period** command is configured, the resulting ASCII file will include the following additional syntax for the **policy validity period** command:

  from {cli | ldap | blt}

  This syntax indicates how the service was created. The **cli** and **ldap** options can 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 validity period vp01 days tuesday thursday months january february
-> policy validity period vp01 hours 13:00 to 19:00
-> policy validity period vp02 interval 01/01/05 12:01 to 02/01/05 11:59
-> policy validity period vp01 no days thursday
-> no policy validity period vp02
```

Release History

Release 6.1; command was introduced.

Related Commands

policy rule	Configures a policy rule on the switch and optionally associates that rule with a validity period.
show policy validity period	Displays information about policy validity periods.

MIB Objects

alaQoSValidityPeriodTable

- alaQoSValidityPeriodName
- alaQoSValidityPeriodSource
- alaQoSValidityPeriodDays
- alaQoSValidityPeriodDaysStatus
- alaQoSValidityPeriodMonths
- alaQoSValidityPeriodMonthsStatus
- alaQoSValidityPeriodHour
- alaQoSValidityPeriodHourStatus
- alaQoSValidityPeriodEndHour
- alaQoSValidityPeriodInterval
- alaQoSValidityPeriodIntervalStatus
- alaQoSValidityPeriodEndInterval

alaQoSAppliedValidityPeriodTable

- alaQoSAppliedValidityPeriodName
- alaQoSAppliedValidityPeriodSource
- alaQoSAppliedValidityPeriodDays
- alaQoSAppliedValidityPeriodDaysStatus
- alaQoSAppliedValidityPeriodMonths
- alaQoSAppliedValidityPeriodMonthsStatus
- alaQoSAppliedValidityPeriodHour
- alaQoSAppliedValidityPeriodHourStatus
- alaQoSAppliedValidityPeriodEndHour
- alaQoSAppliedValidityPeriodInterval
- alaQoSAppliedValidityPeriodIntervalStatus
- alaQoSAppliedValidityPeriodEndInterval

policy list

Configures a list of policy rules. There are two types of lists supported: User Network Profile (UNP) and egress. Rules assigned to a UNP list are applied to traffic classified into a specific profile. Rules assigned to an egress list are applied to traffic egressing on QoS ports.

policy list *list_name* **type [unp | egress] rules** *rule_name* **[***rule_name2***...] [enable | disable]**

no policy list *list_name*

policy list *list_name* **no rules** *rule_name* **[***rule_name2***...]**

Syntax Definitions

list_name	The name to assign to the policy list. Note that the list name is case sensitive.
unp	Applies the list of policy rules to the User Network Profile to which the list is assigned.
egress	Applies the list of policy rules to traffic egressing on QoS ports.
rule_name	The name of an existing QoS policy rule to include in the policy list.
rule_name2	Optional. The name of another QoS policy rule to include in the policy list. Separate each rule name specified with a space.
enable	Enables the policy list.
disable	Disables the policy list.

Defaults

A default policy list is available when the switch boots up. This list has no name and is not configurable. All QoS policy rules are assigned to this default list unless the **no default-list** option of the **policy rule** command is used.

parameter	default
unp | **egress**	**unp**
enable | **disable**	enabled

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E
OmniSwitch 6400, 6855-U24X, 9000E **egress** parameter supported.

Usage Guidelines

- Use the **no** form of the command to remove a policy list from the configuration or to remove a policy rule from an existing list.
- The QoS policy rule name specified with this command must already exist in the switch configuration.

- Only those rules that are assigned to an egress policy list are applied to egress traffic. However, certain policy conditions and actions are not supported within an egress policy list. For example, IPv6 conditions are not allowed. See the "Configuring QoS" chapter in the *OmniSwitch AOS Release 6 Network Configuration Guide* for more information.
- QoS changes DSCP and 802.1p values for traffic ingressing on an *untrusted* port. As a result, the new values can not match any egress policy list rules as expected. To avoid this scenario, trust the ingress port or configure a default ToS/DSCP/802.1p value as required.
- If an egress policy list rule contains an 802.1p condition and the ingress port is *trusted*, set the default classification of the ingress port to 802.1p. If the default classification of the ingress port is set to DSCP, the 802.1p value of the traffic is changed per the DSCP classification and will not match the egress 802.1p condition.
- Egress rate limiting configured through an Ethernet Service SAP profile takes precedence over egress rate limiting specified within a QoS egress policy list rule.
- A rule can belong to a UNP list, the default list, and an egress policy list at the same time. By default, a rule is assigned to a default policy list when the rule is created. If the rule is subsequently assigned to another policy list, it still remains associated with the default list.
- If a rule is a member of multiple policy lists but one or more of these lists are disabled, the rule is still active in those lists that are enabled.
- If the QoS status of a rule is disabled, then the rule is disabled for all lists even if a list to which the policy belongs is enabled.
- Any policy list configured through this command is not active on the switch until the **qos apply** command is issued.
- If the **snapshot** command is entered after the **policy list** command is configured, the resulting ASCII file will include the following additional syntax for the **policy list** command:

  from {cli | ldap | blt}

  This syntax indicates how the list was created. The **cli** and **ldap** options can 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 list unp1 type rules r1 r2 r3
-> policy list unp1 disable
-> policy list unp1 no rules r2
-> policy list unp1 enable
-> no policy list unp1
-> policy list egr1 type egress rules r1 r2 r3
-> policy list egr1 disable
-> policy list egr1 no rules r3
-> policy list egr1 enable
-> no policy list egr1
```

Release History

Release 6.3.4; command was introduced.
Release 6.4.3; **egress** parameter added.

Related Commands

policy rule	Configures a policy rule on the switch and optionally associates that rule with a validity period.
show policy rule	Displays information for policy rules configured on the switch.
show active policy list	Displays only those policy lists that are currently being enforced on the switch.
show policy list	Displays information for policy lists configured on the switch.

MIB Objects

```
alaQoSRuleGroupsTable
   alaQoSRuleDefaultList
   alaQoSRuleGroupsName
   alaQosRuleGroupsSource
   alaQosRuleGroupsType
   alaQosRuleGroupsEnabled
   alaQosRuleGroupsStatus
alaQosAppliedRuleGroupsTable
   alaQosAppliedRuleGroupsName
   alaQosAppliedRuleGroupsSource
   alaQosAppliedGroupsType
   alaQosAppliedGroupsEnabled
   alaQosAppliedRuleGroupsStatus
```

policy network group

Configures a network group name and its associated IP addresses. The group can 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 IPv4 address included in the network group. IPv6 addresses are not supported with network groups.
net_mask	The mask for the IPv4 address. If no mask is entered, the IPv4 address is assumed to be a host address.
ip_address2	Optional. Another IPv4 address to be included in the network group. Multiple IP addresses can be configured for a network group. Separate each address/mask combination with a space.
net_mask2	Optional mask for the IPv4 address. If no mask is entered, the natural mask for the address will be used.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use this command to configure a group of IPv4 addresses to which you want to apply QoS rules. Rather than create a condition for each IPv4 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 can 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 6.1; command was introduced.

Related Commands

policy condition	Configures a policy condition. A network group can 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 can 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 can be configured for a service group. Separate each service name with a space.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 *OmniSwitch AOS Release 6 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 can 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 6.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy service	Configures a service that can be used as part of a policy service group.
policy condition	Configures a policy condition. A network group can 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 can 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 can 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 6400, 6850E, 6855, 9000E

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.
- The MAC group name “alaPhones” is a reserved group name used to identify the MAC addresses of IP phones. See the **qos phones** command for more information.
- The MAC group name “Quarantined” is a reserved group name used to identify MAC address that are restricted through the Quarantine Manager and Remediation (QMR) switch application. This name is

configurable by the user, but “Quarantined” is used by default if a different name is not specified. See the **qos quarantine mac-group** command for more information.

- 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 can 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 6.1; command was introduced.

Related Commands

policy condition	Configures a policy condition. A MAC group can 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 can 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 can be included in the group; each combination should be separated by a space.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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* (that is, 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.
- 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.
- To prevent IP source address spoofing, add ports 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 traffic while still allowing normal traffic on the port. Refer to the *OmniSwitch AOS Release 6 Network Configuration Guide* for more information about ACL security enhancements.
- Use the **qos user-port** command to configure the option to filter or administratively disable a port when a specific type of traffic (Spoof, RIP, BPDU, OSPF, and/or BGP) is received on a port that is a member of the pre-defined UserPorts group.

- 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 can 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
-> policy port group UserPorts 4/1-8 5/1-8
```

Release History

Release 6.1; command was introduced.

Related Commands

policy condition	Configures a policy condition. A port group can 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 vlan group

Configures a VLAN group and its associated VLAN ID numbers. A VLAN group can be attached to a policy condition. The action associated with that policy will be applied to all members of the VLAN group.

policy vlan group *group_name vlan_id***[-***vlan_id***] [***vlan_id***[-***vlan_id***]...]**

no policy vlan group *group_name*

policy vlan group *group_name* **no** *vlan_id***[-***vlan_id***] [***vlan_id***[-***vlan_id***]...]**

Syntax Definitions

group_name	The name of the VLAN group (up to 31 alphanumeric characters).
*vlan_id***[-***vlan_id***]**	The VLAN ID to include in the group. At least one VLAN ID combination is required. To specify a contiguous range of VLAN IDs, use a hyphen. To specify multiple ID entries, use a space (for example, 10-15 50 100 250-252).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use this command to configure a group of VLAN IDs to which you want to apply QoS rules. Rather than create a condition for each VLAN, group VLANs together. Use the **policy condition** command to associate a condition with the VLAN group.
- Use the **no** form of the command to remove a VLAN group from the configuration, or to remove a VLAN from a VLAN group.
- If a range of VLANs is specified using the syntax *vlan_id-vlan_id* (that is, 1-8), a single VLAN within that range cannot be removed on its own. The entire range must be deleted as it was entered.
- If the **snapshot** command is entered after the **policy vlan 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 VLAN group was created. The **cli** and **ldap** options can 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 vlan group vlan_group1 100-200 205 240-245 1000
-> policy vlan group vlan_group2 1000-2000
-> policy vlan group vlan_group3 3000
```

```
-> policy vlan group vlan_group3 3000 3100-3105
-> no policy vlan group vlan_group2
-> policy vlan group vlan_group1 no 100-200
```

Release History

Release 6.3.4; command was introduced.

Related Commands

policy condition source vlan	Configures a source VLAN policy condition. A VLAN group can be configured as part of this type of policy condition.
policy condition inner source vlan	Configures an inner source VLAN policy condition. A VLAN group can be configured as part of this type of policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy vlan group	Displays information about policy VLAN groups.

MIB Objects

```
alaQoSVlanGroupsTable
   alaQoSVlanGroupsName
   alaQoSVlanGroupsSource
   alaQoSVlanGroupsStatus
alaQoSAppliedVlanGroupsTable
   alaQoSAppliedVlanGroupsName
   alaQoSAppliedVlanGroupsSource
   alaQoSAppliedVlanGroupsStatus
alaQoSVlanGroupTable
   alaQoSVlanGroupVlan
   alaQoSVlanGroupVlanEnd
   alaQoSVlanGroupStatus
alaQoSAppliedVlanGroupTable
   alaQoSAppliedVlanGroupVlan
   alaQoSAppliedVlanGroupVlanEnd
   alaQoSAppliedVlanGroupStatus
```

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 can 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. can 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 can be included.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a mapping pair or to remove the map group entirely.
- The map group can contain more than one mapping pair.
- 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 can 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 6.1; 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 service

Configures a service that can 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 can 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. Specify a range of ports using a hyphen (for example, **22-23**).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 can be used in combination.*
UDP ports for a service	**source udp port** **destination udp port**	*Keywords can 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 can 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 6.1; 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 can 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 6400, 6850E, 6855, 9000E

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 can 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 6.1; 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 can 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 6400, 6850E, 6855, 9000E

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 can 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 can 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 6.1; 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 can 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a service from the configuration, or to remove parameters from a particular service.
- This command is a shortcut for the **policy service protocol** command.
- A policy service can be grouped in a policy group using the **policy service group** command. A policy condition can then be associated with the service group.
- 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 can 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 6.1; 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 can 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 6400, 6850E, 6855, 9000E

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 can 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 can 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 6.1; 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 can 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- This command is a shortcut for the **policy service protocol** command.
- A policy service can be grouped in a policy group using the **policy service group** command. A policy condition can 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 can 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 6.1; 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 condition

Creates a QoS policy condition. The condition determines what parameters the switch uses to classify incoming flows. Condition parameters can be configured when the condition is created; or parameters can 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 can 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 can not be supported depending on the platform you are using. Also some condition parameters can not be supported with some action parameters. See the condition/action tables in the *OmniSwitch AOS Release 6 Network Configuration Guide*.

policy condition *condition_name*
[source ip *ip_address* **[mask** *netmask***]]**
[source ipv6 {any | *ipv6_address* **[mask** *netmask***]}**
[destination ip *ip_address* **[mask** *netmask***]]**
[destination ipv6 {any | *ipv6_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***]**
[ipv6]
[nh *next_header_value***]**
[flow-label *flow_label_value***]**
[tos *tos_value tos_mask***]**
[dscp {*dscp_value***[-***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***]**
[source vlan group *group_name***]**
[inner source vlan *vlan_id* **]**

[inner source vlan group *mac_group***]**
[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***]**
[vrf { *vrf_name* **| default}]**

no policy condition *condition_name*

Syntax Definitions

condition_name	The name of the condition. Any alphanumeric string.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of the command to remove a condition from a policy rule.
- A policy condition and a policy action are combined to make a policy rule. See the **policy rule** command for more information.
- Use the **qos apply** command to activate configuration changes.
- 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.
- For OmniSwitch 9000E, the detailed QoS policy condition is not accepted if it is based on both IPv6 source and destination addresses simultaneously. The detailed QoS policy rule including the policy condition and action must be applied separately on either IPv6 source or destination address.
- 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 can 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 6.1; 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
   alaQoSConditionSourceVlanGroup
   alaQoSConditionInnerSourceVlan
   alaQoSConditionInnerSourceVlanGroup
   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
   alaQoSConditionVrfName
   alaQoSConditionVrfNameStatus

alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionSource
   alaQoSAppliedConditionSourceSlot
   alaQoSAppliedConditionSourcePort
   alaQoSAppliedConditionSourcePortEnd
   alaQoSAppliedConditionSourcePortGroup
   alaQoSAppliedConditionDestinationSlot
   alaQoSAppliedConditionDestinationPort
   alaQoSAppliedConditionDestinationPortEnd
   alaQoSAppliedConditionDestinationPortGroup
   alaQoSAppliedConditionSourceInterfaceType
   alaQoSAppliedConditionDestinationInterfaceType
   alaQoSAppliedConditionSourceMacAddr
   alaQoSAppliedConditionSourceMacMask
   alaQoSAppliedConditionSourceMacGroup
   alaQoSAppliedConditionDestinationMacAddr
   alaQoSAppliedConditionDestinationMacMask
   alaQoSAppliedConditionDestinationMacGroup
   alaQoSAppliedConditionSourceVlan
   alaQoSAppliedConditionSourceVlanGroup
   alaQoSAppliedConditionInnerSourceVlan
   alaQoSAppliedConditionInnerSourceVlanGroup
   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
alaQoSAppliedConditionVrfName
alaQoSAppliedConditionVrfNameStatus
```

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 6400, 6850E, 6855, 9000E

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 6.1; 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 source ipv6

Configures a source IPv6 address for a policy condition.

policy condition *condition_name* **source ipv6 {any |** *ipv6_address* **[mask** *netmask***]}**

policy condition *condition_name* **no source ipv6**

Syntax Definitions

condition_name	The name of the condition.
any	Any source IPv6 address.
ipv6_address	A specific source IPv6 address.
netmask	The mask for the source IPv6 address.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of the command to remove a source IPv6 address from a condition; however, at least one classification parameter must be associated with a condition.
- If a mask is not specified, the IPv6 address is assumed to be a host address.
- For OmniSwitch 9000E, the detailed QoS policy condition is not accepted if it is based on both IPv6 source and destination addresses simultaneously. The detailed QoS policy rule including the policy condition and action must be applied separately on either IPv6 source or destination address.

Examples

```
-> policy condition cond3 source ipv6 ::1234:531F:BCD2:F34A
```

Release History

Release 6.1.3; 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
   alaQoSConditionSourceIpv6Addr
   alaQoSConditionSourceIpv6AddrStatus
   alaQoSConditionSourceIpv6Mask
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionSourceIpv6Addr
   alaQoSAppliedConditionSourceIpv6AddrStatus
   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 6400, 6850E, 6855, 9000E

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 6.1; 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
   alaQoSConditionDestinationIpAddr
   alaQoSConditionDestinationIpMask
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionDestinationIpAddr
   alaQoSAppliedConditionDestinationIpMask
```

policy condition destination ipv6

Configures a destination IPv6 address for a policy condition.

policy condition *condition_name* **destination ipv6 {any |** *ipv6_address* **[mask** *netmask***]}**

policy condition *condition_name* **no destination ipv6**

Syntax Definitions

condition_name	The name of the condition.
any	Any destination IPv6 address.
ipv6_address	A specific destination IPv6 address.
netmask	The mask for the source IPv6 address.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a destination IPv6 address from a condition; however, at least one classification parameter must be associated with a condition.
- If a mask is not specified, the IPv6 address is assumed to be a host address.

Examples

```
-> policy condition cond3 destination ipv6 ::1234:531F:BCD2:F34A
```

Release History

Release 6.1.3; 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
   alaQoSConditionDestinationIpv6Addr
   alaQoSConditionDestinationIpv6AddrStatus
   alaQoSConditionDestinationIpv6Mask
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionDestinationIpv6Addr
   alaQoSAppliedConditionDestinationIpv6AddrStatus
   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 6400, 6850E, 6855, 9000E

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.
- An IP multicast condition is used in IGMP ACLs. The multicast IP is the multicast group address used in the IGMP report packet.

Examples

```
-> policy condition cond4 multicast ip 224.1.1.1
```

Release History

Release 6.1; 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 38-17 for more information about this command.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 6.1; 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 38-17 for more information about this command.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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
   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) can be specified instead of a single port.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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** for more information.
- 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 6.1; 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) can be specified instead of a single port.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 for more information.
- 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 6.1; 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) can be specified instead of a single port.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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.
- Use this condition in combination with the IPv6 condition (**policy condition ipv6**) to configure IPv6 policies for Layer 4 information, services, and service groups.

Examples

```
-> policy condition cond3 source tcp port 137
-> policy condition cond4 ipv6 source tcp port 21
-> policy condition cond3 no source tcp port
```

Release History

Release 6.1; command was introduced.
Release 6.3.1; support for IPv6 policies added.

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) can be specified instead of a single port.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of the command to remove a destination 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 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.
- Use this condition in combination with the IPv6 condition (**policy condition ipv6**) to configure IPv6 policies for Layer 4 information, services, and service groups.

Examples

```
-> policy condition cond4 destination tcp port 137-138
-> policy condition cond5 ipv6 destination tcp port 140
-> policy condition cond4 no destination tcp port
```

Release History

Release 6.1; command was introduced.
Release 6.3.1; support for IPv6 policies added.

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) can be specified instead of a single port.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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.
- Use this condition in combination with the IPv6 condition (**policy condition ipv6**) to configure IPv6 policies for Layer 4 information, services, and service groups.

Examples

```
-> policy condition cond5 source udp port 1200-1400
-> policy condition cond6 ipv6 source udp port 1000
-> policy condition cond5 no source udp port
```

Release History

Release 6.1; command was introduced.
Release 6.3.1; support for IPv6 policies added.

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) can be specified instead of a single port.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of the command to remove a destination 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 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.
- Use this condition in combination with the IPv6 condition (**policy condition ipv6**) to configure IPv6 policies for Layer 4 information, services, and service groups.

Examples

```
-> policy condition cond4 destination udp port 137-138
-> policy condition cond5 ipv6 destination udp port 140
-> policy condition cond4 no destination udp port
```

Release History

Release 6.1; command was introduced.
Release 6.3.1; support for IPv6 policies added.

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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this 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 6.1; 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
   alaQoSConditionEthertype
   alaQoSConditionEthertypeStatus
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionEthertype
   alaQoSAppliedConditionEthertypeStatus
```

policy condition established

Configures an established TCP connection as a policy condition. A connection is considered established if the **ack** or **rst** flags in the TCP header of the packet are set.

policy condition *condition_name* **established**

policy condition *condition_name* **no established**

Syntax Definitions

condition_name	The name of the condition.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove **established** from a condition; however, at least one classification parameter must be associated with a condition.
- When an initial TCP connection packet is received only the **syn** flag is set. As a result, TCP packets are only examined if they are not the starting packet.
- Typically this condition is used in combination with **source ip, destination ip**, **source port**, **destination port**, **source TCP port**, or **destination TCP port** conditions.
- The **source mac**, **destination mac**, and **ethertype conditions** cannot be combined with the **established** condition parameter.
- Note that even though **established** can be used with most action parameters, it is mainly intended for ACL use.

Examples

```
-> policy condition cond2 source ip 192.168.5.10 established
-> policy condition cond3 destination ip 10.255.11.40
```

Release History

Release 6.1; 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
   alaQoSConditionTcpEstablished
alaQoSAppliedConditionTable
   alaQoSAppliedConditionTcpEstablished
```

policy condition tcpflags

Configures a specific TCP flag value or combination of flag values as a policy condition.

policy condition *condition_name* **tcpflags [any | all] {F | S | R | P | A | U | E | W} mask {F | S | R | P | A | U | E | W}**

policy condition *condition_name* **no tcpflags**

Syntax Definitions

condition_name	The name of the condition.
any	Match on any of the specified TCP flags.
all	Match all specified TCP flags.
F | S | R | P | A | U | E | W	TCP flag value to match (**F**=fin, **S**=syn, **R**=rst, **P**=psh, **A**=ack, **U**=urg, **E**=ecn, and **W**=cwr). *The **E** and **W** flags are currently not supported*.

Defaults

parameter	default
any | **all**	all

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of the command to remove **tcpflags** from a condition; however, at least one classification parameter must be associated with a condition.
- Use the **any** option to indicate that a match on any one of the specified TCP flags qualifies as a match for the condition. Use the **all** option to indicate that a match on all specified TCP flags is required to qualify as a match for the condition.
- Enter one or more TCP flags after the **any** or **all** keyword to indicate that the value of the flag bit must be set to one to qualify as a match.
- Enter one or more TCP flags after the **mask** keyword to indicate which TCP flags to match.
- If a TCP flag is specified as part of the **mask** but does not have a corresponding match value specified with the **any** or **all** options, then zero is assumed as the match value. For example, **tcpflags all f s mask f s a** looks for the following bit values to determine a match: **f**=1, **s**=1, **a**=0.
- Typically this condition is used in combination with **source ip, destination ip**, **source port**, **destination port**, **source TCP port**, or **destination TCP port** conditions.
- The **source mac**, **destination mac**, and **ethertype conditions** cannot be combined with the **established** condition parameter.

- Note that even though **tcpflags** can be used with most action parameters, it is mainly intended for ACL use.

Examples

```
-> policy condition c1 tcpflags all f s mask f s a
-> policy condition c2 tcpflags any a r mask a r
```

Release History

Release 6.1; 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
   alaQoSConditionTcpFlags,
   alaQoSConditionTcpFlagsStatus,
   alaQoSConditionTcpFlagsVal,
   alaQoSConditionTcpFlagsValStatus,
   alaQoSConditionTcpFlagsMask,
   alaQoSConditionTcpFlagsMaskStatus,
alaQoSAppliedConditionTable
   alaQoSAppliedConditionTcpFlags,
   alaQoSAppliedConditionTcpFlagsStatus,
   alaQoSAppliedConditionTcpFlagsVal,
   alaQoSAppliedConditionTcpFlagsValStatus,
   alaQoSAppliedConditionTcpFlagsMask,
   alaQoSAppliedConditionTcpFlagsMaskStatus,
```

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 6400, 6850E, 6855, 9000E

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 6.1; command was introduced.

Related Commands

policy service	Configures a service that can 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 38-19 for more information about this command.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 6.1; 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 icmptype

Configures an ICMP type value to use for traffic classification.

policy condition *condition_name* **icmptype** *type*

policy condition *condition_name* **no icmptype**

Syntax Definitions

condition_name	The name of the condition.
type	The ICMP type value, in the range 0–255.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the **no** form of the command to remove an ICMP type value from a condition; however, at least one classification parameter must be associated with a condition.

Examples

```
-> policy condition cond12 icmptype 100
```

Release History

Release 6.1; command was introduced.

Related Commands

policy condition	Creates a policy condition.
policy condition icmpcode	Configures an ICMP code value for traffic classification.
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
   alaQoSConditionIcmpType
   alaQoSConditionIcmpTypeStatus
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionIcmpType
   alaQoSAppliedConditionIcmpTypeStatus
```

policy condition icmpcode

Configures an ICMP code value to use for traffic classification.

policy condition *condition_name* **icmpcode** *code*

policy condition *condition_name* **no icmpcode**

Syntax Definitions

condition_name	The name of the condition.
code	The ICMP code value, in the range 0–255.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the **no** form of the command to remove an ICMP code value from a condition; however, at least one classification parameter must be associated with a condition.

Examples

```
-> policy condition cond12 icmpcode 150
```

Release History

Release 6.1; command was introduced.

Related Commands

policy condition	Creates a policy condition.
policy condition icmptype	Configures an ICMP type value for traffic classification.
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
   alaQoSConditionIcmpCode
   alaQoSConditionIcmpCodeStatus
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionIcmpCode
   alaQoSAppliedConditionIcmpCodeStatus
```

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. The range is 0–255.

Defaults

parameter	default
protocol	6

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 6.1; 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 ipv6

Configures a policy condition to classify IPv6 traffic.

policy condition *condition_name* **ipv6**

policy condition *condition_name* **no ipv6**

Syntax Definitions

condition_name	The name of the condition.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of the command to remove IPv6 traffic as a condition; however, at least one classification parameter must be associated with a condition.
- When the **ipv6** keyword is used in a condition, a policy that uses the condition is considered an IPv6 policy. IPv6 policies are effected only on IPv6 traffic. All other IP policies are considered IPv4 policies and are effected only on IPv4 traffic.
- IPv6 Layer 4 policies are supported and are configured using the **ipv6** keyword in a condition that specifies Layer 4 information, services, or service groups. Note that IPv6 Layer 4 policies only work with packets that contain a single header.
- The **icmptype** and **icmpcode** keywords in an IPv6 policy imply the ICMPv6 protocol, not the ICMPv4 protocol.

Examples

```
-> policy condition cond4 ipv6
-> policy condition cond5 ipv6 tos 7
-> policy condition cond6 ipv6 source port 1/1
-> policy condition cond7 ipv6 source tcp port 21
-> policy condition cond8 ipv6 source tcp port 0-1024
-> policy condition cond6 no ipv6
```

Release History

Release 6.1.3; command was introduced.
Release 6.3.1; support for IPv6 Layer 4 policies added.

Related Commands

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
   alaQoSConditionIpv6Traffic
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionIpv6Traffic
```

policy condition nh

Configures an IPv6 next header value as a policy condition. This value is compared to the next header value in the IPv6 header.

policy condition *condition_name* **nh** *next_header_value*

policy condition *condition_name* **no nh**

Syntax Definitions

condition_name	The name of the condition.
next_header_value	The next header value (0–255).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the **no** form of the command to remove the next header value as a condition; however, at least one classification parameter must be associated with a condition.

Examples

```
-> policy condition cond4 nh 100
-> policy condition cond4 no nh
```

Release History

Release 6.1.3; command was introduced.

Related Commands

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
- alaQoSConditionIpv6NH
- alaQoSConditionIpv6NHStatus

alaQoSAppliedConditionTable
- alaQoSAppliedConditionName
- alaQoSAppliedConditionIpv6NH
- alaQoSAppliedConditionIpv6NHStatus

policy condition flow-label

Configures an IPv6 flow label value as a policy condition. This value is compared to the flow label value in the IPv6 header.

policy condition *condition_name* **flow-label** *flow_label_value*

policy condition *condition_name* **no flow-label**

Syntax Definitions

condition_name	The name of the condition.
flow_label_value	The flow-label value (0–1048575).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the **no** form of the command to remove the flow label value as a condition; however, at least one classification parameter must be associated with a condition.

Examples

```
-> policy condition cond4 flow-label 1500
-> policy condition cond4 no flow-label
```

Release History

Release 6.1.3; command was introduced.

Related Commands

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
   alaQoSConditionIpv6FlowLabel
   alaQoSConditionIpv6FlowLabelStatus
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionIpv6FlowLabel
   alaQoSAppliedConditionIpv6FlowLabelStatus
```

policy condition tos

Configures the precedence bits in the Type of Service (ToS) byte value for a policy condition.

policy condition *condition_name* **tos** *tos_value* **[mask** *tos_mask***]**

policy condition *conditioning* **no tos**

Syntax Definitions

conditioning	The name of the condition. can be an existing condition name or a new condition.
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).
tos_mask	The mask for the ToS bits, in the range 0–7.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a ToS value from a condition; however, at least one classification parameter must be associated with a condition.
- If a ToS value is specified, a DSCP value can not be specified.

Examples

```
-> policy condition cond2 tos 7
```

Release History

Release 6.1; 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
   alaQoSConditionTos
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionTos
```

policy condition dscp

Configures the Differentiated Services Code Point (DSCP) for a policy condition. The DSCP value defines the six most significant bits of the DS byte in the IP header.

policy condition *condition_name* **dscp {***dscp_value***[-***value***]} [mask** *dscp_mask***]**

policy condition *condition_name* **no dscp**

Syntax Definitions

condition_name	The name of the condition. can be an existing condition name or a new condition.
{*dscp_value*[-*value*]}	The DiffServ Code Point value, in the range 0–63. Use a hyphen to specify a range of DSCP values for the condition (for example, 10-20).
dscp_mask	The mask for the DiffServ Code Point, in the range 0–63.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a DSCP value from a condition; however, at least one classification parameter must be associated with a condition.
- If a DSCP value is specified, a ToS value can not be specified.

Examples

```
-> policy condition cond4 dscp 10
-> policy condition cond5 dscp 20-30
```

Release History

Release 6.1; 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
   alaQoSConditionDscp
   alaQoSConditionDscpMask
   alaQoSConditionDscpEnd
   alaQoSConditionDscpStatus
alaQosAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionDscp
   alaQoSAppliedConditionDscpMask
   alaQoSAppliedConditionDscpEnd
   alaQoSAppliedConditionDscpStatus
```

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. can 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 6400, 6850E, 6855, 9000E

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.

Examples

```
-> policy condition cond2 source mac 00:20:da:05:f6:23
```

Release History

Release 6.1; 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
   alaQoSConditionSourceMacAddr
   alaQoSConditionSourceMacMask
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionSourceMacAddr
   alaQoSAppliedConditionSourceMacMask
```

policy condition destination mac

Configures a destination MAC address for a policy condition.

Note. Specifying a destination MAC address and mask of all zeros (00:00:00:00:00:00) as a policy condition can result in the switch dropping all traffic. Only use this type of condition in combination with other policies that will allow desired traffic and/or if a source or destination slot/port is also part of the destination MAC 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. can 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 6400, 6850E, 6855, 9000E

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 6.1; 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
   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. can 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 38-21 for more information about this command.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 6.1; 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 mac group**

Syntax Definitions

condition_name	The name of the condition. can 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 38-21 for more information about this command.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 6.1; 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. can be an existing condition name or a new condition.
vlan_id	The source VLAN ID for the flow.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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.
- The **source vlan** policy condition classifies double-tagged traffic (for example, VLAN Stacking packets) based on the value of the *outer* VLAN tag of the packet. Use the **inner source vlan** policy condition to classify double-tagged traffic based on the value of the *inner* VLAN tag of the packet.
- A source VLAN ID and a source VLAN group cannot be specified in the same condition. However, a source VLAN ID or group and an inner source VLAN ID or group can be specified in the same condition.

Examples

```
-> policy condition cond5 source vlan 3
-> policy condition cond6 source vlan 150 inner source vlan 500
-> policy condition cond7 source vlan 300 inner source vlan group invlan1
```

Release History

Release 6.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
policy condition source vlan group	Associates a VLAN group with a policy condition.
policy condition inner source vlan	Configures an inner (customer) source VLAN ID as 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 source vlan group

Associates a source VLAN group with a policy condition.

policy condition *condition_name* **source vlan group** *vlan_group*

policy condition *condition_name* **no source vlan group**

Syntax Definitions

condition_name	The name of the condition. can be an existing condition name or a new condition.
vlan_group	The name of an existing VLAN group, configured through the **policy vlan group** command. See page 38-25 for more information about this command.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of the command to remove a source VLAN group from a policy condition; however, at least one classification parameter must be associated with a condition.
- The **source vlan group** condition classifies double-tagged traffic (for example, VLAN Stacking packets) based on the value of the *outer* VLAN tag of the packet. Use the **inner source vlan group** condition to classify double-tagged traffic based on the value of the *inner* VLAN tag of the packet.
- A source VLAN ID and a source VLAN group cannot be specified in the same condition. However, a source VLAN ID or group and an inner source VLAN ID or group can be specified in the same condition.

Examples

```
-> policy condition cond1 source vlan group vlan_group1
-> policy condition cond2 source vlan group vstack1 inner source vlan 150
-> policy condition cond3 source vlan group vstack1 inner source vlan group invlan1
-> policy condition cond1 no source vlan group
```

Release History

Release 6.4.3; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy vlan group	Configures a VLAN group and its associated VLAN IDs.
policy condition	Creates a policy condition.
policy condition inner source vlan group	Associates an inner source VLAN group with a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionSourceVlanGroup
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionSourceVlanGroup
```

policy condition inner source vlan

Configures an inner source VLAN ID as a policy condition. This condition applies to double-tagged VLAN Stacking traffic and is used to classify such traffic based on the inner VLAN ID tag, also known as the customer VLAN ID.

policy condition *condition_name* **inner source vlan** *vlan_id*

policy condition *condition_name* **no inner source vlan**

Syntax Definitions

condition_name	The name of the condition. can be an existing condition name or a new condition.
vlan_id	The inner source VLAN ID (customer VLAN ID) to match on double-tagged packets.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of the command to remove an inner source VLAN from a policy condition; however, at least one classification parameter must be associated with a condition.
- Policies that use the inner source VLAN condition are referred to as QoS VLAN Stacking policies. These are separate policies from those configured through the VLAN Stacking Service application.
- Use the **source vlan** policy condition to classify double-tagged traffic based on the value of the *outer* VLAN tag of the packet.
- Note that if the Quarantine Manager Remediation (QMR) feature is active on the switch, configuring VLAN Stacking services and inner VLAN or 802.1p policies is not available. QMR is considered active when there are MAC addresses present in the Quarantine MAC group.
- An inner source VLAN ID and an inner source VLAN group cannot be specified in the same condition. However, a source VLAN ID or group and an inner source VLAN ID or group can be specified in the same condition.

Examples

```
-> policy condition cond5 inner source vlan 3
-> policy condition cond6 source vlan 500 inner source vlan 150
-> policy condition cond7 source vlan 250 inner source vlan group invlan1
-> policy condition cond5 no inner source vlan
```

Release History

Release 6.3.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
policy condition inner source vlan group	Associates an inner source VLAN group with a policy condition.
policy condition source vlan	Configures a source VLAN ID as a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionInnerSourceVlan
   alaQoSConditionInnerSourceVlanStatus
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionInnerSourceVlan
   alaQoSAppliedConditionInnerSourceVlanStatus
```

policy condition inner source vlan group

Associates an inner source VLAN group with a policy condition.

policy condition *condition_name* **inner source vlan group** *vlan_group*

policy condition *condition_name* **no inner source vlan group**

Syntax Definitions

condition_name	The name of the condition. can be an existing condition name or a new condition.
vlan_group	The name of an existing VLAN group, configured through the **policy vlan group** command. See page 38-25 for more information about this command.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of the command to remove a source VLAN group from a policy condition; however, at least one classification parameter must be associated with a condition.
- The **inner source vlan group** condition classifies double-tagged traffic (for example, VLAN Stacking packets) based on the value of the *inner* VLAN tag of the packet. Use the **source vlan group** condition to classify double-tagged traffic based on the value of the *outer* VLAN tag of the packet.
- An inner source VLAN ID and an inner source VLAN group cannot be specified in the same condition. However, a source VLAN ID or group and an inner source VLAN ID or group can be specified in the same condition.

Examples

```
-> policy condition cond2 inner source vlan group vstack1
-> policy condition cond3 inner source vlan group invlan1 source vlan group vstack1
-> policy condition cond4 inner source vlan group invlan2 source vlan 250
-> policy condition cond2 no inner source vlan group
```

Release History

Release 6.4.3; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy vlan group	Configures VLAN group and its associated VLAN IDs.
policy condition	Creates a policy condition.
policy condition source vlan group	Associates a source VLAN group with a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionInnerSourceVlanGroup
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionInnerSourceVlanGroup
```

policy condition destination vlan

Configures a destination VLAN (multicast only) 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. can be an existing condition name or a new condition.
vlan_id	The destination VLAN ID for the flow.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a destination VLAN from a condition; however, at least one classification parameter must be associated with a condition.
- Note that this condition is supported for multicast only policies.

Examples

```
-> policy condition cond4 destination vlan 3
```

Release History

Release 6.1; 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
- alaQoSConditionDestinationVlan

alaQoSAppliedConditionTable
- alaQoSAppliedConditionName
- alaQoSAppliedConditionDestinationVlan

policy condition 802.1p

Configures the 802.1p value for a policy condition.

policy condition *condition_name* **802.1p** *802.1p_value***[**-*802.1p_value***]**

policy condition *condition_name* **no 802.1p**

Syntax Definitions

condition_name	The name of the condition. Specify an existing condition name or a new condition.
*802.1p_value***[**-*802.1p_value***]**	The 802.1p value, or a range of 802.1p values, in the 802.1Q VLAN tag for the flow. Use a hyphen to specify a range of values (for example, 2-5). Only one entry is allowed per command line (a single 802.1p value or a range of values, not both). Valid 802.1p values range from 0 (lowest priority) to 7 (highest priority).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Rather than creating several policy conditions for contiguous 802.1p values, it is possible to specify a range of values with this command to apply multiple 802.1p values with one condition.
- Use the **no** form of the command to remove an 802.1p value or range of values for a condition; however, at least one classification parameter must be associated with a condition.
- When a range of values is configured for a single condition, removing a single value from within that range is not allowed. All 802.1p values are removed from a condition when the **no** form of this command is used.
- The **802.1p** policy condition classifies double-tagged traffic (for example, VLAN Stacking packets) based on the 802.1p value of the *outer* VLAN tag of the packet. Use the **inner 802.1p** condition to classify double-tagged traffic based on the 802.1p value of the *inner* VLAN tag of the packet.

Examples

```
-> policy condition cond1 802.1p 0-7
-> policy condition cond2 802.1p 5
-> policy condition cond3 802.1p 2-5
-> policy condition cond3 no 802.1p
```

Release History

Release 6.1; command was introduced.
Release 6.4.3; ability to specify a range of 802.1p values was added.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
policy condition inner 802.1p	Configures an inner (customer) source 802.1p value for a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSCondition8021p
   alaQoSCondition8021pEnd
   alaQoSCondition8021pStatus
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedCondition8021p
   alaQoSAppliedCondition8021pEnd
   alaQoSAppliedCondition8021pStatus
```

policy condition inner 802.1p

Configures an inner (customer) source 802.1p value for a policy condition. This condition applies to double-tagged VLAN Stacking traffic and is used to classify such traffic based on the inner 802.1p bit value.

policy condition *condition_name* **inner 802.1p** *802.1p_value***[-***802.1p_value***]**

policy condition *condition_name* **no inner 802.1p**

Syntax Definitions

condition_name	The name of the condition. can be an existing condition name or a new condition.
*802.1p_value***[-***802.1p_value***]**	The 802.1p value, or range of values, to match on the inner 802.1Q VLAN tag of double-tagged packets. Use a hyphen to specify a range of values (for example, 2-5). Only one entry is allowed per command line (a single 802.1p value or a range of values, not both). Valid 802.1p values range from 0 (lowest priority) to 7 (highest priority).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Rather than creating several policy conditions for contiguous inner 802.1p values, it is possible to specify a range of values with this command to apply multiple 802.1p values with one condition.
- Use the **no** form of the command to remove an inner 802.1p value, or range of values, for a condition; however, at least one classification parameter must be associated with a condition.
- When a range of values is configured for a single condition, removing a single value from within that range is not allowed. All 802.1p values are removed from a condition when the **no** form of this command is used.
- Policies that use the inner 802.1p condition are referred to as QoS VLAN Stacking policies. These are separate policies from those configured through the VLAN Stacking Service application.
- Use the **source 802.1p** policy condition to classify double-tagged traffic based on the 802.1p value of the *outer* VLAN tag of the packet.
- Note that if the Quarantine Manager Remediation (QMR) feature is active on the switch, configuring VLAN Stacking services and inner VLAN or 802.1p policies is not available. QMR is considered active when there are MAC addresses present in the Quarantine MAC group.

Examples

```
-> policy condition cond1 inner 802.1p 0-7
-> policy condition cond2 inner 802.1p 5
```

```
-> policy condition cond3 inner 802.1p 2-5
-> policy condition cond3 no inner 802.1p
-> policy condition cond2 no inner 802.1p
```

Release History

Release 6.3.1; command was introduced.
Release 6.4.3; ability to specify a range of 802.1p values was added.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
policy condition 802.1p	Configures the 802.1p value for a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionInner8021p
   alaQoSConditionInner8021pEnd
   alaQoSConditionInner8021pStatus
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionInner8021p
   alaQoSAppliedConditionInner8021pEnd
   alaQoSAppliedConditionInner8021pStatus
```

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. can 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 6400, 6850E, 6855, 9000E

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 6.1; 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
   alaQoSConditionSourceSlot
   alaQoSConditionSourcePort
   alaQoSConditionSourcePortEnd
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionSourceSlot
   alaQoSAppliedConditionSourcePort
   alaQoSAppliedConditionSourcePortEnd
```

policy condition destination port

Configures a destination port number for a policy 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. can 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 6400, 6855, 6850E, 9000E

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.
- The destination port condition only applies to bridged traffic on the OmniSwitch 6400 and 6855. However, this condition is applied to both bridged *and* routed traffic on the OmniSwitch 6850E, 6855-U24X, and 9000E.

Examples

```
-> policy condition cond3 destination port 4/2
-> policy condition cond4 destination port 4/3-4
```

Release History

Release 6.1; 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. can 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 38-23 for more information about this command.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 6.1; command was introduced.

Related Commands

policy port group	Configures a port group and its associated slot and port numbers.
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
- alaQoSConditionSourcePortGroup

alaQoSAppliedConditionTable
- alaQoSAppliedConditionName
- alaQoSAppliedConditionSourcePortGroup

policy condition destination port group

Associates a destination port group with a policy 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. can 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 38-23 for more information about this command.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 6.1; 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 vrf

Associates a Virtual Routing and Forwarding (VRF) instance with a policy condition.

policy condition *condition_name* **vrf {***vrf_name* | **default}**

policy condition *condition_name* **no vrf**

Syntax Definitions

condition_name	The name of the condition. can be an existing condition name or a new condition.
vrf_name	The name of the VRF instance to which the QoS policy condition applies.
default	Specifies the default VRF instance.

Defaults

By default, QoS policy conditions are not associated with any VRF instance. The policy applies across all instances.

Platforms Supported

OmniSwitch 6855-U24X, 9000E

Usage Guidelines

- Use the **no** form of the command to remove a VRF instance from a condition; however, at least one classification parameter must be associated with a condition.
- VRF policies are configured in the default VRF, similar to how all other QoS policies are configured. If the VRF name specified does not exist, the policy is not allocated any system resources.
- Policies that do not specify a VRF name are considered global policies and are applied across all VRF instances and VLANs.
- Policies that specify the default VRF apply only to traffic in the default VRF instance.
- Policies that specify a VRF name apply only to traffic in the VRF instance associated with that name.
- The **switch** network group is supported only in VRF policies that specify the default VRF instance. If this group is specified in a global policy (no VRF specified) then the policy is applied across all VRF instances.

Examples

```
-> policy condition cond6 vrf engr-vrf
-> policy condition cond7 vrf default
-> policy condition cond6 no vrf
```

Release History

Release 6.4.2; 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
   alaQoSConditionVrfName
   alaQoSConditionVrfNameStatus

alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionVrfName
   alaQoSAppliedConditionVrfNameStatus
```

policy action

Configures or deletes a QoS action. A QoS action describes how traffic that matches a particular QoS condition should be treated. It can specify a particular set of bandwidth and queue parameters, or it can 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 can 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 can not be supported depending on the platform you are using. Also some action parameters can not be supported with some conditions. See the condition table in the *OmniSwitch AOS Release 6 Network Configuration Guide*.

policy action *action_name*
[disposition {accept | drop | deny}]
[shared]
[priority *priority_value***]**
[maximum bandwidth *bps***]**
[maximum depth *bytes***]**
[cir *bps* **[cbs** *byte***] [pir** *bps***] [pbs** *byte***] [counter-color [red-nonred | green-nongreen | green-red | green-yellow | red-yellow]]**
[tos *tos_value***]**
[802.1p *802.1p_value***]**
[dcsp *dcsp_value***]**
[map {802.1p | tos | dscp} to {802.1p | tos| dscp} using *map_group***]**
[permanent gateway ip *ip_address***]**
[port-disable]
[redirect port *slot/port***]**
[redirect linkagg *link_agg***]**
[no-cache]
[{ingress | egress | ingress egress | no} mirror *slot/port***]**

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 6400, 6850E, 6855, 9000E

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 can be specified when the action is created or can be specified as separate commands.
- Use the **qos apply** command to activate configuration changes.
- Use the **no** form of the command to remove a QoS action from the configuration.
- 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 can 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 6.1; 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
   alaQoSActionCIR
   alaQoSActionCIRStatus
   alaQoSActionCBS
   alaQoSActionCBSStatus
   alaQoSActionPIR
   alaQoSActionPIRStatus
   alaQoSActionPBS
```

```
   alaQoSActionPBSStatus
   alaQoSActionCounterColor
   alaQoSAction8021p
   alaQoSActionTos
   alaQoSActionTosRewriteMask
   alaQoSActionDscp
   alaQoSActionMapFrom
   alaQoSActionMapTo
   alaQoSActionMapGroup
   alaQoSActionSourceRewriteIpAddr
   alaQoSActionSourceRewriteIpMask
   alaQoSActionSourceRewriteIpGroup
   alaQoSActionDestinationRewriteIpAddr
   alaQoSActionDestinationRewriteIpMask
   alaQoSActionDestinationRewriteIpGroup
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionSource
   alaQoSAppliedActionDisposition
   alaQoSAppliedActionMinimumBandwidth
   alaQoSAppliedActionMaximumBandwidth
   alaQoSAppliedActionPeakBandwidth
   alaQoSAppliedActionPriority
   alaQoSAppliedActionShared
   alaQoSAppliedActionMaximumBuffers
   alaQoSAppliedActionMaximumDepth
   alaQoSAppliedActionCIR
   alaQoSAppliedActionCIRStatus
   alaQoSAppliedActionCBS
   alaQoSAppliedActionCBSStatus
   alaQoSAppliedActionPIR
   alaQoSAppliedActionPIRStatus
   alaQoSAppliedActionPBS
   alaQoSAppliedActionPBSStatus
   alaQoSAppliedActionCounterColor
   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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this 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 a3 disposition deny
-> policy action a3 no disposition
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- If multiple rules have the same action, more than one flow can 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 can 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 6.1; 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
   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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a priority value from an action.
- 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 can be different from the value entered here.

Examples

```
-> policy action action1 priority 1
-> policy action action1 no priority
```

Release History

Release 6.1; 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
   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 can 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of the command to remove a maximum bandwidth value from an action.
- Note that the bandwidth can be entered in bits per second. Alternatively, the bandwidth can 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.

Examples

```
-> policy action action4 maximum bandwidth 10000
-> policy action action4 maximum bandwidth 10k
-> policy action action4 no maximum bandwidth
```

Release History

Release 6.1; 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
   alaQoSActionMaximumBandwidth
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionMaximumBandwidth
```

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 can 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a maximum depth value from a policy action.
- Note that the bandwidth can be entered in bytes. Alternatively, the bandwidth can 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.

Examples

```
-> policy action action2 maximum depth 100
-> policy action action2 no maximum depth
```

Release History

Release 6.1; 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
   alaQoSActionMaximumDepth
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionMaximumDepth
```

policy action cir

Configures a Tri-Color Marking (TCM) policy action. This type of action consists of parameters for Committed Information Rate (CIR), Committed Burst Size (CBS), Peak Information Rate (PIR), Peak Burst Size (PBS), and the counter color mode. TCM marks packets red, green, or yellow based on the parameter values of this policy action. The counter color mode determines which packets marked by this policy action are counted based on the resulting color of the packet.

policy action *action_name* **cir** *bps* **[cbs** *byte***] [pir** *bps***] [pbs** *byte***] [counter-color [red-nonred | green-nongreen | green-red | green-yellow | red-yellow]]**

policy action *action_name* **no cir** *bps*

policy action *action_name* **no pir** *bps*

Syntax Definitions

action_name	The name of the action.
bps	The burst size value, in bits per second.
byte	The desired value for maximum bucket size, in bytes.
green-red	Count the number of packets marked green (low drop precedence) and the number of packets marked red (packet is dropped). Packets marked yellow (high drop precedence) are not counted.
green-yellow	Count the number of green and yellow packets. Red packets are not counted.
red-yellow	Count the number red and yellow packets. Green packets are not counted.
red-nonred	Count the number of red and non-red (yellow and green) packets.
green-nongreen	Count the number of green and non-green (yellow and red) packets.

Defaults

parameter	default
bps	0
byte	10K (50K on 9000E)
counter-color	**red-yellow**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove the TCM parameter values.

- The **cir** and **pir** *bits* and the **cbs** and **pbs** *bytes* parameter values can be entered as an integer (for example, **10000**) or with abbreviated units (for example, **10m**).
- The **cbs** and **pbs** parameters are optional. If not specified, the switch uses 10K for these values by default.
- This implementation of TCM supports two rate limiting modes: Single-Rate (srTCM) and Two-Rate (trTCM). The srTCM mode marks packets based only on the CIR and the two burst sizes: CBS and PBS. The trTCM mode marks packets based on both the CIR and PIR and their associated CBS and PBS values.
- There is no explicit CLI command to configure the mode (srTCM or trTCM) in which the TCM meter operates. Instead, the mode is determined by the CIR and PIR values configured for the policy action. If the PIR value is greater than the CIR value, trTCM is used. If the PIR value is less than the CIR value, srTCM is used.
- Configuring CIR and CBS is similar to configuring a maximum bandwidth. Configuring CIR and PIR is similar to configuring maximum depth.
- The number of packets counted as a result of the counter color mode setting is displayed using the **show active policy rule meter-statistics** command. These statistics are only shown for those rules that are configured with a TCM policy action.

Examples

The following command examples configure srTCM (the default):

```
-> policy action A3 cir 10M
-> policy action A4 cir 10M cbs 4k
-> policy action A5 cir 10M cbs 4k pir 10M
-> policy action A6 cir 10M cbs 4k pir 10M pbs 4k
-> policy action a7 cir 5M cbs 2k counter-color green-nongreen
-> policy action A3 no cir
-> policy action A5 no pir
```

The following command examples configure trTCM (note that PIR is greater than CIR):

```
-> policy action A7 cir 10M cbs 4k pir 20M
-> policy action A8 cir 10M cbs 4k pir 20M pbs 40M
-> policy action a9 cir 5M cbs 1M pbs 10M pbs 2M counter-color green-yellow
-> policy action A7 no cir
```

Release History

Release 6.4.3; command was introduced.

Related Commands

policy action	Creates a policy action.
show policy action	Displays information about actions configured on the switch.
show active policy rule	Displays information about pending and applied policy rules that are active (enabled) on the switch.
show active policy rule meter-statistics	Displays TCM packet color statistics for a policy rule.

MIB Objects

```
alaQoSActionTable
   alaQoSActionCIR
   alaQoSActionCIRStatus
   alaQoSActionCBS
   alaQoSActionCBSStatus
   alaQoSActionPIR
   alaQoSActionPIRStatus
   alaQoSActionPBS
   alaQoSActionPBSStatus
   alaQoSActionCounterColor
alaQoSAppliedActionTable
   alaQoSAppliedActionCIR
   alaQoSAppliedActionCIRStatus
   alaQoSAppliedActionCBS
   alaQoSAppliedActionCBSStatus
   alaQoSAppliedActionPIR
   alaQoSAppliedActionPIRStatus
   alaQoSAppliedActionPBS
   alaQoSAppliedActionPBSStatus
   alaQoSAppliedCounterColor
```

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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a ToS value from a policy action.
- 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 6.1; 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
   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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of the command to remove an 802.1p value from a policy action.
- 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 6.1; 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
- 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a DSCP value from a policy action.
- 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 6.1; 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
   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 6400, 6850E, 6855, 9000E

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).
- 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 6.1; 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 policy actions.
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 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of the command to remove a gateway IP address from a policy action.
- 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 6.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
show policy action	Displays information about policy actions.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionPermanentGatewayIpAddr
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionPermanentGatewayIpAddr
```

policy action port-disable

Administratively disables the source port of the traffic to which this action is applied.

policy action *action_name* **port-disable**

policy action *action_name* **no port-disable**

Syntax Definitions

action_name	The name of the action.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove **port-disable** from the policy action.
- An SNMP trap is sent when a port is administratively disabled through a port disable action or a User-Ports shutdown function.
- To enable a port disabled by this action, use the **interfaces admin** command to administratively enable the port or disconnect and reconnect the port cable.

Examples

```
-> policy action pd01 port-disable
-> policy action pb02 no port-disable
```

Release History

Release 6.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
show policy action	Displays information about policy actions.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionPortdisable
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionPortdisable
```

policy action redirect port

Redirects all traffic (flooded, bridged, routed, and multicast) matching a redirect policy to the specified port instead of the port to which the traffic was destined.

policy action *action_name* **redirect port** *slot/port*

policy action *action_name* **no redirect port**

Syntax Definitions

action_name	The name of the action.
slot/port	The slot and port number (or range of ports) that will receive the redirected traffic.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of the command to remove **redirect port** from the policy action.
- When redirecting routed traffic from VLAN A to VLAN B, the redirect port must belong to VLAN B (tagged or default VLAN).
- Routed packets (from VLAN A to VLAN B) are not modified after they are redirected; the source and MAC address remain the same. In addition, if the redirect port is tagged, the redirected packets will have a tag from the ingress VLAN A.
- If a route exists for the redirected flow, then redirected packets are the final post-routing packets.
- If a route does not exist for the redirected flow, the flow is not redirected to the specified port or link aggregate and is “blackholed”. As soon as a route is available, the flow is then redirected as specified in the policy.
- In most cases, a redirected flow will *not* trigger an update to the routing and ARP tables. If necessary, create a static route for the flow or assign the redirect port to the ingress VLAN (VLAN A) to send packets to the redirect port until a route is available.
- When redirecting bridged traffic on VLAN A, the redirect port must belong to VLAN A (tagged or default VLAN).

Examples

```
-> policy action rp01 redirect port 1/12
-> policy action rp01 no redirect port
```

Release History

Release 6.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
show policy action	Displays information about policy actions.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionRedirectSlot
   alaQoSActionRedirectPort
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionRedirectSlot
   alaQoSAppliedActionRedirectPort
```

policy action redirect linkagg

Redirects all traffic (flooded, bridged, routed, and multicast) matching a redirect policy to the specified link aggregate ID instead of the link aggregate to which the traffic was destined.

policy action *action_name* **redirect linkagg** *link_agg*

policy action *action_name* **no redirect linkagg**

Syntax Definitions

action_name	The name of the action.
link_agg	The link aggregate ID number (0–32) to assign to the specified VLAN. See Chapter 7, “Link Aggregation Commands.”.”

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove **redirect linkagg** from the policy action.
- When redirecting routed traffic from VLAN A to VLAN B, the redirect link aggregate ID must belong to VLAN B (tagged or default VLAN).
- Routed packets (from VLAN A to VLAN B) are not modified after they are redirected; the source and MAC address remain the same. In addition, if the redirect link aggregate ID is tagged, the redirected packets will have a tag from the ingress VLAN A.
- If a route exists for the redirected flow, then redirected packets are the final post-routing packets.
- If a route does not exist for the redirected flow, the flow is not redirected to the specified link aggregate ID and is “blackholed”. As soon as a route is available, the flow is then redirected as specified in the policy.
- In most cases, a redirected flow will *not* trigger an update to the routing and ARP tables. If necessary, create a static route for the flow or assign the redirect port or link aggregate ID to the ingress VLAN (VLAN A) to send packets to the redirect port until a route is available.
- When redirecting bridged traffic on VLAN A, the redirect port or link aggregate ID must belong to VLAN A (tagged or default VLAN).

Examples

```
-> policy action rp01 redirect port 1/12
-> policy action rp01 no redirect port
```

Release History

Release 6.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
show policy action	Displays information about policy actions.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionRedirectAgg
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionRedirectAgg
```

policy action no-cache

Prevents entries from being added to the hardware cache or TCAM and treats the policy as a software policy by sending all packets to the CPU to be processed.

policy action *action_name* **no-cache**

policy action *action_name* **no no-cache**

Syntax Definitions

action_name	The name of the action.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove **no cache** from the policy action.
- Recommended for use on traffic destined for the switch.
- This command is useful to reduce hardware ACL entries by moving switch access ACLs to the CPU.

Examples

```
-> policy action nc01 no-cache
-> policy action nc01 no no-cache
```

Release History

Release 6.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
show policy action	Displays information about policy actions.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionNocache
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionNocache
```

policy action mirror

Mirrors ingress, egress, or both ingress and egress packets that match a mirroring policy to the specified port.

policy action *action_name* **[ingress | egress | ingress egress] mirror** *slot/port*

policy action *action_name* **no mirror** *slot/port*

Syntax Definitions

action_name	The name of the action.
ingress	Mirrors ingress packets.
egress	Mirrors egress packets.
ingress egress	Mirrors ingress and egress packets.
slot/port	The slot and port number that will receive the mirrored traffic.

Defaults

parameter	default
ingress | egress | ingress egress	**ingress**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of the command to remove **mirror** from the policy action.
- Use this command to configure a mirror-to-port (MTP) action that is used for policy based mirroring.
- Only one MTP session is supported at any given time. As a result, all mirroring policies should specify the same MTP port.
- Policy based mirroring and the port based mirroring feature can run simultaneously on the same switch.

Examples

```
-> policy action a1 mirror 1/7 (default ingress)
-> policy action a1 ingress mirror 1/7
-> policy action a1 egress mirror 1/7
-> policy action a1 ingress egress mirror 1/7
-> policy action a1 no mirror
```

Release History

Release 6.3.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
show policy action	Displays information about policy actions.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionMirrorSlot
   alaQosActionMirrorPort
   alaQosActionMirrorMode
   alaQosActionMirrorModeStatus
```

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 can 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 specified 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 38-167 for more information about the potential screen display.

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

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 38-167 for more information about the potential screen display.

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

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 38-167 for more information about the potential screen display.

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

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 38-167 for more information about the potential screen display.

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

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 38-167 for more information about the potential screen display.

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

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 38-167 for more information about the potential screen display.

Release History

Release 6.1; 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 currently.*
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 6400, 6850E, 6855, 9000E

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 38-167 for more information about the potential screen display.

Release History

Release 6.1; 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 currently.*
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 6400, 6850E, 6855, 9000E

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 38-167 for more information about the potential screen display.

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

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 38-167 for more information about the potential screen display.

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

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 38-167 for more information about the potential screen display.

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

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 38-167 for more information about the potential screen display.

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

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 38-167 for information about the displayed fields.

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

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 can not be specified.

Examples

```
-> show policy classify l3 tos 7
```

See the output example given on page 38-167 for more information about the potential screen display.

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

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 can not be specified.

Examples

```
-> show policy classify l3 dscp 63
```

See the output example given on page 38-167 for more information about the potential screen display.

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

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 38-167 for more information about the potential screen display.

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

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 38-167 for more information about the potential screen display.

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

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 38-167 for more information about the potential screen display.

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Information for all policy network groups displays unless *network_group* is specified.
- The display can 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 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Information about all policy services is displayed unless *service_name* is specified.
- The display can 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 6.1; command was introduced.

Related Commands

policy service	Configures a service that can 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Information for all policy service groups displays unless *service_group* is specified.
- The display can 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 6.1; command was introduced.

Related Commands

policy service group	Configures a service group and its associated services. A service group can 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Information for all policy MAC groups displays unless *mac_group* is specified.
- The display can 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 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Information for all policy port groups displays unless *group_name* is specified.
- The display can 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**, and so on.).
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 6.1; 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 vlan group

Displays information about pending and applied policy VLAN groups.

show [applied] policy vlan group [*group_name***]**

Syntax Definitions

applied	Displays only those policy VLAN groups that have been applied.
group_name	The name of the policy VLAN group for which you want to display information; or a wildcard sequence of characters for displaying information about VLAN groups with similar names. Use an asterisk (*) to indicate a wildcard character.

Defaults

By default, all VLAN groups are displayed with this command.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the *group_name* parameter to display information for a specific VLAN group.
- The display can 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 vlan group
Group Name       vlan                  From
----------+------------------------+---------------
Vlan_grp1        100                    cli
Vlan_grp1        101                    cli
Vlan_grp1        200                    cli
Vlan_grp2        1234                   cli
Vlan_grp3        2000                   cli
Vlan_grp3        2001                   cli
Vlan_grp3        2003-2005              cli
Vlan_grp3        2500                   cli
Vlan_grp3        3000                   cli
```

```
-> show policy vlan group
Group Name       vlan                  From
---------+-----------------------+---------------
Vlan_grp2        1234                   cli
```

output definitions

Group Name	The name of the VLAN group.
VLAN	The VLAN IDs associated with the VLAN group.
From	The origin of the VLAN group: **cli** indicates that the entry was configured on the switch; **ldap** indicates the entry was configured through PolicyView; **blt** indicates the entry was set up automatically by the switch based on the current hardware.

Release History

Release 6.4.3; command was introduced.

Related Commands

policy vlan group	Configures a VLAN group and its associated VLAN ID numbers.

MIB Objects

```
alaQoSVlanGroupsTable
   alaQoSVlanGroupsName
   alaQoSVlanGroupsSource
   alaQoSVlanGroupsStatus
alaQoSAppliedVlanGroupsTable
   alaQoSAppliedVlanGroupsName
   alaQoSAppliedVlanGroupsSource
   alaQoSAppliedVlanGroupsStatus
alaQoSVlanGroupTable
   alaQoSVlanGroupVlan
   alaQoSVlanGroupVlanEnd
   alaQoSVlanGroupStatus
alaQoSAppliedVlanGroupTable
   alaQoSAppliedVlanGroupVlan
   alaQoSAppliedVlanGroupVlanEnd
   alaQoSAppliedVlanGroupStatus
```

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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Information for all policy map groups displays unless *group_name* is specified.
- The display can 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.
From	The origin of the port group: **cli** indicates that the entry was configured on the switch; **ldap** indicates the entry was configured through PolicyView.
Entries	The slot/port combinations associated with the port group.

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Information for all policy actions displays unless *action_name* is specified.
- The display can 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                      Burst size
Action Name From  Disp  Pri Share Min Max CIR PIR Max-Depth Bufs CBS PBS To
-----------+----+------+---+-----+---+---+---+---+---------+----+---+---+---
A3         cli   accept    No            10M
+A4        cli   accept    No            10M                    4K
A5         cli   accept    No            10M 10M                4K
A6         cli   accept    No
+A7        cli   accept    No
+A8        cli   accept    Yes
action1    cli   accept    No            10M 20M                4K
action2    cli   accept    No            10M 20M                4K  40M
```

```
-> show policy action a5
                                  Bandwidth                     Burst size
Action Name From  Disp  Pri Share Min Max CIR PIR Max-Depth Bufs CBS PBS To
-----------+----+------+---+-----+---+---+---+---+---------+----+---+---+---
A5          cli   accept    No            10M 10M               4K

-> show applied policy action
                                  Bandwidth                     Burst size
Action Name From  Disp  Pri Share Min Max CIR PIR Max-Depth Bufs CBS PBS To
-----------+----+------+---+-----+---+---+---+---+---------+----+---+---+---
A3          cli   accept    No            10M
A5          cli   accept    No            10M 10M               4K
A6          cli   accept    No
action1     cli   accept    No            10M 20M               4K
action2     cli   accept    No            10M 20M               4K  40M

-> show policy action action*
                                  Bandwidth                     Burst size
Action Name From  Disp  Pri Share Min Max CIR PIR Max-Depth Bufs CBS PBS To
-----------+----+------+---+-----+---+---+---+---+---------+----+---+---+---
action1     cli   accept    No            10M 20M               4K
action2     cli   accept    No            10M 20M               4K  40M
```

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.
Max Depth Bufs	Maximum depth (in Kbytes) of queues for traffic.

Release History

Release 6.1; command was introduced.

Related Commands

policy action	Creates a policy action. A QoS action is a particular set of bandwidth and queue parameters that can be applied to a flow matching particular QoS conditions.

MIB Objects

alaQoSActionTable

- alaQoSActionName
- alaQoSActionSource
- alaQoSActionDisposition
- alaQoSActionShared
- alaQoSActionMinimumBandwidth
- alaQoSActionMaximumBandwidth
- alaQosActionMaximumDepth

alaQoSAppliedActionTable

- alaQoSAppliedActionName
- alaQoSAppliedActionSource
- alaQoSAppliedActionDisposition
- alaQoSAppliedActionShared
- alaQoSAppliedActionMinimumBandwidth
- alaQoSAppliedActionMaximumBandwidth
- alaQoSAppliedActionMaximumDepth

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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Information for all policy conditions displays unless *condition_name* is specified.
- The display can 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 6.1; 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 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Information for all rules is displayed unless *rule_name* is specified.
- Use the **show policy rule** command to display inactive as well as active policy rules.
- Information for all rule types is displayed unless a keyword (**bridged**, **routed**, **multicast**) is specified.
- Applied rules can or can 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 can 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.

- A match can show for a rule that is not the highest precedence rule for a particular flow, but only the rule with the highest precedence is actually applied.

Examples

```
-> show active policy rule
            Policy              From  Prec Enab Act Refl Log Trap Save Def Matches
 R1                                cli     0  Yes Yes   No  No  Yes  Yes Yes   2
  (L2/3):                                C1 -> QoS_Action1

 R2                                cli     0  Yes Yes   No  No  Yes  Yes Yes   0
  (L2/3):                                C2 -> QoS_Action1

 R3                                cli     0  Yes Yes   No  No  Yes  Yes  Yes  0
  (L2/3):                                C3 -> QoS_Action1
```

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.)
Act	Whether or not the rule is enforceable by the switch (for example, qos is enabled, rule is valid and enabled, validity period is active).
Refl	Whether the rule is reflexive or not.
Log	Whether or not the switch will log messages about specific flows coming into the switch that match this policy rule. Configured through the **policy rule** command.
Trap	Whether or not traps are enabled for the rule. Configured through the **policy rule** command. A trap is sent when a port is administratively disabled through a port disable action or a UserPort shutdown function
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 **reload issu** command is entered, or saved after a reboot. Configured through the **policy rule** command.
Def	Whether or not the rule is a member of the default policy list. Configured through the **policy rule** command.
Matches	The number of flows matching this rule. Note that for ingress maximum bandwidth policies, the value in this field indicates the number of packets that exceed the bandwidth limit, not the packets that match the rule.
{L2/3}	The condition and the action associated with the rule; configured through the **policy condition** and **policy action** commands respectively.

Release History

Release 6.1; command was introduced.
Release 6.1.1; **Trap** column added; **Inact** column changed to **Act**.
Release 6.3.4; **Def** column added.

Related Commands

show policy rule	Displays information for policy rules configured on the switch.
show policy list	Displays information for policy lists configured on the switch.

MIB Objects

```
alaQoSRuleTable
   alaQoSRuleName
   alaQoSRuleEnabled
   alaQoSRuleSource
   alaQoSRulePrecedence
   alaQoSRuleActive
   alaQoSRuleReflexive
   alaQosRuleLog
   alaQosRuleTrapEvents
   alaQosRuleSave
   alaQosRuleDefaultList
   alaQoSRuleCondition
   alaQoSRuleAction
```

show active policy rule meter-statistics

Displays Tricolor Marking (TCM) packet color statistics for the policy rule. These statistics are kept for those rules that consist of a TCM policy action (**policy action cir**). A counter color mode is specified with the TCM policy action. The counter color mode determines which counter color statistics are displayed with this command.

show active policy rule [*rule_name***] meter-statistics**

Syntax Definitions

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

By default, statistics are displayed for all rules.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the optional *rule_name* parameter to display statistics for a specific policy rule.
- This command displays statistics for applied policy rules that are active (enabled) on the switch. Use the **show policy rule** command to display inactive as well as active policy rules.
- Applied rules can or can 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.
- Statistics are shown only for two out of the five available counter colors. The two counters shown are determined by the counter color mode configured for the TCM policy action. See the **policy action cir** command for more information.
- A TCM action specifies the rates and burst sizes used to determine drop precedence for packets to which the action is applied. Packets are marked a certain color based on whether or not they conform to the specified rates and burst sizes. The packet color indicates the drop precedence (Green = low drop precedence, Yellow = high drop precedence, and Red = packet is always dropped).
- Counter color statistics are shown even if there is no bandwidth management configured for the rule. In this case, the green counter will display the number of packets that matched the rule and the nongreen counter is set to zero.

Examples

The following command examples display statistics for the Green and Red counters. These are the two counters specified by the TCM policy action that is assigned to the “R1” and “R2” policy rules.

```
-> show active policy rule meter-statistics
Policy: R1, Counter Color Mode: GREEN_RED,
  Green     :       75,     Non-Green :       0,
  Red       :       50,     Non-Red   :       0,
  Yellow    :        0
```

```
Policy: R2, Counter Color Mode: GREEN_RED,
  Green     :       70,     Non-Green :       0,
  Red       :       50,     Non-Red   :       0,
  Yellow    :        0

-> show active policy rule r2 meter-statistics
Policy: R2, Counter Color Mode: GREEN_RED,
  Green     :       70,     Non-Green :       0,
  Red       :       50,     Non-Red   :       0,
  Yellow    :        0
```

output definitions

Policy	The name of the policy rule, configured through the **policy rule** command.
Counter Color Mode	The counter color mode configured for the TCM policy action using the **policy action cir** command.
Green	Packets marked green as a result of the TCM policy action; green packets have a low drop precedence.
Red	Packets marked red as a result of the TCM policy action; red packets are always dropped.
Yellow	The number of packets marked yellow as a result of the TCM policy action; yellow packets have a high drop precedence.
Non-Green	The number of yellow and red packets combined.
Non-Red	The number of green and yellow packets combined.

Release History

Release 6.4.3; command was introduced.

Related Commands

policy action cir	Configures a TCM policy action, including the counter color mode for the action.
qos stats reset	Resets QoS statistic counters to zero.
show policy action	Displays information for policy actions configured on the switch.
show policy rule	Displays information for policy rules configured on the switch.

MIB Objects

```
alaQoSRuleTable
   alaQoSRuleName
   alaQoSRuleGreenCount
   alaQoSRuleRedCount
   alaQoSRuleYellowCount
   alaQoSRuleNonGreenCount
   alaQoSRuleNonRedCount
alaQoSAppliedRuleTable
   alaQoSAppliedRuleName
   alaQoSAppliedRuleGreenCount
```

```
   alaQoSAppliedRuleRedCount
   alaQoSAppliedRuleYellowCount
   alaQoSAppliedRuleNonGreenCount
   alaQoSAppliedRuleNonRedCount
alaQoSActionTable
   alaQoSActionCounterColor
alaQoSAppliedActionTable
   alaQoSAppliedActionCounterColor
```

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 6400, 6850E, 6855, 9000E

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 can 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   Act Refl Log Trap Save Def
 r1                                cli     0  Yes   Yes   No  No  Yes  Yes Yes
  (L2/3):                               c1 -> a1

 r2                                cli     0  Yes   Yes   No  No  Yes  Yes Yes
  (L2/3):                               c2 -> a2

+r3                                cli     0  Yes   Yes   No  No  Yes  Yes  No
  (L2/3):                               c2 -> a3

+r4                                cli     0  Yes   Yes   No  No  Yes  Yes  No
  (L2/3):                               c1 -> a1

-> show applied policy rule
            Policy                From  Prec Enab   Act Refl Log Trap Save Def
 r1                                cli     0  Yes   Yes   No  No  Yes  Yes Yes
  (L2/3):                               c1 -> a1

 r2                                cli     0  Yes   Yes   No  No  Yes  Yes Yes
  (L2/3):                               c2 -> a2
```

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. Configured through the
Enab	Whether or not the rule is enabled.
Act	Whether or not the rule is enforceable by the switch (for example, qos is enabled, rule is valid and enabled, validity period is active).
Refl	Whether the rule is reflexive or not.
Log	Whether or not the switch will log messages about specific flows coming into the switch that match this policy rule. Configured through the **policy rule** command.
Trap	Whether or not traps are enabled for the rule. Configured through the **policy rule** command. A trap is sent when a port is administratively disabled through a port disable action or a UserPort shutdown function.
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 **reload issu** command is entered, or saved after a reboot. Configured through the **policy rule** command.

output definitions

Def	Whether or not the rule is a member of the default policy list. Configured through the **policy rule** command.
{L2/3}	The condition and the action associated with the rule; configured through the **policy condition** and **policy action** commands respectively.

Release History

Release 6.1; command was introduced.
Release 6.1.1; **Trap** column added; **Inact** column changed to **Act**.
Release 6.3.4; **Def** column added.

Related Commands

show active policy rule	Displays only those policy rules that are currently being enforced on the switch.
show policy list	Displays information for policy lists configured on the switch.

MIB Objects

```
alaQoSRuleTable
   alaQoSRuleName
   alaQoSRuleEnabled
   alaQoSRuleSource
   alaQoSRulePrecedence
   alaQoSRuleActive
   alaQoSRuleReflexive
   alaQosRuleLog
   alaQosRuleTrapEvents
   alaQosRuleSave
   alaQosRuleDefaultList
   alaQoSRuleCondition
   alaQoSRuleAction
```

show policy validity period

Displays information about policy validity periods.

show policy validity period [*name***]**

Syntax Definitions

name	The name of the validity period.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Information for all validity periods is displayed unless *name* is specified.
- Use the **show policy rule** command to display the validity period that is associated with a policy rule.

Examples

```
-> show policy validity period
        ValidityPeriod            From
 vp01                              cli
 *Days  : tuesday thursday
 *Months: january february
 *Hours : 13:00 - 14:00

 vp02                              cli
 *Days  : monday wednesday
 *Hours :  9:00 - 10:00

-> show policy validity period vp01
        ValidityPeriod            From
 vp01                              cli
 *Days  : tuesday thursday
 *Months: january february
 *Hours : 13:00 - 14:00
```

output definitions

ValidityPeriod	The name of the policy validity period, configured through the **policy validity period** 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 validity period originated: **cli** indicates that the entry was configured on the switch; **ldap** indicates the entry was configured through PolicyView.

output definitions

Days	The days of the week the validity period is active, configured through the **policy validity period** command. If this field does not appear, then the validity period is not restricted to specific days.
Months	The months during which the validity period is active, configured through the **policy validity period** command. If this field does not appear, then the validity period is not restricted to specific months.
Hours	The time of day the validity period begins and ends, configured through the **policy validity period** command. If this field does not appear, then the validity period is not restricted to a specific time.
Interval	The date and time a validity period interval begins and ends, configured through the **policy validity period** command. If this field does not appear, then the validity period is not restricted to a specific date and time interval.

Release History

Release 6.1; command was introduced.

Related Commands

policy validity period	Configures a validity period that specifies days, times, and/or months during which an associated policy rule is in effect.

MIB Objects

```
alaQoSValidityPeriodTable
   alaQoSValidityPeriodName
   alaQoSValidityPeriodSource
   alaQoSValidityPeriodDays
   alaQoSValidityPeriodDaysStatus
   alaQoSValidityPeriodMonths
   alaQoSValidityPeriodMonthsStatus
   alaQoSValidityPeriodHour
   alaQoSValidityPeriodHourStatus
   alaQoSValidityPeriodEndHour
   alaQoSValidityPeriodInterval
   alaQoSValidityPeriodIntervalStatus
   alaQoSValidityPeriodEndInterval
alaQoSAppliedValidityPeriodTable
   alaQoSAppliedValidityPeriodName
   alaQoSAppliedValidityPeriodSource
   alaQoSAppliedValidityPeriodDays
   alaQoSAppliedValidityPeriodDaysStatus
   alaQoSAppliedValidityPeriodMonths
   alaQoSAppliedValidityPeriodMonthsStatus
   alaQoSAppliedValidityPeriodHour
   alaQoSAppliedValidityPeriodHourStatus
   alaQoSAppliedValidityPeriodEndHour
   alaQoSAppliedValidityPeriodInterval
   alaQoSAppliedValidityPeriodIntervalStatus
   alaQoSAppliedValidityPeriodEndInterval
```

show active policy list

Displays information about applied policy lists that are active (enabled) on the switch.

show active policy list [*list_name***]**

Syntax Definitions

list_name	The name of the list for which you want to display information; or a wildcard sequence of characters for displaying information about lists with similar names. Use an asterisk (*) to indicate a wildcard character.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Information for all active rules is displayed unless a *list_name* is specified.
- Use the **show policy list** command to display inactive as well as active policy lists.
- Applied lists can or can not be active on the switch. Applied lists are inactive if they have been administratively disabled with the **disable** option in the **policy list** command.
- The display can include any of the following characters:

character	definition
+	Indicates that the policy list has been modified or has been created since the last **qos apply**.
-	Indicates the policy list is pending deletion.
#	Indicates that the policy list differs between the pending/ applied lists.

Examples

```
-> show active policy list
 Group Name                      From  Type  Enabled  Entries

 list1                           cli   unp    Yes      r1
                                                      r2

 +list2                          cli   unp    Yes      r3

 egress_list1                    cli   egress Yes      r1
                                                      r2
                                                      r3
```

output definitions

Group Name	The name of the policy list. Configured through the **policy list** command. A plus sign (+) preceding a policy list name indicates that the list was modified or created since the last **qos apply**.
From	Where the list originated.
Type	The type of rule (**unp** or **egress**). Configured through the **policy list** command. Note that the default policy list is not shown. Use the **show policy rule** command to display rules that are members of the default policy list.
Enabled	Whether or not the rule is enabled. Configured through the **policy list** command.
Entries	The QoS policy rules that are grouped together in this policy list. Configured through the **policy list** command.

Release History

Release 6.3.4; command was introduced.
Release 6.4.3; **egress** policy list type supported.

Related Commands

show policy list	Displays information about pending and applied policy lists.
show policy rule	Displays information about pending and applied policy rules

MIB Objects

```
alaQoSRuleGroupsTable
   alaQoSRuleDefaultList
   alaQoSRuleGroupsName
   alaQosRuleGroupsSource
   alaQosRuleGroupsType
   alaQosRuleGroupsEnabled
   alaQosRuleGroupsStatus
alaQosAppliedRuleGroupsTable
   alaQosAppliedRuleGroupsName
   alaQosAppliedRuleGroupsSource
   alaQosAppliedGroupsType
   alaQosAppliedGroupsEnabled
   alaQosAppliedRuleGroupsStatus
```

show policy list

Displays information about pending and applied policy lists.

show [applied] policy list [*list_name***]**

Syntax Definitions

applied	Displays only those policy lists that have been applied to the switch configuration.
list_name	The name of the list for which you want to display information; or a wildcard sequence of characters for displaying information about lists with similar names. Use an asterisk (*) to indicate a wildcard character.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Information for all rules is displayed unless a *list_name* is specified.
- Use the **show active policy list** command to display only active policy lists that are currently enforced on the switch.
- The display can include any of the following characters:

character	definition
+	Indicates that the policy list has been modified or has been created since the last **qos apply**.
-	Indicates the policy list is pending deletion.
#	Indicates that the policy list differs between the pending/ applied lists.

Examples

```
-> show policy list
 Group Name                      From  Type  Enabled  Entries
 list1                           cli   unp     Yes      r1
                                                       r2

 +list2                          cli   unp     Yes      r3

 egress_list1                    cli   egress  No       r1
                                                       r2
                                                       r3
```

```
-> show applied policy list
Group Name                        From  Type  Enabled  Entries
 list1                             cli   unp     Yes      r1
                                                         r2

 egress_list1                      cli   egress  No       r1
                                                         r2
                                                         r3
```

output definitions

Group Name	The name of the policy list. Configured through the **policy list** command. A plus sign (+) preceding a policy list name indicates that the list was modified or created since the last **qos apply**.
From	Where the list originated.
Type	The type of rule (**unp** or **egress**). Configured through the **policy list** command. Note that the default policy list is not shown. Use the **show policy rule** command to display rules that are members of the default policy list.
Enabled	Whether or not the rule is enabled. Configured through the **policy list** command.
Entries	The QoS policy rules that are grouped together in this policy list. Configured through the **policy list** command.

Release History

Release 6.3.4; command was introduced.
Release 6.4.3; **egress** policy list type supported.

Related Commands

show active policy list	Displays only those policy lists that are currently being enforced on the switch.
show policy rule	Displays information about pending and applied policy rules

MIB Objects

```
alaQoSRuleGroupsTable
   alaQoSRuleDefaultList
   alaQoSRuleGroupsName
   alaQosRuleGroupsSource
   alaQosRuleGroupsType
   alaQosRuleGroupsEnabled
   alaQosRuleGroupsStatus
alaQosAppliedRuleGroupsTable
   alaQosAppliedRuleGroupsName
   alaQosAppliedRuleGroupsSource
   alaQosAppliedGroupsType
   alaQosAppliedGroupsEnabled
   alaQosAppliedRuleGroupsStatus
```

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 37, "QoS Commands," for information about commands for creating and managing policies directly on the switch.

The policy commands are based on RFC 2251 and RFC 3060.

MIB information for policy server commands is as follows:

Filename: alcatelIND1policy.mib
Module: ALCATEL-IND1-POLICY-MIB

The 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 this 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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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.

output definitions (continued)

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 6.1; 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 6400, 6850E, 6855, 9000E

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 successful 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 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

This command displays information about policies created on directory servers only. Chapter 37, "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 currently.
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 6.1; 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 6400, 6850E, 6855, 9000E

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
```

:

output definitions

Event Time	The date and time the policy event occurred.
event description	A description of the event.

Release History

Release 6.1; 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
```

40 802.1X 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.

MIB information for the 802.1X port commands is as follows:

Filename: IEEE_8021X.mib
Module: IEEE8021-PAE-MIB

A summary of the available commands is listed here:

802.1X port commands	**802.1x** **802.1x initialize** **802.1x re-authenticate** **802.1x supp-polling retry** **show 802.1x** **show 802.1x users** **show 802.1x statistics** **show 802.1x non-supplicant** **show 802.1x rate-limit**
Access Guardian commands	**802.1x supplicant bypass** **802.1x non-supplicant allow-eap** **802.1x supplicant policy authentication** **802.1x pass-through** **captive-portal pass-through** **802.1x non-supplicant policy authentication** **802.1x non-supplicant policy** **802.1x policy default** **802.1x captive-portal policy authentication** **802.1x captive-portal name** **802.1x captive-portal session-limit** **802.1x captive-portal inactivity-logout** **802.1x captive-portal retry-count** **802.1x captive-portal address** **802.1x captive-portal proxy-server-url** **802.1x captive-portal proxy-server-port** **802.1x captive-portal dns-keyword-list** **802.1x captive-portal success-redirect-url** **802.1x captive-portal fail-redirect-url** **802.1x auth-server-down** **802.1x auth-server-down policy** **802.1x auth-server-down re-authperiod** **show 802.1x device classification policies** **show 802.1x auth-server-down** **show 802.1x captive-portal configuration**

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/port	The slot and port number of the 802.1x port.
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 6400, 6850E, 6855, 9000E

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 6.1; command was introduced.

Related Commands

aaa authentication 802.1x	Enables/disables the switch for 802.1X authentication.
vlan port 802.1x	Enables or disables 802.1X port-based access control on a mobile port.
aaa radius-server	Configures or modifies a RADIUS server for Authenticated VLANs, Authenticated Switch Access, or 802.1X port access control.
802.1x captive-portal address	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/port	The slot and port number of the 802.1x port.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 6.1; 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/port	The slot and port number of the 802.1x port.

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 6400, 6850E, 6855, 9000E

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 6.1; 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 (0–99).

Defaults

By default, the number of retries is set to 2.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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).
- Specify **0** for the number of retries to bypass polling attempts and automatically classify the device connected to the 802.1x port as a non-supplicant.
- Any devices previously authenticated on the port remain authenticated; however, re-authentication will not occur.
- 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 3/9 supp-polling retry 10
-> 802.1x 2/1 supp-polling retry 0
```

Release History

Release 6.1; command was introduced.
Release 6.3.1; command modified to accept **0** for the number of retries.

Related Commands

show 802.1x	Displays information about ports configured for 802.1X.
show 802.1x non-supplicant	Displays a list of all non-802.1x supplicants learned on one or more 802.1x ports.

MIB Objects

```
alaDot1xSuppPollingCnt
```

802.1x supplicant bypass

Configures whether or not MAC authentication is applied first to any client device (supplicant or non-supplicant) that is trying to connect through the specified 802.1x port.

802.1x *slot/port* **supplicant bypass {enable | disable}**

Syntax Definitions

slot/port	The slot and port number of the 802.1x port.
enable	Enables supplicant bypass on the specified port; MAC authentication is performed first.
disable	Disables supplicant bypass on the specified port; 802.1x authentication is attempted first.

Defaults

By default, supplicant bypass is disabled; 802.1x authentication is attempted first.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use this command together with the **802.1x non-supplicant allow-eap** command to initiate MAC authentication first on any device and then specify whether or not subsequent 802.1x authentication is also performed on that same device.
- This command is only supported on 802.1x ports configured for auto access control mode. See the **802.1x** command for more information about configuring the access control mode.
- Configuring 802.1x supplicant bypass is not allowed on ports where the 802.1x supplicant polling retry count is set to zero. Both operations are mutually exclusive on the same port.
- If supplicants are already connected to the specified port when 802.1x bypass is enabled for that port, the supplicants are automatically logged off to undergo authentication according to the enabled bypass configuration.
- When the 802.1x bypass configuration is modified or disabled, any non-supplicant devices are automatically logged off the port. This will free up those devices to undergo the authentication specified by the new bypass configuration.
- If re-authentication is configured for the 802.1x port and supplicant bypass is enabled, the MAC authentication followed by 802.1x authentication are initially performed as configured. However, only 802.1x authentication is performed during the re-authentication process, so there is no recheck to see if the MAC address of the user device is restricted.

Examples

```
-> 802.1x 3/1 supplicant bypass enable
-> 802.1x 3/1 supplicant bypass disable
```

Release History

Release 6.4.4; command was introduced.

Related Commands

802.1x	Configures 802.1x parameters for the specified port.
802.1x non-supplicant allow-eap	Configures whether or not subsequent 802.1x authentication is attempted based on the MAC authentication results.
show 802.1x	Displays the 802.1x configuration for the port.

MIB Objects

```
alaDot1xAuthPolicyTable
   alaDot1xSupplicantBypass
```

802.1x non-supplicant allow-eap

Configures whether or not the switch attempts subsequent 802.1x authentication for a device connected to an 802.1x bypass-enabled port. When 802.1x bypass is enabled on the port, MAC authentication is performed first on any device connected to that port. This command specifies the conditions under which 802.1x authentication is performed or bypassed after the initial MAC authentication process.

802.1x *slot/port* **non-supplicant allow-eap {pass | fail | noauth | none}**

Syntax Definitions

slot/port	The slot and port number of the 802.1x port.
pass	Allows 802.1x (EAP frame) authentication if the supplicant passes MAC authentication.
fail	Allows 802.1x (EAP frame) authentication if the supplicant fails MAC authentication.
noauth	Allows 802.1x (EAP frame) authentication if there is no MAC authentication configured on the port.
none	Prevents 802.1x authentication; only MAC authentication is performed on any device accessing this port.

Defaults

By default, only MAC authentication is applied to the supplicant device (802.1x classification is not performed on the supplicant device).

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The port specified with this command must also have 802.1x bypass enabled (see the **802.1x supplicant bypass** command). If bypass is not enabled, this command is not configurable and MAC authentication will not take precedence over 802.1x authentication.
- Using this command with the **none** parameter is similar to setting the supplicant polling retry counter to zero (see the **802.1x supp-polling retry** command). However, the functionality configured with each command differs as follows:
  - When the supplicant polling retry is set to zero, EAP frames are ignored. MAC authentication is only triggered when a non-EAP frame is received, which is when the supplicant times out and is in an open state.
  - When the allow EAP is set to none, EAP frames are ignored but MAC authentication is triggered when the first EAP frame is received and the supplicant is not in an open state.
- When successful MAC authentication returns a VLAN ID or User Network Profile (UNP) and the 802.1x bypass operation is configured to initiate 802.1x authentication when a device passes MAC authentication, the device is *not* moved into that VLAN or UNP. Instead, the device is moved into the

VLAN or UNP returned by 802.1x authentication. If 802.1x authentication does not provide such information, the device is moved based on the supplicant device classification policies.

Examples

```
-> 802.1x 3/1 non-supplicant allow-eap pass
-> 802.1x 4/1 non-supplicant allow-eap fail
-> 802.1x 5/1 non-supplicant allow-eap noauth
-> 802.1x 6/1 non-supplicant allow-eap none
```

Release History

Release 6.4.4; command was introduced.

Related Commands

802.1x	Configures 802.1x parameters for the specified port.
802.1x supplicant bypass	Configures the 802.1x bypass operation status for the 802.1x port.
show 802.1x	Displays the 802.1x configuration for the port.
show 802.1x device classification policies	Displays device classification policies configured for an 802.1x port.

MIB Objects

```
alaDot1xAuthPolicyTable
   alaDot1xSBAllowEAP
```

802.1x pass-through

Globally sets the switch to transparently forward 802.1x EAP frames.

802.1x pass-through {enable | disable}

Syntax Definitions

enable	Enables transparent forwarding of 802.1x EAP frames on the switch.
disable	Disables transparent forwarding of 802.1x EAP frames on the switch.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use this command to globally set the switch to transparently forward 802.1x EAP frames.
- Pass through mode must be enabled on the Layer 2 switch to allow EAP packets to be trapped on the Layer 3 switch for authentication.

Examples

```
-> 802.1x pass-through enable
-> 802.1x pass-through disable
```

Release History

Release 6.4.5; command introduced.

Related Commands

vlan port 802.1x	Configures 802.1X parameters on a particular slot/port.Typically used for port access control on a dedicated 802.1X port.
show 802.1x	Displays information about ports configured for 802.1X.

MIB Objects

```
alaDot1xPassThroughStatus
```

captive-portal pass-through

Globally sets the bridge OmniSwitch that does not have an IP address to transparently forward Captive-portal frames to reach the AAA server.

captive-portal pass-through {enable | disable}

Syntax Definitions

enable	Enables transparent forwarding of packets with Captive Portal IP address as destination are forwarded to the Layer 3 switch.
disable	Disables transparent forwarding of packets with Captive Portal IP address as destination are forwarded to the Layer 3 switch.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- No 802.1x configurations must be present on the switch before captive-portal pass-through is configured.
- Use this command to globally set the switch to transparently forward packets with Captive Portal IP address as destination to the AAA server on the Layer 3 switch.
- Use this command when **aaa radius server** has to be configured. Usually, captive portal pass-through is configured on a bridge OmniSwitch that does not have any IP address to reach the AAA server.

Examples

```
-> captive-portal pass-through enable
-> captive-portal pass-through disable
```

Release History

Release 6.4.5; command introduced.

Related Commands

show 802.1x	Displays information about ports configured for 802.1X.

MIB Objects

```
alaDot1xPassThroughStatus
```

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 | user-network-profile** *profile_name* **| vlan** *vid* | **default-vlan | block | captive-portal}...] [[fail] {user-network-profile** *profile_name* | **vlan** *vid* **| block | captive-portal}...]**

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.
profile_name	The name of an existing User Network Profile (UNP) to use for device classification.
vid	Use this VLAN ID number for device classification.
default-vlan	Assigns supplicant to the default VLAN for the 802.1x port.
block	Blocks supplicant access on the 802.1x port.
captive-portal	Use Captive Portal for web-based device classification.

Defaults

When 802.1x is enabled on the port, a default supplicant policy is defined for the port. This policy uses the **group-mobility** and **default-vlan** parameters for the **pass** case and the **block** parameter for the **fail** case.

When the **802.1x supplicant policy authentication** command is used without specifying any parameters, the following values for the **pass** and **fail** case are configured by default:

parameter	default
pass	block
fail	block

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Supplicant device classification policies are applied only 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, block**, or **captive-portal** parameters, referred to as terminal parameters (or policies). This applies to both pass and fail policies. If a terminal parameter is not specified, the **block** parameter is used by default.
- If the **captive-portal** parameter is specified with this command, then the Captive Portal authentication policy is applied to supplicant traffic. See the **802.1x captive-portal policy authentication** command page for more information.
- A User Network Profile (UNP) specifies a VLAN assignment for the device, whether or not Host Integrity Check (HIC) is required for the device, and if any QoS access control list (ACL) policies are applied to the device. See the **aaa user-network-profile** command page for information about how to create a UNP.
- 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.

Examples

```
-> 802.1x 3/1 supplicant policy authentication
-> 802.1x 4/1 supplicant policy authentication vlan 27 default-vlan
-> 802.1x 5/1 supplicant policy authentication group-mobility captive-portal
-> 802.1x 5/10 supplicant policy authentication pass group-mobility default-vlan
fail vlan 43 block
-> 802.1x 6/1 supplicant policy authentication pass group-mobility default-vlan
fail captive-portal
-> 802.1x 4/10 supplicant policy authentication pass user-network-profile fail
captive-portal
```

Release History

Release 6.1.2; command was introduced.
Release 6.3.4; **user-network-profile, captive-portal** parameters added.

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-supplicant	Displays a list of all non-supplicants learned on all 802.1x ports.
aaa certificate-password	Displays a list of all users for one or more 802.1X ports.

MIB Objects

```
alaDot1xAuthPolicyTable
   alaDot1xSuppPolicy
```

802.1x non-supplicant policy authentication

Configures a non-supplicant device 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 | user-network-profile** *profile_name* | **vlan** *vid* **| default-vlan | block | captive-portal}] [[fail] {group-mobility | user-network-profile** *profile_name* | **vlan** *vid* | **default-vlan | block | captive-portal}]**

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.
profile_name	The name of an existing User Network Profile (UNP) to use for device classification.
vlan *vid*	Use this VLAN ID number for device classification.
default-vlan	Assigns supplicant to the default VLAN for the 802.1x port.
block	Blocks supplicant traffic on the 802.1x port.
captive-portal	Use Captive Portal for web-based device classification.

Defaults

When 802.1x is enabled on the port, all non-supplicant traffic is blocked by default.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Non-supplicant device classification policies are applied only when successful MAC authentication *does not* return a VLAN ID, returns a VLAN ID that does not exist, or 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 determines the order in which they are applied. However, this type of policy must end with either the **default-vlan** or **block**, or **captive-portal** parameters, referred to as terminal parameters (or policies). This applies to both pass and fail policies. If a terminal parameter is not specified, the **block** parameter is used by default.
- If the **captive-portal** parameter is specified with this command, then the Captive Portal authentication policy is applied to supplicant traffic. See the **802.1x captive-portal policy authentication** command page for more information.
- A User Network Profile (UNP) specifies a VLAN assignment for the device, whether or not Host Integrity Check (HIC) is required for the device, and if any QoS access control list (ACL) policies are applied to the device. See the **aaa user-network-profile** command page for information about how to create a UNP.
- 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 3/1 non-supplicant policy authentication
-> 802.1x 4/1 non-supplicant policy authentication pass group-mobility fail
default-vlan
-> 802.1x 5/1 non-supplicant policy authentication group-mobility captive-portal
-> 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
-> 802.1x 6/1 non-supplicant policy authentication pass group-mobility default-vlan
fail captive-portal
-> 802.1x 4/10 non-supplicant policy authentication pass user-network-profile fail
captive-portal
```

Release History

Release 6.1.2; command was introduced.
Release 6.3.4; **user-network-profile, captive-portal** parameters added.

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-supplicant	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 | user-network-profile** *profile_name* | **vlan** *vid* | **default-vlan | block | captive-portal}**

Syntax Definitions

slot/port	The slot and port number of the 802.1x port.
group-mobility	Use Group Mobility rules for device classification.
profile_name	The name of an existing User Network Profile (UNP) to use 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.
captive-portal	Use Captive Portal for web-based device classification.

Defaults

By default no device classification policies are configured for an 802.1x port.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Because this policy does not use 802.1x or MAC authentication, only one classification parameter is specified and 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.
- If the **captive-portal** parameter is specified with this command, then the Captive Portal authentication policy is applied to non-supplicant traffic. See the **802.1x captive-portal policy authentication** command page for more information.
- A User Network Profile (UNP) specifies a VLAN assignment for the device, whether or not Host Integrity Check (HIC) is required for the device, and if any QoS access control list (ACL) policies are applied to the device. See the **aaa user-network-profile** command page for information about how to create a UNP.
- 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
-> 802.1x 5/10 non-supplicant policy vlan 500
-> 802.1x 6/1 non-supplicant policy user-network-profile
-> 802.1x 4/10 non-supplicant policy captive-portal
```

Release History

Release 6.1.2; command was introduced.
Release 6.3.4; **user-network-profile, captive-portal** parameters added.

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-supplicant	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 6400, 6850E, 6855, 9000E

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 6.1.2; 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-supplicant	Displays a list of all non-supplicants learned on all 802.1x ports.

MIB Objects

```
alaDot1xAuthPolicyTable
   alaDot1xSuppPolicy
```

802.1x captive-portal policy authentication

Configures a Captive Portal device classification policy for an 802.1x port. This type of policy is applied to both supplicants and non-supplicants that were classified by a supplicant or non-supplicant policy to use Captive Portal web-based authentication.

802.1x *slot/port* **captive-portal policy authentication pass {group-mobility | user-network-profile** *profile_name* | **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 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 authentication fails.
group-mobility	Use Group Mobility rules for device classification.
profile_name	The name of a User Network Profile to use for device classification.
vlan *vid*	Use this VLAN ID number for device classification.
default-vlan	Assigns the device to the default VLAN for the 802.1x port.
block	Blocks device traffic on the 802.1x port.

Defaults

A default Captive Portal policy is automatically configured when 802.1x is enabled on a port. This default policy uses the **default-vlan** parameter for the **pass** case and the **block** parameter for the **fail** case.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Captive Portal device classification policies are applied only when successful web-based authentication *does not* return a VLAN ID, returns a VLAN ID that does not exist, or when web-based authentication fails.
- When web-based authentication does return a VLAN ID that exists in the switch configuration, the device 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.
- 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 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.

- Captive Portal policies are applied only to 802.1x enabled mobile ports that are configured with an 802.1x supplicant or non-supplicant policy that specifies the use of Captive Portal web-based authentication.

Examples

```
-> 802.1x 3/1 captive-portal policy authentication pass vlan 100 block fail vlan 10
-> 802.1x 4/1 captive-portal policy authentication pass group-mobility
```

Release History

Release 6.3.4; 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 captive-portal session-limit	Configures the length of a Captive Portal session and the number of login attempts allowed before the device is classified as a failed login.
show 802.1x device classification policies	Displays device classification policies configured for an 802.1x port.
show 802.1x captive-portal configuration	Displays the global Captive Portal configuration for the switch.

MIB Objects

```
alaDot1xAuthPolicyTable
   alaDot1xCaptivePortalPolicy
```

802.1x captive-portal session-limit

Configures the length of an active Captive Portal session.

802.1x *slot/port* **captive-portal session-limit** *time*

Syntax Definitions

slot/port	The slot and port number of the 802.1x port.
time	The amount of time the Captive Portal session remains active. Valid range is from 1—999 hours.

Defaults

parameter	default
time	12 hours

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The parameters configured with this command apply to the Captive Portal configuration for the specified 802.1x port.
- At the end of the Captive Portal session time limit, the user is automatically logged out of the session and is no longer allowed to access the network.

Examples

```
-> 802.1x 3/1 captive-portal session-limit 8 retry-count 5
-> 802.1x 4/1 captive-portal session-limit 4 retry-count 2
```

Release History

Release 6.3.4; command was introduced.

Related Commands

802.1x captive-portal retry-count	Configures the number of login attempts allowed before the Captive Portal fail policy is applied to the device.
802.1x captive-portal policy authentication	Configures a Captive Portal device classification policy for an 802.1x port.
show 802.1x captive-portal configuration	Displays the global Captive Portal configuration for the switch.

MIB Objects

```
alaDot1xAuthPolicyTable
   alaDot1xCaptivePortalSessionLimit
```

802.1x captive-portal name

Configures the name of the rediret URL that is used for accessing a public certificate.

802.1x captive-portal name *cp_url_name*

802.1x captive-portal no name

Syntax Definitions

cp_url_name	The name to be used for the redirect URL.

Defaults

By default, the name of the redirect URL is set to “captive-portal”.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use this command to change the Captive Portal redirect URL name (captive-portal) to match the common name (cn) used by the public certificate on the switch. Matching these two names prevents a certificate warning message caused when these names do not match.
- Use the **no** form of this command to remove the configured Captive Portal redirect URL name. This reverts the URL name back to the default of “captive-portal”.
- This feature is not supported on HTTPS sessions.

Examples

```
-> 802.1x captive-portal name certname
-> 802.1x captive-portal no name
```

Release History

Release 6.4.4; command was introduced.

Related Commands

aaa certificate-password	Configures the password for accessing a public certificate on the switch.
show 802.1x captive-portal configuration	Displays the global Captive Portal configuration for the switch.

MIB Objects

```
alaDot1xAuthPolicyTable
   alaDot1xCPortalRedirectString
```

802.1x captive-portal inactivity-logout

Configures whether or not a user MAC address is flushed from the Captive Portal user table due to inactivity.

802.1x *slot/port* **captive-portal inactivity-logout {enable | disable}**

Syntax Definitions

slot/port	The slot and port number of the 802.1x port.
enable	Enables inactivity logout.
disable	Disables inactivity logout.

Defaults

By default, inactivity logout is disabled.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

This timer is based on the MAC address aging timer. If a user is flushed from the MAC address table due to inactivity, the user MAC address is also flushed from the Captive Portal user table.

Examples

```
-> 802.1x 3/1 captive-portal inactivity-logout enable
-> 802.1x 3/1 captive-portal inactivity-logout disable
```

Release History

Release 6.4.4; command was introduced.

Related Commands

802.1x captive-portal retry-count	Configures the number of login attempts allowed before the Captive Portal fail policy is applied to the device.
802.1x captive-portal policy authentication	Configures a Captive Portal device classification policy for an 802.1x port.
show 802.1x captive-portal configuration	Displays the global Captive Portal configuration for the switch.

MIB Objects

```
alaDot1xAuthPolicyTable
   alaDot1xCPortalInactivityLogout
```

802.1x captive-portal retry-count

Configures the number of login attempts allowed before the Captive Portal fail policy is applied to the device.

802.1x *slot/port* **captive-portal retry-count** *retries*

Syntax Definitions

slot/port	The slot and port number of the 802.1x port.
retries	The number of login attempts allowed (1–99).

Defaults

parameter	default
retries	3

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The parameters configured with this command apply to the Captive Portal configuration for the specified 802.1x port.
- When a device has failed the allowed number of login attempts, the **fail** case for the Captive Portal policy configured for the 802.1x port is applied. To allow an unlimited number of login attempts, specify zero for the retry count value.

Examples

```
-> 802.1x 3/1 captive-portal session-limit 8 retry-count 5
-> 802.1x 4/1 captive-portal session-limit 4 retry-count 2
```

Release History

Release 6.3.4; command was introduced.

Related Commands

802.1x captive-portal session-limit	Configures the length of an active Captive Portal session.
802.1x captive-portal policy authentication	Configures a Captive Portal device classification policy for an 802.1x port.
show 802.1x captive-portal configuration	Displays the global Captive Portal configuration for the switch.

MIB Objects

```
alaDot1xAuthPolicyTable
   alaDot1xCaptivePortalRetryCnt
```

802.1x captive-portal address

Configures a different subnet for the Captive Portal IP address (10.123.0.1).

802.1x captive-portal address *ip_address*

Syntax Definitions

address	The IP address for the Captive Portal login page. This IP address must use the following octet values: 10.x.0.1, where “x” is used to specify a new subnet value.

Defaults

By default, the Captive Portal IP address is set to 10.123.0.1.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- If the 10.123.0.1 subnet is already in use on the network, use this command to change the second octet of this IP address. Note that the second octet is the only configurable part of the Captive Portal IP address that is allowed.
- This IP address is used exclusively by the Captive Portal feature to serve various pages and to assign a temporary IP address for a client device that is attempting web-based authentication.

Examples

```
-> 802.1x captive-portal address 10.11.0.1
-> 802.1x captive-portal address 10.124.0.1
```

Release History

Release 6.3.4; command was introduced.

Related Commands

show 802.1x captive-portal configuration	Displays the global Captive Portal configuration for the switch.

MIB Objects

```
alaDot1xCportalConfig
   alaDot1xCPortalIpAddress
```

802.1x captive-portal proxy-server-url

Configures Captive Portal to work with a specific proxy server URL used by the client.

802.1x captive-portal proxy-server-url *proxy_url*

Syntax Definitions

proxy_url	The URL address for the users proxy server.

Defaults

N/A.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Changing the Captive Portal proxy server URL value is only necessary if the proxy server URL does not contain any of following in the address:

  www
  http
  https
  proxy

- When using a proxy server with Microsoft's Internet Explorer browser, select the "bypass proxy for local address" option.
- When using a proxy server with the Firefox or Netscape browsers, add the name "captive-portal" to the proxy exception list.
- To remove the configured proxy server URL, specify a null value ("") with this command.

Examples

```
-> 802.1x captive-portal proxy-server-url ind.platform.fr
-> 802.1x captive-portal proxy-server-url ""
```

Release History

Release 6.3.4; command was introduced.

Related Commands

show 802.1x captive-portal configuration	Displays the global Captive Portal configuration for the switch.

MIB Objects

```
alaDot1xCportalConfig
   alaDot1xCPortalProxyURL
```

802.1x captive-portal proxy-server-port

Configures Captive Portal to work with a specific proxy server port.

802.1x captive-portal proxy-server-port *proxy_port*

802.1x captive-portal no proxy-server-port *proxy_port*

Syntax Definitions

proxy_port	The configured port for the proxy server. Valid range is between 1024-49151.

Defaults

N/A.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- This command is only necessary if the port required is not 80 or 8080.

Examples

```
-> 802.1x captive-portal proxy-server-port 1200
-> 802.1x captive-portal no proxy-server-port
```

Release History

Release 6.4.4; command was introduced.

Related Commands

show 802.1x captive-portal configuration	Displays the global Captive Portal configuration for the switch.

MIB Objects

```
alaDot1xCportalConfig
   alaDot1xCPortalProxyPort
```

802.1x captive-portal dns-keyword-list

Configures a list of up to four DNS strings (keywords) that are used to identify DNS packets to which Captive Portal will accept and reply.

802.1x captive-portal dns-keyword-list {*keyword1* **[***keyword2***] [***keyword3***] [***keyword4***]}**

802.1x captive-portal no dns-keyword-list

Syntax Definitions

keyword	The DNS string that Captive Portal will look for in DNS packets. Up to four strings are supported. Each string may contain up to 63 characters.

Defaults

By default, Captive Portal replies to DNS packets containing the following pre-defined DNS strings:

www	**captive-portal**
http	**go.microsoft**
proxy	**mozilla**
wpad	

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The DNS strings configured with this command are added to the list of the pre-defined DNS strings, as shown above. Note that the pre-defined strings are not configurable and will always remain on the list.
- Use the **no** form of this command to remove all the user-defined keywords from the DNS keyword list.
- Any DNS packets received that do not contain the specified DNS strings (pre-defined or user-defined) are dropped.
- Up to four keywords are configurable. Each time this command is used, the user-defined keyword strings are overwritten with the new strings. For example, if the DNS string list contains four user-defined strings, the next time this command is used and only two strings are specified, the four existing strings are removed and only the two new strings are added to the list.

Examples

```
-> 802.1x captive-portal dns-keyword-list univ.intranet.jp
-> 802.1x captive-portal dns-keyword-list univ.intranet1.jp univ.intranet2.jp
-> 802.1x captive-portal dns-keyword-list univ.intranet1.jp univ.intranet2.jp
univ.intrante3.jp univ.intranet4.jp
```

Release History

Release 6.4.3; command was introduced.

Related Commands

show 802.1x captive-portal configuration	Displays the global Captive Portal configuration for the switch.

MIB Objects

```
alaDot1xCportalConfig
   alaDot1xCPortalDnsKeyword1
   alaDot1xCPortalDnsKeyword2
   alaDot1xCPortalDnsKeyword3
   alaDot1xCPortalDnsKeyword4
```

802.1x captive-portal success-redirect-url

Configures Captive Portal to redirect the user to a specific site upon successful authentication. This command specifies the URL of an HTTP site where a Java script is defined that specifies the actual destination URL.

802.1x captive-portal success-redirect-url *redirect_url*

802.1x captive-portal no success-redirect-url

Syntax Definitions

redirect_url	The internal HTTP server URL, up to 63 characters, for the redirect Java script (for example, **http://test-cp.com/success.html**).

Defaults

No success redirect URL is configured.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a success redirect URL configuration.
- Make sure the HTTP server URL and Java script exist and are reachable by the user during the authentication phase.
- A Java script is only needed to redirect a user to a website outside of the network; a script is not needed to redirect users to an intranet site.
- After the user attempts to authenticate through the Captive Portal login page, the Captive Portal status page displays and attempts to run the Java script that is located at the URL site specified with this command.
- If the redirect URL is not configured or is invalid, the Captive Portal status page remains open and displays an error message regarding the attempted redirection.

Examples

The following command example configures the success URL to point to the **success.html** Java script on the **test-cp.com** HTTP server.

```
-> 802.1x captive-portal success-redirect-url http://test-cp.com/success.html
```

The following is an example Java script (**success.html**) in which the “TARGET” field specifies the actual URL to which the user is redirected.

```
<html>
<head> <meta http-equiv="expires" content="Tue, 20 Aug 1996 14:25:47 GMT">
<meta http-equiv=Pragma content=no-cache>
<meta http-equiv=cache-control content=no-cache,no-store,must-revalidate,proxy-
```

```
revalidate>
</head>
<body>
<script type="text/javascript">
    var TARGET = "http://www.google.com";
    top.location = TARGET;
</script>
</body>
```

Release History

Release 6.4.3; command was introduced.

Related Commands

show 802.1x captive-portal configuration	Displays the global Captive Portal configuration for the switch.
802.1x captive-portal fail-redirect-url	Configures Captive Portal to redirect the user to a specific site if authentication fails.

MIB Objects

```
alaDot1xCportalConfig
   alaDot1xCPortalPostAuthSuccessRedirectURL
```

802.1x captive-portal fail-redirect-url

Configures Captive Portal to redirect the user to a specific site if authentication fails (user login is invalid or user bypasses authentication). This command specifies the URL of an HTTP server where a Java script is defined that specifies the actual destination URL.

802.1x captive-portal fail-redirect-url *redirect_url*

802.1x captive-portal no fail-redirect-url

Syntax Definitions

redirect_url	The internal HTTP server URL, up to 63 characters, for the redirect Java script (for example, **http://test-cp.com/fail.html**).

Defaults

No fail redirect URL is configured.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a fail redirect URL configuration.
- Make sure the HTTP server URL and Java script exist and are reachable by the user during the authentication phase.
- A Java script is only needed to redirect a user to a website outside of the network; a script is not needed to redirect users to an intranet site.
- After the user attempts to authenticate through the Captive Portal login page, the Captive Portal status page displays and attempts to run the Java script that is located at the URL site specified with this command.
- If the redirect URL is not configured or is invalid, the Captive Portal status page remains open and displays an error message regarding the attempted redirection.

Examples

The following command example configures the fail URL to point to the **fail.html** Java script on the **test-cp.com** HTTP server.

```
-> 802.1x captive-portal fail-redirect-url http://test-cp.com/fail.html
```

The following is an example Java script (named **fail.html**) in which the “TARGET” field specifies the actual URL to which the user is redirected:

```
<html>
<head> <meta http-equiv="expires" content="Tue, 20 Aug 1996 14:25:47 GMT">
<meta http-equiv=Pragma content=no-cache>
<meta http-equiv=cache-control content=no-cache,no-store,must-revalidate,proxy-
revalidate>
</head>
```

```
<body>
<script type="text/javascript">
    var TARGET = "http://www.mycompany.com";
    top.location = TARGET;
</script>
</body>
```

Release History

Release 6.4.3; command was introduced.

Related Commands

show 802.1x captive-portal configuration	Displays the global Captive Portal configuration for the switch.
802.1x captive-portal success-redirect-url	Configures Captive Portal to redirect the user to a specific site upon successful authentication.

MIB Objects

```
alaDot1xCportalConfig
   alaDot1xCPortalPostAuthFailRedirectURL
```

802.1x auth-server-down

Enables or disables the authentication server down classification policy.

802.1x auth-server-down {enable | disable}

Syntax Definitions

enable	Enables the auth-server-down policy.
disable	Disables the auth-server-down policy.

Defaults

By default, authentication server down policy is disabled.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

This command is global and applies to all 802.1x ports on the switch.

Examples

```
-> 802.1x auth-server-down enable
-> 802.1x auth-server-down disable
```

Release History

Release 6.4.2; command was introduced.

Related Commands

show 802.1x auth-server-down	Displays the configured authentication server down classification policy.

MIB Objects

```
alaDot1xAuthSvrTimeoutStatus
```

802.1x auth-server-down policy

Configures the policy for classifying devices attempting to authenticate when the RADIUS servers are not reachable.

802.1x auth-server-down policy {user-network-profile *profile_name* **| block}**

Syntax Definitions

profile_name	The name of an existing User Network Profile (UNP) to use for device classification.
block	Blocks device access on the 802.1x port.

Defaults

By default, this policy is configured to block access to such devices and is disabled for the switch.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **user-network-profile** parameter to classify device traffic into a specific profile when the RADIUS server is down.
- Use the **block** parameter to block device traffic on the 802.1x port when the RADIUS server is down.
- This command applies to all 802.1x-enabled ports on the switch.
- When device authentication fails due to an unreachable RADIUS server, an event message is sent to the switch logging utility (swlog). See the “Switch Logging Command” chapter for more information.

Examples

```
-> 802.1x auth-server-down policy user-network-profile unp1
-> 802.1x auth-server-down policy block
```

Release History

Release 6.4.2; command was introduced.

Related Commands

802.1x auth-server-down	Enables or disables the authentication server down policy.
802.1x auth-server-down re-authperiod	Configures the amount of time to wait before re-authentication is attempted for devices classified by the server down policy.
show 802.1x auth-server-down	Displays the configured authentication server down policy.

MIB Objects

```
alaDot1xAuthServerTimeoutPolicy
```

802.1x auth-server-down re-authperiod

Configures the amount of time to wait before re-authentication is attempted for devices that were classified by the authentication server down policy.

802.1x auth-server-down re-authperiod {*value***}**

Syntax Definitions

value	The value of re-authentication timer. The range is 1 to 9999 seconds.

Defaults

parameter	default
value	30

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- This timer only applies to devices that were classified by the authentication server down policy. This policy classifies devices whenever RADIUS servers become unreachable.
- This command sets the time interval for all 802.1x-enabled ports on the switch.

Examples

```
-> 802.1x auth-server-down re-authperiod 500
```

Release History

Release 6.4.2; command was introduced.

Related Commands

802.1x auth-server-down policy	Configures the authentication server down policy.
show 802.1x auth-server-down	Displays the configured re-authentication time interval value.

MIB Objects

```
alaDot1xAuthSvrTimeoutReAuthPeriod
```

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 6400, 6850E, 6855, 9000E

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
  Captive Portal Session Limit (hrs)  = 12
  Captive Portal Login Retry Count    = 3
  Supplicant Bypass                   = enable
  Supplicant Bypass allow-eap Branch  = pass,
  Captive Portal Inactivity Logout   = disable
  Kerberos Snooping                  = Enabled
```

output definitions

direction	Whether the port is configured for control on bidirectional traffic or incoming traffic only (**both** or **in**). Configured through the **802.1x** command.
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**.
port-control	The value of the port control parameter for the port (**auto**, **force-authorized**, or **force-unauthorized**). Configured 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. Configured through the **802.1x** command.
tx-period	The time before an EAP Request Identity will be transmitted. The range is 1 to 65535 seconds. Configured through the **802.1x** command.
supp-timeout	The number of seconds before the switch will time out an 802.1x user who is attempting to authenticate. Configured through the **802.1x** command.
server-timeout	The timeout for the authentication server for authentication attempts. Configured for the switch port through the **802.1x** command. However, 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. Configured through the **802.1x** command.
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. Configured through the **802.1x** command.
reauthentication	Whether or not the port will be re-authenticated after the re-authperiod expires. Configured through the **802.1x** command.
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.
Captive Portal Session Limit (hrs)	The amount of time, in hours, that a Captive Portal session can remain active. Configured through the **802.1x captive-portal session-limit** command.
Captive Portal Login Retry Count	The number of login attempts allowed before the Captive Portal fail policy is applied to the device. Configured through the **802.1x captive-portal retry-count** command.
Supplicant Bypass	The status of 802.1x authentication bypass (**enable** or **disable**). Configured through the **802.1x supplicant bypass** command.

output definitions (continued)

Supplicant Bypass allow-eap Branch	Specifies the conditions under which subsequent 802.1x authentication is attempted based on the outcome of the initial MAC authentication (**pass**, **fail**, **noauth**, or **none**). Configured through the **802.1x non-supplicant allow-eap** command. This value only applies when **Supplicant Bypass** is set to **enable**.
Captive Portal Inactivity Logout	Whether or not a user MAC address is removed from the Captive Portal user table when the same MAC ages out of the switch MAC address table due to inactivity (**enabled** or **disabled**). Configured through the **802.1x captive-portal inactivity-logout** command.
Kerberos Snooping	Kerberos Snooping information is displayed only when Kerberos snooping configurations are activated (**Enabled** or **Disabled**).

Release History

Release 6.1; command was introduced.
Release 6.3.4; Captive Portal fields added.
Release 6.4.4; **Supplicant Bypass**, **Supplicant Bypass allow-eap Branch**, **Captive Portal Inactivity Logout** fields added.

Related Commands

show 802.1x users	Displays information about users connected to the 802.1x port..
show 802.1x statistics	Displays 802.1x port statistics..

MIB Objects

```
dot1xAuthConfigTable
   dot1xAuthAdminControlledDirections
   dot1xAuthOperControlledDirections
   dot1xAuthAuthControlledPortControl
   dot1xAuthQuietPeriod
   dot1xAuthTxPeriod
   dot1xAuthSuppTimeout
   dot1xAuthServerTimeout
   dot1xAuthMaxReq
   dot1xAuthReAuthPeriod
   dot1xAuthReAuthEnabled
   alaDot1xSuppPollingCnt
   alaDot1xCPortalSessionLimit
   alaDot1xCPortalRetryCnt
   alaDot1xSupplicantBypass
   alaDot1xSBAllowEAP
   alaDot1xCPortalInactivityLogout
```

show 802.1x users

Displays a list of all users for one or more 802.1X ports.

show 802.1x users [*slot/port***] [unp | detail]**

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.
unp	Lists all the users associated with user network profiles.
detail	Lists additional details.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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  Classification Auth         Auth Last Successful User
Port Address          State  Policy      Failure Reason Retry Count Auth Time Name
-------+--------------------+------------+----------------+-------------------
04/05 00:13:72:ae:f3:1c Connecting AUTHENTICATION FAILURE 1             -     user

->show 802.1x users 4/5

Slot MAC               Port     Classification Auth   Auth Last Successful User
Port Address          State      Policy  Failure Reason Retry Count Auth Time Name
-------+--------------------+------------+----------------+-------------------
04/05 00:13:72:ae:f3:1c Authenticated Basic-Dft VLAN      -     0   SUN FEB 10
```

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** • **Authenticated-L** • **Authenticated-T -** Supplicant learned according to the auth-server-down policy • **Aborting** • **Held** • **Force-Authenticated** • **Force-Unauthenticated**
Classification Policy	The 802.1x device classification policy that was applied to the device.
User Name	The user name that is used for authentication.
Auth Failure Reason	Reason for authentication failure as “SERVER UNREACHABLE” or “AUTHENTICATION FAILURE”.
Auth Retry Count	Number of times the switch retransmits a request for authentication information to the 802.1x user.
Last Successful Auth Time	Latest successful authentication time. If the port was not authenticated before, then “**-**” is displayed.

Release History

Release 6.1; command was introduced.
Release 6.1.2; **Classification Policy** field added.
Release 6.4.4; **unp** and **detail** parameters added.
Release 6.4.5; **Auth Failure Reason, Auth Retry Count** and **Last Successful Auth Time** fields added.

Related Commands

802.1x	Configures 802.1X parameters on a particular slot/port.

MIB Objects

```
alaDot1xPortTable
   alaDot1xPortSlotNumber
   alaDot1xPortPortNumber
   alaDot1xPortMACAddress
   alaDot1xPortUserName
   alaDot1xPortState
   alaDot1xHicEnabledMAC
   alaDot1xNonSupplicantHicEnabledMAC
   alaDot1xHicFlag

alaDot1xAuthPolicyTable
   alaDot1xSuppPolicy
   alaDot1xNonSuppPolicy
```

show 802.1x statistics

Displays statistics for 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 6400, 6850E, 6855, 9000E

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 (continued)

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 6.1; command was introduced.

Related Commands

802.1x captive-portal address 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 6400, 6850E, 6855, 9000E

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:
       pass: group-mobility, default-vlan (default)
       fail: block (default)
 Non-Supplicant:
    block (default)
 Captive Portal:
    authentication:
       pass: default-vlan (default)
       fail: block (default)
Device classification policies on 802.1x port 2/48
 Supplicant:
    authentication:
       pass: vlan 500, block
       fail: block (default)
 Non-Supplicant:
    block (default)
 Captive Portal:
    authentication:
       pass: default-vlan (default)
       fail: block (default)
```

```
-> show 802.1x device classification policies 2/48
Device classification policies on 802.1x port 2/48
 Supplicant:
    authentication:
       pass: vlan 500, block
       fail: block (default)
 Non-Supplicant:
    block (default)
 Captive Portal:
    authentication:
       pass: default-vlan (default)
       fail: block (default)
```

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.
Captive Portal	Displays the Captive Portal device classification policy configured for the 802.1x port.

Release History

Release 6.1.2; command was introduced.

Related Commands

802.1x captive-portal address	Displays information about ports configured for 802.1X.
show 802.1x non-supplicant	Displays a list of all non-supplicants learned on all 802.1x ports.

MIB Objects

```
alaDot1xAuthPolicyTable
   alaDot1xSuppPolicy
   alaDot1xNonSuppPolicy
```

show 802.1x non-supplicant

Displays a list of all non-802.1x supplicants learned on one or more 802.1x ports.

show 802.1x non-supplicant [*slot/port***] [unp | detail]**

Syntax Definitions

slot/port	The slot/port number of the 802.1x port for which you want to display information.
unp	Lists all the users associated with user network profiles.
detail	Lists additional details .

Defaults

All non-supplicants associated with all 802.1X ports are displayed.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the *slot/port* parameter to display a list of non-supplicants learned on a specific 802.1x port.

Examples

```
->show 802.1x non-supplicant

Slot  MAC               MAC Authent      Classification  Vlan    Dynamic
Port  Address           Status           Policy         Learned    UNP
-----+-----------------+----------------+--------------+--------+----------
03/3  00:61:22:15:22:33 N/A              Basic-UNP-Usr   Cfg 20   Enabled
03/3  00:61:22:44:75:66 N/A              Basic-UNP-Usr   Cfg 20   Enabled
03/11 00:00:39:47:4f:0c Failed           Vlan ID         1001     Disabled
03/11 00:00:39:c9:5a:0c Authenticated    Group Mobility  12       Disabled
03/11 00:b0:d0:52:47:35 Authenticated    Group Mobility  12       Disabled
03/11 00:c0:4f:0e:70:68 Authenticated    MAC Authent     14       Disabled


->show 802.1x non-supplicant 3/3

Slot  MAC               MAC Authent      Classification  Vlan     Dynamic
Port  Address           Status           Policy         Learned     UNP
-----+-----------------+----------------+--------------+--------+----------
03/3  00:61:22:15:22:33 N/A              Basic-UNP-Usr   Cfg 20   Enabled
03/3  00:61:22:44:75:66 N/A              Basic-UNP-Usr   Cfg 20   Enabled
```

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.
MAC Authent Status	Indicates whether or not MAC authentication failed. • **Success -** Non-supplicant learned according to the Success policy. • **Failed -** Non-supplicant learned according to the Failed policy • **Fail (timeout) -** Non-Supplicant learned according to the auth-server-down policy.
Classification Policy	The 802.1x device classification policy that was applied to the device.
VLAN Learned	The VLAN ID of the VLAN in which the source MAC address of the non-802.1x device was learned.
Dynamic UNP	The status of dynamic UNP; enabled or disabled.

Release History

Release 6.1; command was introduced.
Release 6.1.2; **Authentication Status** and **Classification Policy** columns added.
Release 6.4.4; **unp** and **detail** parameters added.

Related Commands

802.1x captive-portal address	Displays information about ports configured for 802.1X.
show 802.1x device classification policies	Displays device classification policies configured for an 802.1x port.

MIB Objects

```
alaDot1xPortTable
   alaDot1xNonSupplicantSlotNum
   alaDot1xNonSupplicantPortNum
   alaDot1xNonSupplicantMACAddress
   alaDot1xNonSupplicantVlanID
   alaDot1xHicEnabledMAC
   alaDot1xNonSupplicantHicEnabledMAC
   alaDot1xHicFlag
```

show 802.1x rate-limit

Displays current rate limit configuration on 8021x enabled ports. If a port is not specified, then current rate limit configuration for all 8021x ports in switch is displayed.

show 802.1x rate-limit [*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 6400, 6850E, 6855, 9000E

Usage Guidelines

- In the show output, **Type** field shows "QOS", "UNP" or "-". If the current bandwidth set by the user classified under UNP, then it shows as "UNP". If the current bandwidth on port is set by using the “qos port” command, then it shows "QOS". By default, if no QoS or UNP are used on 8021x port, then it shows "-", which denotes no limitation currently configured on the port.
- **Ingress/Egress BW UNP-ProfileName** field displays the UNP profile name under which bandwidth has been applied on the port. This is applicable only for clients getting classified under UNP. For the rest, "N/A" is displayed.

Examples

```
-> show 802.1x rate-limit

Slot    Max                Ingress  BW       Max                 Egress   BW
Port  Ingress-BW  Type   UNP-ProfileName   Egress-BW   Type     UNP-ProfileName
-----+----------+------+-----------------+-----------+-------+---------------
1/10   50.0M      UNP       50down50up      50.0M      UNP      50down50up
1/25   10.0M      UNP       100down10up     100M       UNP      100down10up
```

output definitions

Slot	The slot number of the 802.1X port.
Port	The 802.1X port number.
Max Ingress-BW	Ingress bandwidth configured on the 8021X port.
Type	Application under which current maximum ingress bandwidth is set.
Ingress BW UNP-Profile Name	UNP profile name under which current ingress bandwidth is set.
Max Egress-BW	Egress bandwidth configured on the 8021X port.

output definitions (continued)

Type	Application under which current maximum egress bandwidth is set.
Egress BW UNP-Profile Name	UNP profile name under which current egress bandwidth is set.

Release History

Release 6.4.5; command introduced.

Related Commands

aaa user-network-profile	Configures a UNP that is used to provide role-based access to the switch.

MIB Objects

```
alaDot1xCrlUnpTable
   alaDot1xCrlSlotNumber
   alaDot1xCrlPortNumber
   alaDot1xCrlIngBw
   alaDot1xCrlIngTypeFlag
   alaDot1xCrlIngProfile
   alaDot1xCrlEgrBw
   alaDot1xCrlEgrTypeFlag
   alaDot1xCrlEgrProfile
```

show 802.1x auth-server-down

Displays the configured authentication server down classification policy.

show 802.1x auth-server-down

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show 802.1x auth-server-down

Status                        = Enabled
Re-authentication Interval    = 30 seconds
Classification policy         = block

-> show 802.1x auth-server-down

Status                        = Disabled
Re-authentication Interval    = 30 seconds
Classification policy         = block
```

output definitions

Status	Authentication server down policy status: **Enabled** or **Disabled**
Re-authentication Interval	The amount of time for the device to authenticate again with the RADIUS server when the device is classified according to the Auth-server-policy.
Classification Policy	The 802.1x device classification policy that was applied to the device.

Release History

Release 6.4.2; command was introduced.

Related Commands

802.1x auth-server-down	Enables or disables the authentication server down policy.
802.1x auth-server-down re-authperiod	Configures the re-authentication time for the device to authenticate again with the RADIUS server when it is classified according to the Auth-server-down policy
802.1x auth-server-down policy	Configures the policy for classifying the device when the authentication server is not reachable

MIB Objects

```
alaDot1xAuthSvrTimeout
   alaDot1xAuthSvrTimeoutStatus
   alaDot1xAuthSvrTimeoutReAuthPeriod
   alaDot1xAuthServerTimeoutPolicy
```

show 802.1x captive-portal configuration

Displays the global Captive Portal configuration for the switch.

show 802.1x captive-portal configuration

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

This command displays the Captive Portal IP address and the proxy server URL.

Examples

```
-> show 802.1x captive-portal configuration

Captive Portal Global Configuration:

  Captive Portal IP address = 10.123.0.1

  Proxy Server URL = proxy

  Proxy Server Port = 8080

  Redirect URL Key string = captive-portal

  Post Auth Success Redirect URL = http://test-cp.com/fail.html

  Post Auth Fail Redirect URL = http://test-cp.com/success.html

  DNS Keyword 1 = univ.intranet1.jp

  DNS Keyword 2 = univ.intranet2.jp

  DNS Keyword 3 = univ.interanet3.jp

  DNS Keyword 4 = univ.intranet4.jp
```

output definitions

Captive Portal IP address	The Captive Portal IP address. Configured through the **802.1x captive-portal address** command.
Proxy Server URL	The website URL for the client proxy web server. Configured through the **802.1x captive-portal proxy-server-url** command.
Proxy Server Port	The port number for the configured proxy. Configured through the **802.1x captive-portal proxy-server-port** command.
Post Auth Success Redirect URL	The internal HTTP server URL for the intermediate Java script used to redirect the user upon successful authentication. Configured through the **802.1x captive-portal success-redirect-url** command.
Redirect URL String	The name of the redirect URL to be used with a public certificate. Configured through the **802.1x captive-portal name** command.
Post Auth Fail Redirect URL	The internal HTTP server URL for the intermediate Java script used to redirect the user when authentication fails. Configured through the **802.1x captive-portal fail-redirect-url** command.
DNS Keyword	A user-defined DNS string. Captive Portal replies to DNS packets that contain this string. Configured through the **802.1x captive-portal proxy-server-port** command.

Release History

Release 6.3.4; command was introduced.
Release 6.4.3; **Post Auth Success Redirect URL**, **Post Auth Fail Redirect URL**, and **DNS Keyword** fields added.
Release 6.4.4; **Proxy Server Port** and **Redirect URL String** fields added.

Related Commands

show 802.1x device classification policies	Displays device classification policies configured for 802.1x ports.

MIB Objects

```
alaDot1xCportalConfig
   alaDot1xCPortalIpAddress
   alaDot1xCPortalProxyURL
   alaDot1xCPortalProxyPort
   alaDot1xCPortalRedirectString
   alaDot1xCPortalPostAuthSuccessRedirectURL
   alaDot1xCPortalPostAuthFailRedirectURL
   alaDot1xCPortalDnsKeyword1
   alaDot1xCPortalDnsKeyword2
   alaDot1xCPortalDnsKeyword3
   alaDot1xCPortalDnsKeyword4
```

41 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, TACACS+, or LDAP server.
- **Authenticated Switch Access**. Authenticates users into the switch to manage the switch. User information is stored on a RADIUS, TACACS+, 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.

MIB information for the AAA commands is as follows:

Filename: alcatelIND1AAA.mib
Module: ALCATEL-IND1-AAA-MIB

Filename: alcatelIND1Dot1x.mib
Module: ALCATEL-IND1-DOT1X-MIB

A summary of the available commands is listed here:

Authentication servers	**aaa radius-server** **aaa radius agent preferred** **aaa tacacs+-server** **aaa ldap-server** **aaa ace-server clear** **system fips** **aaa test-radius-server** **show aaa server** **show system fips-status**
Authenticated VLANs	**aaa authentication vlan single-mode** **aaa authentication vlan multiple-mode** **aaa vlan no** **aaa accounting mac** **aaa avlan dns** **aaa avlan default dhcp** **aaa accounting command** **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 tacacs command-authorization** **aaa accounting session** **aaa accounting session-id** **aaa accounting command** **show aaa authentication** **show aaa accounting**
802.1X Port-Based Network Access Control	**aaa authentication 802.1x** **aaa authentication mac** **aaa certificate-password** **aaa accounting 802.1x** **aaa accounting mac** **show aaa authentication mac** **show aaa accounting 802.1x** **show aaa accounting mac**
Local User Database and Partitioned Management	**user** **password** **user password-size min** **user password-expiration** **show user** **show aaa hic server**

Password Policy	**user password-size min** **user password-expiration** **user password-policy cannot-contain-username** **user password-policy min-uppercase** **user password-policy min-lowercase** **user password-policy min-digit** **user password-policy min-nonalpha** **user password-history** **user password-size min** **user password-min-age** **user password-expiration** **show user** **show user password-size** **show user password-expiration** **show user password-policy**
User Lockout Settings	**user lockout-window** **user lockout-threshold** **user lockout-duration** **user lockout unlock** **show user** **show user lockout-setting**
Administrative User Logout	**aaa admin-logout**
End-user Profiles	**user** **end-user profile** **end-user profile port-list** **end-user profile vlan-range** **show end-user profile**
User Network Profiles	**aaa user-network-profile** **aaa classification-rule mac-address** **aaa classification-rule mac-address-range** **aaa classification-rule ip-address** **show aaa user-network-profile** **show aaa classification-rule**
Host Integrity Check	**aaa hic server-name** **aaa hic redundancy background-poll-interval** **aaa hic server-failure mode** **aaa hic server-failure policy user-network-profile change** **aaa hic allowed-name** **aaa hic** **aaa hic web-agent-url** **aaa hic custom-proxy-port** **show aaa hic** **show aaa hic host** **show aaa hic server** **show aaa hic server-failure policy** **show aaa hic allowed**

User Authentication Status	**show aaa-device all-users** **show aaa-device supplicant-users** **show aaa-device non-supplicant-users** **show aaa-device captive-portal-users**
Kerberos Snooping commands	**802.1x kerberos** **aaa kerberos mac-move** **aaa kerberos inactivity-timer** **aaa kerberos ip-address** **aaa kerberos server-timeout** **aaa kerberos authentication-pass policy-list-name** **aaa kerberos authentication-pass domain** **show aaa kerberos configuration** **show aaa kerberos port** **show aaa kerberos users** **show aaa kerberos statistics** **show aaa kerberos port statistics** **clear aaa kerberos statistics** **clear aaa kerberos port statistics**

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-name* **[host {***hostname* | *ip_address***} [***hostname2* | *ip_address2***]] [key** *secret***] [retransmit** *retries***] [timeout** *seconds***] [auth-port** *auth_port***] [acct-port** *acct_port***] [vrf-name** *vrf_name***]**

no aaa radius server *server-name*

Syntax Definitions

server-name	The name of the RADIUS server. This name is used in the related CLI commands to refer to the 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 text string shared secret known to the switch and the server, but which is not sent over the network. It can be any text or hexadecimal string but MUST match the secret configured on the server. The secret is case-sensitive. It is 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.
vrf_name	Specifies the VRF instance to which the RADIUS server belongs.

Defaults

parameter	default
retries	3
seconds	2
auth_port	1812
acct_port	1813

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E
OmniSwitch 9000E, 6855-U24X; **vrf-name** parameter supported.

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.
- Configuring multiple RADIUS servers is possible, but all RADIUS servers must belong to the same VRF instance.
- If the **vrf-name** parameter is not specified, the default VRF instance is assigned.
- Use the **no** form of the command to remove a RADIUS server from the configuration. Only one server may be removed at a time. Note that if any Authenticated Switch Access (such as telnet) is configured for the server, remove the switch access configuration first before attempting to remove the server.
- To move the RADIUS servers to a different VRF instance, first remove each server from the current VRF instance and then add each server to the new VRF instance.

Examples

```
-> aaa radius-server pubs2 host 10.10.2.1 key wwwtoe timeout 5 vrf-name
Management-vrf
-> no aaa radius-server pubs2
```

Release History

Release 6.1; command was introduced.
Release 6.4.2; **vrf-name** parameter 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 mac	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
   aaasTimeout
   aaasRadAuthPort
   aaasRadAcctPort
   aaasVrfName
```

aaa radius agent preferred

Configures the source IP address field of the Radius packet.

aaa radius agent preferred {default | no-loopback | *ip_address***}**

no aaa radius agent preferred

Syntax Definitions

default	The Loopback0 address, if configured, will be used for the source IP address field. If no Loopback0 is configured, the first IP address on the switch will be used.
no-loopback	The Loopback0 address should not be used for the source IP address field and the first available IP address on the switch should be used for this field.
ip_address	The IP address to be used in the source IP field.

Defaults

By default, the radius agent setting is set to the **default** parameter.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- When configuring a specific IP address, that address must already exist on the switch.
- Use the **no** form of the command to clear a specific IP address and change the behavior back to **default**.

Examples

```
-> aaa radius agent preferred 192.168.10.1
-> aaa radius agent preferred no-loopback
-> aaa radius agent preferred default
```

Release History

Release 6.3.4; command was introduced.
Release 6.4.3; command was deprecated, use **ip managed-interface.**

Related Commands

show aaa server	Displays information about AAA servers.

MIB Objects

```
radiusAgentVal
ipedrUsrConfiguredIPaaasRetries
```

aaa tacacs+-server

Configures or modifies a TACACS+ server for Authenticated VLANs or Authenticated Switch Access.

aaa tacacs+-server *server-name* **[host {***hostname* **|** *ip_address***} {***hostname2* **|** *ip_address2***}] [key** *secret***][timeout** *seconds***] [port** *port***]**

no aaa tacacs+-server *server-name*

Syntax Definitions

server-name	The name of the TACACS+ server.
hostname	The host name (DNS name) of the primary TACACS+ server. The host name or IP address is required when creating a server.
ip_address	The IP address of the primary TACACS+ server. An IP address or host name is required when creating a server.
hostname2	The host name (DNS name) of an optional backup TACACS+ server.
ip_address2	The IP address of an optional backup TACACS+ 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.
seconds	The timeout for server replies to authentication requests.
port	The port number for the primary TACACS+ server.

Defaults

parameter	default
seconds	2
port	49

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of the command to remove a TACACS+ server from the configuration. Only one server may be deleted at a time. Note that if any Authenticated Switch Access (such as telnet) is configured for the server, remove the switch access configuration first before attempting to remove the server.
- A host name (or IP address) and a secret are required when configuring a server.
- The server and the backup server must both be TACACS+ servers.

Examples

```
-> aaa tacacs+-server tpub host 10.10.2.2 key otna timeout 10
-> no aaa tacacs+-server tpub
```

Release History

Release 6.1.3; 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 mac	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
   aaasName
   aaasProtocol
   aaasHostName
   aaasIpAddress
   aaasHostName2
   aaasIpAddress2
   aaasTacacsKey
   aaasTimout
   aaasTacacsPort
```

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***}]] [***port***] [dn** *dn_name***] [password** *super_password***] [base** *search_base***] [type** *server_type***] [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.
server-type	The different directory server types used in LDAP Authentication: **Generic** = Generic Schema **Netscape** = Netscape Directory Server **Novell** = Novell NDS **Sun** = Sun Directory Services **Microsoft** = Microsoft AD.
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 6400, 6850E, 6855, 9000E

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. Note that if any Authenticated Switch Access (such as telnet) is configured for the server, remove the switch access configuration first before attempting to remove the server.
- The port number configured on the switch must match the port number configured for the server.
- When communicating with the LDAP server, the Loopback0 address is used if configured, otherwise the VLAN's IP address is used.

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 6.1; 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 mac	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
   aaasTimout
   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 shared secret between the switch and the ACE/Server cannot be configured on the switch but can be cleared on the switch.

aaa ace-server *server-name* **clear**

Syntax Definitions

server-name	The name of the ACE Server. Usually only one ACE server is configured for a switch.

Defaults

The default server name is provided as ACE

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Clear the ACE secret on the switch if the server and the switch get out of sync. 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 6.1; 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
```

system fips

Enable or disable the FIPS mode on the switch.

system fips [*enable* | *disable***]**

Syntax Definitions

enable FIPS mode is enabled.

disable FIPS mode is disabled.

Defaults

parameter	default
enable | *disable*	*disable*

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- FIPS mode is disabled by default.
- Enabling or disabling FIPS mode takes effect only after a switch reboot. The FIPS mode configuration is persistent across reboots.
- Deletion of *fips.conf* file under */flash/switch* directory will automatically disable the FIPS configuration.
- When FIPS mode is disabled, all other existing cryptographic algorithms will be supported.
- A FIPS supported client is required to access the AOS in FIPS enabled mode. For example, Absolute Telnet.
- Other insecure management interfaces like Telnet/ FTP has to be manually disabled, after FIPS mode is enabled in order to achieve a completely secure device.

Examples

```
->system fips enable
/* the output of above CLI */
WARNING: FIPS mode has been enabled. System reboot required for the changes to take
effect.

->system fips disable
/* Output of above CLI */
WARNING: FIPS mode has been disabled. System reboot required for the changes to
take effect.
```

Release History

Release 6.4.5; command introduced.

Related Commands

show system fips-status	Show the Configured and Running status of the FIPS mode on the Switch.

MIB Objects

```
systemServicesFipsEnable
```

show system fips-status

Shows the configured and running status of the FIPS mode on the Switch.

show system fips-status

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 9000E, 6850E, 6855, 6400

Usage Guidelines

- Status of the FIPS mode can be checked using the **show system fips-status** command
- The **show system fips-status** is the only command that can be used to view FIPS mode status. The **showconfiguration snaphot** does not display the FIPS status.

Examples

```
-> show system fips-status

FIPS mode Configured status: Enabled
FIPS mode Running status: Disabled
```

Release History

Release 6.4.5; command introduced.

Related Commands

system fips	Enable or disable the FIPS mode on the switch.

MIB Objects

```
systemServicesFipsStatus
systemServicesFipsEnable
```

aaa test-radius-server

RADIUS test tool allows the user to test the RADIUS server reachability from OmniSwitch. Use this command to start the authentication or accounting test for the specified user name and password.

aaa test-radius-server *server-name* **type {authentication user** *user-name* **password** *password* **[method {MD5 | PAP}] | accounting user** *user-name***}**

Syntax Definitions

server-name	RADIUS server name for which test has been configured.
authentication | accounting	Type of test to run.
user-name	User name configured on the server.
password	Password for the given user name.
MD5|PAP	Authentication method for the test.

Defaults

By default, MD5 is used as the authentication method.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- RADIUS server must be configured on the switch to test the tool.
- The switch must have the following RADIUS server configuration before starting the test tool: RADIUS server name, acct-port, auth-port, secret key, retransmit count, and timeout. See **aaa test-radius-server** command for more information on RADIUS server configuration.
- Supports multiple sessions (console, telnet, SSH) to test multiple RADIUS servers.
- The CLI of the user session (console, telnet, SSH) goes in the blocking state when the test is started. In the blocking state, no other command (CLI) is accepted. The blocking state of the CLI prompt of the switch can be terminated by pressing any key.
- Two IP addresses is configurable for a RADIUS server. When the test starts, the requests are sent to the first address. When all the requests to the first address time out, then the requests are sent to the second address.

Examples

```
-> aaa test-radius-server rad1 type authentication user admin password switch
method MD5
-> aaa test-radius-server rad2 type authentication user admin password switch
method pap
```

Release History

Release 6.4.5; command 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

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, TACACS+, or LDAP authentication server used for authenticating users through all Authenticated VLANs on the switch. At least one server is required. RADIUS, TACACS+, and LDAP server names are set up through the **aaa radius-server**, **aaa tacacs+-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 *server_name1* 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of the command to disable Authenticated VLANs in single mode.
- The servers may be RADIUS, TACACS+, or LDAP servers. 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, TACACS+, and LDAP servers may each have an additional backup specified through the **aaa radius-server**, **aaa tacacs+-server**, and **aaa ldap-server** commands.

Examples

```
-> aaa authentication vlan single-mode pubs1 pubs2 pubs3
```

Release History

Release 6.1; 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, TACACS+, or LDAP authentication server used for this Authenticated VLAN in multiple mode. At least one server is required. RADIUS, TACACS+, and LDAP server names are set up through the **aaa radius-server**, **aaa tacacs+-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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of the command to remove Authenticated VLANs in multiple mode.
- The servers may be RADIUS, TACACS+, 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, TACACS+, and LDAP servers may each have an additional backup specified through the **aaa radius-server**, **aaa tacacs+-server**, and **aaa ldap-server** commands.

Examples

```
-> aaa authentication vlan multiple-mode 2 pubs1 pubs2
```

Release History

Release 6.1; 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
   aaatvVlan
   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 6400, 6850E, 6855, 9000E

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 6.1; 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
   aaaaMacAddress
```

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] *dns_name*

Syntax Definitions

dns_name	The name of the DNS host.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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, TACACS+, LDAP, ACE/Server, or the local user database. RADIUS, TACACS+, and LDAP server names are set up through the **aaa radius-server**, **aaa tacacs+-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.
- By default, the telnet, ftp, http, and snmp login is disabled
- The default user on the switch is **admin**, and **switch** is the password.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove the Authenticated Switch Access configuration for the specified interface type. If the switch access configuration for an external authentication server is not removed first, attempting to remove the server configuration from the switch will fail.
- The server type may be RADIUS, TACACS+, 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, TACACS+, and LDAP servers may each have an additional backup specified through the **aaa radius-server**, **aaa tacacs+-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 6.1; command was introduced.

Related Commands

aaa radius-server	Configures or modifies a RADIUS server for Authenticated VLANs or Authenticated Switch Access.
aaa tacacs+-server	Configures or modifies a TACAS+ 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
   aaatsInterface
   aaasName
   aaatsName1
   aaatsName2
   aaatsName3
   aaatsName4
   aaatsRowStatus
```

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 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the **aaa authentication** command to set the default servers.

Examples

```
-> aaa authentication telnet default
-> aaa authentication default default
```

Release History

Release 6.1; command was introduced.

Related Commands

aaa radius-server	Configures or modifies a RADIUS server for Authenticated VLANs or Authenticated Switch Access.
aaa tacacs+-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 tacacs command-authorization

Enables or disables command authorization for TACACS server.

aaa tacacs command-authorization {enable | disable}

Syntax Definitions

enable	Enables command authorization for TACACS server.
disable	Disables command authorization for TACACS server.

Defaults

By default, TACACS command-authorization is disabled.

Platforms Supported

OmniSwitch 9000E, 6850E, 6855, 6400

Usage Guidelines

- The TACACS+ server can be programmed to determine specific authorization for CLI commands. When TACACS command authorization is enabled on OmniSwitch, these authorization settings are applied.
- To check whether command authorization configuration is applied, use the **show configuration snapshot** command with **aaa** option.

Examples

```
-> aaa tacacs command-authorization enable
-> aaa tacacs command-authorization disable
```

Release History

Release 6.4.5; command introduced.

Related Commands

aaa tacacs+-server	Configures or modifies a TACACS+ server for Authenticated VLANs or Authenticated Switch Access.
show configuration snapshot	Displays the switch current running configuration for specified feature(s).

MIB Objects

```
aaaServerMIBTable
   aaaTacacsServerCmdAuthorization
```

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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to disable 802.1x authentication for the switch.
- 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; those that fail authentication are blocked on the 802.1X port.

Examples

```
-> aaa authentication 802.1x rad1 rad2
-> no aaa authentication 802.1x
```

Release History

Release 6.1; 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.
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 6400, 6850E, 6855, 9000E

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 6.1.2; 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 mac	Displays information about the global 802.1X configuration on the switch.

MIB Objects

```
AaaAuthMACTable
   aaaMacSrvrName1
   aaaMacSrvrName2
   aaaMacSrvrName3
   aaaMacSrvrName4
```

aaa certificate-password

Configures the password for accessing a public certificate on the switch.

aaa certificate-password *password*

no aaa certificate-password *password*

Syntax Definitions

password	The password required to access the certificate.

Defaults

By default, the certiificate password is set to “alcatel”.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove the configured password from the switch configuration.
- This command is used with the Captive Portal feature to allow public certificate support.
- The password should match the passhprase used when the certificate was created.

Examples

```
-> aaa certificate-password certpass
-> no aaa certificate-password
```

Release History

Release 6.4.4; Command was introduced.

Related Commands

802.1x captive-portal name	Configures the name of the Captive Portal rediret URL.

MIB Objects

```
aaaServerTable
   aaaCertPassword
```

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, TACACS+, or LDAP server used for 802.1X accounting. At least one server is required. RADIUS, TACACS+, and LDAP server names are set up through the **aaa radius-server**, **aaa tacacs+-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 57, "Switch Logging Commands," for information about Switch Logging commands.

Defaults

Accounting is disabled by default.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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, TACACS+, 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, TACACS+, and LDAP servers may each have an additional backup specified through the **aaa radius-server**, **aaa tacacs+-server**, and **aaa ldap-server** commands.

Examples

```
-> aaa accounting 802.1x rad1 local
-> no aaa accounting 802.1x
```

Release History

Release 6.1; 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 mac

Enables/disables accounting for 802.1X non-supplicant (MAC-based) authentication sessions. Accounting servers keep track of network resources (time, packets, bytes, etc.) and user activity.

aaa accounting mac *server1* **[***server2***...] [local]**

no aaa accounting mac

Syntax Definitions

server1	The name of the RADIUS, TACACS+, or LDAP server used for accounting. At least one server is required. RADIUS, TACACS+, and LDAP server names are set up through the **aaa radius-server**, **aaa tacacs+-server**, and **aaa ldap-server** commands.
server2...	The names of backup servers for 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 57, "Switch Logging Commands," for information about Switch Logging commands.

Defaults

Accounting is disabled by default.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of the command to disable accounting.
- 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, TACACS+, 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, TACACS+, and LDAP servers may each have an additional backup specified through the **aaa radius-server**, **aaa tacacs+-server**, and **aaa ldap-server** commands.

Examples

```
-> aaa accounting mac rad1 local
-> no aaa accounting mac
```

Release History

Release 6.4.4; command was introduced.

Related Commands

aaa radius-server	Configures or modifies a RADIUS server for Authenticated VLANs, Authenticated Switch Access, or 802.1X port access control.
show aaa accounting mac	Displays information about accounting servers for 802.1X non-supplicant sessions.

MIB Objects

```
aaaAcctMACTable
   aaaAcctSvrInterface
   aaaAcctSvr1
   aaaAcctSvr2
   aaaAcctSvr3
   aaaAcctSvr4
   aaaAcctSvrRowStatus
```

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, TACACS+, 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**, **aaa tacacs+-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 57, "Switch Logging Commands," for information about Switch Logging commands.

Defaults

Accounting is disabled by default.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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, TACACS+, 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, TACACS+, and LDAP servers may each have an additional backup specified through the **aaa radius-server**, **aaa tacacs+-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 6.1; command was introduced.

Related Commands

aaa radius-server	Configures or modifies a RADIUS server for Authenticated VLANs or Authenticated Switch Access.
aaa tacacs+-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
   aaacvRowStatus
```

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 [*server_name1***] [***server_name2***...] [local]**

no aaa accounting session

Syntax Definitions

server_name1	The name of the RADIUS, TACACS+, or LDAP server used for accounting of authenticated switch sessions. At least one server is required. RADIUS, TACACS+, and LDAP server names are set up through the **aaa radius-server**, **aaa tacacs+-server**, and **aaa ldap-server** commands.
server_name2...	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 57, "Switch Logging Commands," for information about Switch Logging commands.

Defaults

Accounting is disabled by default.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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, TACACS+, 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, TACACS+, and LDAP servers may each have an additional backup specified through the **aaa radius-server**, **aaa tacacs+-server**, and **aaa ldap-server** commands.

Examples

```
-> aaa accounting session ldap1 radius2 local
-> no aaa accounting session
```

Release History

Release 6.1; 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
   aaacsRowStatus
```

aaa accounting session-id

Enable or disable session ID for AAA accounting for supplicant and non-supplicant clients and for management sessions like FTP, telnet, HTTP, console, HTTPS, SSH, and SNMP.

aaa accounting session-id {enable | disable]

Syntax Definitions

enable	Enable session ID for AAA accounting.
disable	Disable session ID for AAA accounting.

Defaults

By default, session ID for AAA accounting is disabled.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Accounting server must be configured as RADIUS server.
- RADIUS server configuration like RADIUS server name, acct-port, auth-port, secret key, retransmit count, timeout must be configured on the switch before configuring the accounting commands.

Examples

```
-> aaa accounting session-id enable
-> aaa accounting session-id disable
```

Release History

Release 6.4.5; command introduced.

Related Commands

aaa radius-server	Configures or modifies a RADIUS server for Authenticated VLANs, Authenticated Switch Access, or 802.1X port access control.
aaa accounting session	Configures an accounting server or servers for authenticated switch sessions.

MIB Objects

```
aaaAcctSATable
   aaaAccountingSessionIdStatus
```

aaa accounting command

Enables or disables the server for command accounting. Accounting servers keep track of network resources (time, packets, bytes, etc.) and user activity.

aaa accounting command *server1* **[***server2***...] [local]**

no accounting command

Syntax Definitions

server1	The name of the TACACS+ server used for command accounting. At least one server is required. TACACS+ server names are set up through the **aaa tacacs+-server** commands.
server2...	The names of TACACS+ backup servers. Up to 3 backups may be specified; 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 57, "Switch Logging Commands," for information about Switch Logging commands.

Defaults

Accounting is disabled by default.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of the command to disable command accounting.
- 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 can be only TACACS+ servers.
- 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*.
- TACACS+ server may each have an additional backup specified through the **aaa tacacs+-server** command.

Examples

```
-> aaa accounting command tacacs1 tacacs2 tacacs3
-> no aaa accounting command
```

Release History

Release 6.1.3; command was introduced.

Related Commands

show aaa accounting	Displays information about accounting servers configured for Authenticated Switch Access.

MIB Objects

```
aaaAcctCmdTable
   aaacmdSrvName1
   aaacmdSrvName2
   aaacmdSrvName3
   aaacmdSrvName4
```

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 Definitions

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 6400, 6850E, 6855, 9000E

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 6.1; 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 Definitions

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 6400, 6850E, 6855, 9000E

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

For more information about commands for configuring port binding rules, see Chapter 43, “Port Mobility Commands.”

Examples

```
-> avlan port-bound enable
```

Release History

Release 6.1; 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	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.
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 Definitions

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 6400, 6850E, 6855, 9000E

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*.
- When modifying the authentication address for a specific VLAN, make sure that the new address does not match an IP router interface address for the same VLAN. IP address resolution problems can occur if these two addresses are not unique.
- VLANs are set up for authentication through the **vlan authentication** command.

Examples

```
-> avlan 3 auth-ip 10.10.2.4
```

Release History

Release 6.1; 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 Definitions

N/A

Defaults

By default, the switch displays the HTTP client login page username and password prompts in English.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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**, **Hsecu.img**, or **Jsecu.img** file is installed. 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 6.1; command was introduced.

Related Commands

N/A

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***] [console-only {enable | disable}] [SHA+AES| SHA+3DES]**

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.
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.
console-only enable	Enables console only access for the user *admin*.
console-only disable	Disables console only access for the user *admin*.
SHA+AES	SHA is used for authentication and AES for privacy
SHA+3DES	SHA is used for authentication and 3DES for privacy

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**
console-only	**disable**

For more information about the default user account, see the *OmniSwitch AOS Release 6 Switch Management Guide*.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 OmniVista 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* and **password** *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*.
- Note that the exclamation point (!) is not a valid password character. In addition, specifying an asterisk (*) as one or more characters in a password is allowed as long as every character is not an asterisk. For example, **password** ****123456**** is allowed; **password ********** is not allowed.
- 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** or **configuration snapshot** command to save user settings over a reboot.
- When FIPS mode is enabled, user configuration for SNMPv3 access must use SHA+AES or SHA+3DES. Session establishment with MD5 or DES is rejected.

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 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 6.1; command was introduced.
Release 6.4.3; **Console-only** paramater was added.
Release 6.4.5; SHA+AES, SHA+3DES parameters added.

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
aaaAsaConfig
   aaaAsaAccessPolicyAdminConsoleOnly
```

password

Configures the current user's password.

password

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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. The default minimum password length is 8 characters.
- Note that the exclamation point (!) is not a valid password character. In addition, specifying an asterisk (*) as one or more characters in a password is allowed as long as every character is not an asterisk. For example, **password** ****123456**** is allowed; **password ********** is not allowed.
- Password settings are saved *automatically*; that is, the **write memory** 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 6.1; 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. The range is 1 to 14 characters.

Defaults

parameter	default
size	8

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A.

Examples

```
-> user password-size min 9
```

Release History

Release 6.1; command was introduced.
Release 6.3.1; minimum password size range changed to 1–14 characters.

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.
show user password-policy	Displays the global password policy configuration for the switch.

MIB Objects

```
aaaAsaConfig
   aaaAsaPasswordSizeMin
```

user password-expiration

Configures an expiration date for all 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 6400, 6850E, 6855, 9000E

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 6.1; 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.
show user password-policy	Displays the global password policy configuration for the switch.

MIB Objects

```
aaaAsaConfig
   aaaAsaDefaultPasswordExpirationInDays
```

user password-policy cannot-contain-username

Specifies whether or not a user can configure a password that contains the username for the account.

user password-policy cannot-contain-username {enable | disable}

Syntax Definitions

enable	Does not allow the password to contain the username.
disable	Allows the password to contain the username.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The status of this function is specified as part of a global password policy that is applied to all passwords when they are created or modified.
- When this function is enabled, a check is done at the time the password is created or modified to ensure that the username is not specified as part of the password text.

Examples

```
-> user password-policy cannot-contain-username enable
-> user password-policy cannot-contain-username disable
```

Release History

Release 6.3.1; command was introduced.

Related Commands

show user password-policy	Displays the global password policy configuration for the switch.

MIB Objects

```
aaaAsaConfig
   aaaAsaPasswordContainUserName
```

user password-policy min-uppercase

Configures the minimum number of uppercase English characters required for a valid password.

user password-policy min-uppercase *number*

Syntax Definitions

number	The minimum number of uppercase characters. The range is 0 to 7.

Defaults

parameter	default
number	0

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Specify **0** with this command to disable the minimum uppercase character requirement.
- The minimum number of uppercase characters is specified as part of a global password policy that is applied to all passwords when they are created or modified.

Examples

```
-> user password-policy min-uppercase 2
-> user password-policy min-uppercase 0
```

Release History

Release 6.3.1; command was introduced.

Related Commands

show user password-policy	Displays the global password policy configuration for the switch.

MIB Objects

```
aaaAsaConfig
   aaaAsaPasswordMinUpperCase
```

user password-policy min-lowercase

Configures the minimum number of lowercase English characters required for a valid password.

user password-policy min-uppercase *number*

Syntax Definitions

number	The minimum number of lowercase characters. The range is 0 to 7.

Defaults

parameter	default
number	0

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Specify **0** with this command to disable the minimum lowercase character requirement.
- The minimum number of lowercase characters is specified as part of a global password policy that is applied to all passwords when they are created or modified.

Examples

```
-> user password-policy min-lowercase 2
-> user password-policy min-lowercase 0
```

Release History

Release 6.3.1; command was introduced.

Related Commands

show user password-policy	Displays the global password policy configuration for the switch.

MIB Objects

```
aaaAsaConfig
   aaaAsaPasswordMinLowerCase
```

user password-policy min-digit

Configures the minimum number of base-10 digits required for a valid password.

user password-policy min-digit *number*

Syntax Definitions

number	The minimum number of digits. The range is 0 to 7.

Defaults

parameter	default
number	0

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Specify **0** with this command to disable the minimum number of digits requirement.
- The minimum number of digits requirement is specified as part of a global password policy that is applied to all passwords when they are created or modified.

Examples

```
-> user password-policy min-digit 2
-> user password-policy min-digit 0
```

Release History

Release 6.3.1; command was introduced.

Related Commands

show user password-policy	Displays the global password policy configuration for the switch.

MIB Objects

```
aaaAsaConfig
   aaaAsaPasswordMinDigit
```

user password-policy min-nonalpha

Configures the minimum number of non-alphanumeric characters (symbols) required for a valid password.

user password-policy min-nonalpha *number*

Syntax Definitions

number	The minimum number of non-alphanumeric characters. The range is 0 to 7.

Defaults

parameter	default
number	0

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Specify **0** with this command to disable the minimum non-alphanumeric character requirement.
- The minimum number of non-alphanumeric characters is specified as part of a global password policy that is applied to all passwords when they are created or modified.

Examples

```
-> user password-policy min-nonalpha 2
-> user password-policy min-nonalpha 0
```

Release History

Release 6.3.1; command was introduced.

Related Commands

show user password-policy	Displays the global password policy configuration for the switch.

MIB Objects

```
aaaAsaConfig
   aaaAsaPasswordMinNonAlpha
```

user password-history

Configures the maximum number of old passwords to retain in the password history.

user password-history *number*

Syntax Definitions

number	The maximum number of old passwords to retain. The range is 0 to 24.

Defaults

parameter	default
number	4

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Specify **0** with this command to disable the password history function.
- The user is prevented from specifying any passwords that are recorded in the password history and fall within the range configured through this command.
- The password history value is specified as part of a global password policy that is applied to all passwords when they are created or modified.

Examples

```
-> user password-history 2
-> user password-history 0
```

Release History

Release 6.3.1; command was introduced.

Related Commands

show user password-policy	Displays the global password policy configuration for the switch.

MIB Objects

```
aaaAsaConfig
   aaaAsaPasswordHistory
```

user password-min-age

Configures the minimum number of days during which a user is prevented from changing a password.

user password-min-age *days*

Syntax Definitions

days	The number of days to use as the minimum age of the password. The range is 0 to 150.

Defaults

parameter	default
days	0

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Specify **0** with this command to disable the minimum number of days requirement.
- Configure the minimum age of a password with a value that is less than the value configured for the password expiration.
- The password minimum age value is specified as part of a global password policy that is applied to all passwords when they are created or modified.

Examples

```
-> user password-min-age 7
-> user password-min-age 0
```

Release History

Release 6.3.1; command was introduced.

Related Commands

show user password-policy	Displays the global password policy configuration for the switch.

MIB Objects

```
aaaAsaConfig
   aaaAsaPasswordMinAge
```

user lockout-window

Configures a moving period of time (observation window) during which failed login attempts are counted to determine if the number of failed attempts has exceeded the number of allowed attempts. The number of failed login attempts is decremented by the number of failed attempts that age beyond the observation window time period.

user lockout-window *minutes*

Syntax Definitions

minutes	The number of minutes the observation window remains active. The range is 0 to 99999.

Defaults

parameter	default
minutes	0

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- This command is only available to the **admin** user because the **admin** user account is the only account protected from any type of lockout attempt.
- Specify **0** with this command to disable the observation window function. This means that failed login attempts will never age out; the number of failed attempts is never decremented.
- Do not configure an observation window time period that is greater than the lockout duration time period.
- If the number of failed login attempts exceeds the number of failed attempts allowed before the observation window time expires, then the user account is locked out of the switch.
- The observation window time period is a global lockout setting that is applied to all passwords configured on the switch.
- Lockout settings are saved *automatically*; that is, these settings do not require the **write memory** or **configuration snapshot** command to save user settings over a reboot.

Examples

```
-> user lockout-window 500
-> user lockout-window 0
```

Release History

Release 6.3.1; command was introduced.

Related Commands

user lockout-duration	Configures the amount of time a user account remains locked out of the switch.
user lockout-threshold	Configures the number of failed password attempts allowed before the user account is locked out of the switch.
user lockout unlock	Manually locks or unlocks a user account on the switch.
show user lockout-setting	Displays the global user lockout settings for the switch.

MIB Objects

```
aaaAsaConfig
   aaaAsaLockoutWindow
```

user lockout-threshold

Configures the number of failed password login attempts allowed during a certain period of time (observation window). If the number of failed attempts exceeds the lockout threshold number before the observation window period expires, the user account is locked out.

user lockout-threshold *number*

Syntax Definitions

number	The number of failed login attempts allowed. The range is 0 to 999.

Defaults

parameter	default
number	0

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- This command is only available to the **admin** user because the **admin** user account is the only account protected from any type of lockout attempt.
- If the lockout threshold is set to zero (the default), there is no limit to the number of failed login attempts allowed.
- A user account remains locked out for the length of the lockout duration time period; at the end of this time, the account is automatically unlocked.
- If the lockout duration time period is set to zero, only the **admin** user or a user with read/write AAA privileges can unlock a locked user account. An account is unlocked by changing the user account password or with the **user lockout unlock** command.
- The lockout threshold time period is a global lockout setting that is applied to all passwords configured on the switch.
- Lockout settings are saved *automatically*; that is, these settings do not require the **write memory** or **configuration snapshot** command to save user settings over a reboot.

Examples

```
-> user lockout-threshold 3
-> user lockout-threshold 0
```

Release History

Release 6.3.1; command was introduced.

Related Commands

user lockout-window	Configures a window of time during which failed login attempts are counted to determine if the number of failed attempts has exceeded the number of allowed attempts.
user lockout-duration	Configures the length of time a user account remains locked out of the switch.
user lockout unlock	Manually locks or unlocks a user account on the switch.
show user lockout-setting	Displays the global user lockout settings for the switch.

MIB Objects

```
aaaAsaConfig
   aaaAsaLockoutThreshold
```

user lockout-duration

Configures the length of time a user account remains locked out of the switch. At the end of this time period, the user account is automatically unlocked.

user lockout-duration *minutes*

Syntax Definitions

minutes	The number of minutes the user account remains locked out. The range is 0 to 99999.

Defaults

parameter	default
minutes	0

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- This command is only available to the **admin** user because the **admin** user account is the only account protected from any type of lockout attempt.
- Note that if the lockout duration time period is set to zero (the default), then locked user accounts are never automatically unlocked.
- Only the **admin** user or a user with read/write AAA privileges can unlock a locked user account when the lockout duration time is set to zero. An account is unlocked by changing the user password or with the **user lockout unlock** command.
- Do not configure a lockout duration time period that is less than the amount of time configured for the observation window.
- The lockout duration time period is a global lockout setting that is applied to all passwords configured on the switch.
- Lockout settings are saved *automatically*; that is, these settings do not require the **write memory** or **configuration snapshot** command to save user settings over a reboot.

Examples

```
-> user lockout-duration 60
-> user lockout-duration 0
```

Release History

Release 6.3.1; command was introduced.

Related Commands

user lockout-window	Configures a window of time during which failed login attempts are counted to determine if the number of failed attempts has exceeded the number of allowed attempts,
user lockout-threshold	Configures the number of failed password attempts allowed before the user account is locked out of the switch.
user lockout unlock	Manually locks or unlocks a user account on the switch.
show user lockout-setting	Displays the global user lockout settings for the switch.

MIB Objects

```
aaaAsaConfig
   aaaAsaLockoutDuration
```

user lockout unlock

Manually locks or unlocks a user account on the switch.

user {lockout | unlock}

Syntax Definitions

username	The username of the account to lock or unlock.
lockout	Locks the user account out of the switch.
unlock	Unlocks a locked user account.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- This command is only available to the **admin** user or a user with read/write AAA privileges.
- The **admin** user account is protected from any type of lockout attempt.
- User lockouts and unlocks are saved *automatically*; that is, these settings do not require the **write memory** or **configuration snapshot** command to save user settings over a reboot.

Examples

```
-> user j_smith lockout
-> user j_smith unlock
```

Release History

Release 6.3.1; command was introduced.

Related Commands

show user	Displays information about all users or a particular user configured in the local user database on the switch.
show user lockout-setting	Displays the global user lockout settings for the switch.

MIB Objects

```
aaaUserTable
   aaauPasswordLockoutEnable
```

aaa admin-logout

Administratively logs a user out of the network. This command requires administrative privileges.

aaa admin-logout {mac-address *mac_address* **| port** *slot/port* **| user** *user_name* **| user-network-profile name** *profile_name***}**

Syntax Definitions

mac_address	The source MAC address of a user device.
slot/port	The slot and port number designation for a specific switch port. All users learned on this port are logged out.
user_name	The username of the account to log out.
profile_name	The name of an existing User Network Profile (UNP). All users classified with this profile are logged out of the switch.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- This command is only available to the **admin** user.
- The **admin** user account is protected from any attempt to log out the admin user.

Examples

```
-> aaa admin-logout mac-address 00:2a:95:00:3a:10
-> aaa admin-logout port 1/9
-> aaa admin-logout user j_smith
-> aaa admin-logout user-network-profile name marketing
```

Release History

Release 6.3.4; command was introduced.

Related Commands

show aaa-device all-users	Displays the global user lockout settings for the switch.

MIB Objects

```
alaDot1xAdminLogoutParams
   alaDot1xAdminLogoutType
   alaDot1xAdminLogoutMacAddress
   alaDot1xAdminLogoutUserName
```

```
alaDot1xAdminLogoutNetworkProfileName
alaDot1xAdminLogoutInterfaceId
```

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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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
```

aaa user-network-profile

Configures a User Network Profile (UNP) that is used to provide role-based access to the switch. The UNP determines the VLAN ID a device can join, whether or not a Host Integrity Check (HIC) is applied to the device, and if any QoS policy rules are used to control access to network resources, and the maximum ingress and egress bandwidth along with maximum default depth associated with the UNP.

aaa user-network-profile name *profile_name* **vlan** *vlan-id* **[hic [enable | disable]] [policy-list-name** *list_name***] [maximum-ingress-bandwidth** *num* **maximum-egress-bandwidth** *num* **maximum-default-depth** *num***]**

no aaa user-network-profile name *profile_name*

Syntax Definitions

profile_name	The name of an existing or a new user profile. The name specified here must match with the Filter-ID attribute returned by the RADIUS server. The user profile name can range from 1 to 32 characters in length.
vlan-id	The VLAN identification number for an existing VLAN that will be assigned to a user. The valid range is 1-4094.
enable	Enables Host Integrity Check for the profile.
disable	Disables Host Integrity Check for the profile.
list_name	The name of an existing QoS policy list to apply to devices classified by the User Network Profile. It is possible to assign up to 13 policy lists to each user profile.
maximum-ingress-bandwidth	Maximum ingress bandwidth associated to a UNP. The valid range is 0 - 10485760 (Kbit/sec). **Note**: If the ingress bandwidth is configured to ‘0’, all traffic is dropped and the user is isolated from the network. Hence, extra care should be taken to ensure that the bandwidth is not configured as ‘0’.
maximum-egress-bandwidth	Maximum egress bandwidth associated to a UNP. The valid range is 0-10485760 (Kbit/sec).
maximum-default-depth *num*	Maximum default depth associated to a UNP. The valid range is 0 - 16384 in Kilobytes.

Defaults

hic enable | disable	disabled
list_name	none
maximum-ingress-bandwidth **maximum-egress-bandwidth**	No bandwidth limitation is applied.
maximum-default-depth	Optimal default depth value is 1Mbytes is programmed.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E
OmniSwitch 9000E; **hic enable**, **hic disable**, **policy-list-name** parameters not supported.

Usage Guidelines

- Use the **no** form of this command to remove a UNP from the switch configuration.
- This command is used with RADIUS as the authentication server
- Enabling the **hic** parameter triggers the HIC verification process for any devices to which this profile is applied. The switch interacts with the InfoExpress CyberGatekeeper HIC server to determine host compliance.
- The egress and ingress bandwidth can be configured in kilo (K), mega (M), giga (G), or tera (T) unit/ denominator. If no bandwidth unit is specified while configuring the bandwidth, then the bandwidth value is assumed to be in Kbit/sec.
  For example,
  - if maximum ingress bandwidth is configured as 1024, then the maximum ingress bandwidth is considered as 1024 Kbit/sec.
  - If maximum ingress bandwidth is configured as 23.2K, then it is stored as 24K rounding off to next integer value.
- The configured bandwidth is displayed in the show command output with denominator marked as "K", "M" , "G" or "T" rounded off by maximum two decimal points. For example, the maximum ingress bandwidth of 20000Kb/sec, and 2000000Kb/sec is displayed 20.0M, and 2.0G respectively in the show output.
- Maximum ingress and egress bandwidth can be set to 0. Bandwidth ‘0’ is a special valid bandwidth value. On configuring ingress bandwidth as ‘0’, all traffic is dropped on the port on all the supported platforms. And, on configuring egress bandwidth as ‘0’, no traffic is dropped on all the supported platforms.
- When 8021x is disabled on the port or when interface is administratively brought down, the bandwidth applied on 8021x port set by UNP is removed. In both cases, the bandwidth reverts to the bandwidth set by QoS port, if any.
- If multiple users are getting authenticated on a port, then the latest user authenticated will over ride the previous bandwidth associated. If there is no bandwidth associated to a UNP, then no rate limitations are enforced and previous set bandwidth remains untouched. Refer to *OmniSwitch AOS Release 6 Network Configuration Guide* for more information.

Examples

```
-> aaa user-network-profile name engineering vlan 10
-> aaa user-network-profile name marketing vlan 30 hic enable
-> aaa user-network-profile name guest_user vlan 500 hic enable policy-list name
temp_rules
-> aa user-network-profile name "profile1" vlan 50 maximum-ingress-bandwidth 1024
maximum-egress-bandwidth 256 maximum-default-depth 128
```

Release History

Release 6.3.1; command was introduced.
Release 6.3.4; **hic enable**, **hic disable**, **policy-list name** parameters added.
Release 6.4.5; **maximum-ingress-bandwidth**, **maximum-egress-bandwidth**, **maximum-default-depth** parameters added.

Related Commands

show aaa user-network-profile	Displays the UNP configuration for the switch.
aaa hic	Globally enables or disables the HIC feature for the switch.
aaa classification-rule mac-address	Defines a MAC address UNP mobile rule.
aaa classification-rule mac-address-range	Defines a MAC address UNP mobile rule for a range of MAC addresses.
aaa classification-rule ip-address	Defines an IP network address UNP mobile rule.
show 802.1x rate-limit	Displays current rate limit configuration on 8021x enabled ports.

MIB Objects

```
aaaUserNetProfileTable
   aaaUserNetProfileName
   aaaUserNetProfileVlanID
   aaaUserNetProfileHICflag
   aaaUserNetProfileQosPolicyListName
   aaaUserNetProfileMaxIngressBw
   aaaUserNetProfileMaxEgressBw
   aaaUserNetProfileMaxDefaultDepth
```

aaa classification-rule mac-address

Defines a User Network Profile (UNP) MAC address mobile rule. If the source MAC address of a device matches the MAC address defined for the rule, the specified UNP is applied to the device. UNP mobile rules are applied using an Access Guardian Group Mobility device classification policy.

aaa classification-rule mac-address *mac_address* **user-network-profile name** *profile_name*

aaa classification-rule no mac-address *mac_address*

Syntax Definitions

mac_address	MAC address (e.g., 00:00:39:59:f1:0c).
profile_name	The name of an existing user network profile.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove the UNP mobile rule from the switch configuration.
- To change the UNP associated with a mobile rule, enter the MAC address of an existing rule but specify a different UNP name.
- When Group Mobility is configured as an Access Guardian device classification policy for an 802.1x port, both UNP mobile rules and VLAN mobile rules are applied to device traffic on that port.
- Note that UNP mobile rules take precedence over VLAN mobile rules.

Examples

```
-> aaa classification-rule mac-address 00:00:2a:33:44:01 user-network-profile name
accounting
-> aaa classification-rule no mac-address 00:00:2a:33:44:01
```

Release History

Release 6.3.4; command was introduced.

Related Commands

aaa classification-rule mac-address-range	Configures a UNP mobile rule for a range of MAC addresses.
aaa classification-rule ip-address	Configures an IP address UNP mobile rule.
show aaa classification-rule	Displays the UNP configuration.
show aaa user-network-profile	Displays the UNP configuration.

MIB Objects

```
aaaUNPMacRuleTable
   aaaUNPMacRuleAddr
   aaaUNPMacRuleProfileName
```

aaa classification-rule mac-address-range

Defines a User Network Profile (UNP) mobile rule for a range of MAC addresses. If the source MAC address of a device matches any address within the range of MAC addresses, the specified UNP is applied to the device. UNP mobile rules are applied using an Access Guardian Group Mobility device classification policy.

aaa classification-rule mac-address-range *low_mac_address high_mac_address* **user-network-profile name** *profile_name*

aaa classification-rule no mac-address-range *low_mac_address*

Syntax Definitions

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).
profile_name	The name of an existing user network profile.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove the UNP mobile rule from the switch configuration.
- To change the UNP associated with a mobile rule, enter the MAC address range of an existing rule but specify a different user network profile name.
- When Group Mobility is configured as an Access Guardian device classification policy for an 802.1x port, both UNP mobile rules and VLAN mobile rules are applied to device traffic on that port.
- Note that UNP mobile rules take precedence over VLAN mobile rules.

Examples

```
-> aaa classification-rule mac-address-range 00:00:2a:33:44:01 00:00:2a:33:44:10
user-network-profile name accounting
-> aaa classification-rule no mac-address-range 00:00:2a:33:44:01
```

Release History

Release 6.3.4; command was introduced.

Related Commands

aaa classification-rule mac-address	Configures a MAC address UNP mobile rule.
aaa classification-rule ip-address	Configures an IP address UNP mobile rule.
show aaa classification-rule	Displays the UNP mobile rule configuration.
show aaa user-network-profile	Displays the UNP configuration.

MIB Objects

```
aaaUNPMacRangeRuleTable
   aaaUNPMacRangeRuleLoAddr
   aaaUNPMacRangeRuleHiAddr
   aaaUNPMacRangeRuleProfileName
```

aaa classification-rule ip-address

Defines a User Network Profile (UNP) IP address mobile rule. If the source IP address of a device matches the IP address defined for the rule, the specified UNP is applied to the device. UNP mobile rules are applied using an Access Guardian Group Mobility device classification policy

aaa classification-rule ip-address *ip_address* **[***subnet_mask***] user-network-profile name** *profile_name*

aaa classification-rule no ip-address *ip_address* **[***subnet_mask***]**

Syntax Definitions

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).
profile_name	The name of an existing user network profile.

Defaults

By default, the subnet mask is set to the default subnet mask value for the IP address class.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove the UNP mobile rule from the switch configuration.
- To change the UNP associated with a mobile rule, enter the IP address of an existing rule but specify a different UNP name.
- When Group Mobility is configured as an Access Guardian device classification policy for an 802.1x port, both UNP mobile rules and VLAN mobile rules are applied to device traffic on that port.
- Note that UNP mobile rules take precedence over VLAN mobile rules.

Examples

```
-> aaa classification-rule ip-address 10.1.1.1 user-network-profile name accounting
-> aaa classification-rule ip-address 198.4.21.1 255.255.0.0 user-network-profile
name marketing
-> aaa classification-rule no ip-address 10.1.1.1
```

Release History

Release 6.3.4; command was introduced.

Related Commands

aaa classification-rule mac-address	Configures a MAC address UNP mobile rule.
aaa classification-rule mac-address-range	Configures a UNP mobile rule for a range of MAC addresses.
show aaa classification-rule	Displays the UNP mobile rule configuration.
show aaa user-network-profile	Displays the UNP configuration.

MIB Objects

```
aaaUNPIpNetRuleTable
   aaaUNPIpNetRuleAddr
   aaaUNPIpNetRuleMask
   aaaUNPIpNetRuleProfileName
```

aaa hic server-name

Configures the identity of the Host Integrity Check (HIC) InfoExpress CyberGatekeeper server. HIC is a User Network Profile (UNP) option that when enabled, verifies the integrity of a device connected to the switch. Both HIC and UNP are components of the Access Guardian security framework.

aaa hic server-name *server* **ip-address** *ip_address* **secret** *secret* **[role {primary | backup}] [udp-port** *udp_port***]**

aaa hic no server-name *server*

Syntax Definitions

server	The name of the HIC server.
ip_address	The IP address of the HIC 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.
primary | backup	Configures this server as either the Primary or Backup HIC server**.**
udp_port	The UDP destination port number (1025–65536) for HIC requests.

Defaults

parameter	default
udp_port	11707

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- Configuring the HIC server identity and related parameters is required before globally enabling the HIC feature for the switch.
- The primary server is initially configured as the active server and the backup server as inactive.
- A keepalive message will be sent to the active server if the switch does not receive any HIC-UPDATEs from the server for 16 seconds. The switch will remain the active server upon receiving the keepalive acknowledgement.
- The switch will send a total of four keepalive messages to the active server in 6 second intervals. If no response is received, the inactive server becomes the active server provided the server status is UP.
- If both servers are unavailable the switch operates in either Hold or Pass-through mode based on the HIC Server failure mode that has been configured.
- Background polling (Keepalive) packets are sent to the primary server every 16 seconds.

- If the server's role is not specified the first configured server will be the primary and the next configured server will be backup.

Examples

```
-> aaa hic server-name hic-srv1 ip-address 2.2.2.2 secret wwwtoe mode primary
-> aaa hic server-name hic-srv1 ip-address 2.2.2.2 udp-port 12049
-> aaa hic no server-name hic-srv1
```

Release History

Release 6.3.4; command was introduced.
Release 6.4.4; **role** parameter was introduced.

Related Commands

show aaa hic server	Displays the HIC server configuration for the switch.
aaa hic server-failure mode	Configures the failure mode to be applied when both servers are unavailable.
show aaa server	Displays information about AAA servers.
aaa hic redundancy background-poll-interval	Configures a download server as an exception to the HIC process.
aaa hic	Globally enables and disables the HIC feature for the switch.

MIB Objects

```
aaaHicSvrTable
   aaaHicSvrName
   aaaHicSvrIpAddr
   aaaHicSvrRole
   aaaHicSvrConnection
   aaaHicSvrPort
   aaaHicSvrKey
   aaaHicSvrStatus
```

aaa hic redundancy background-poll-interval

Configures the background polling interval that determines when the primary server is considered active after being inactive.

aaa hic redundancy background-poll-interval *value*

Syntax Definitions

value	The background polling interval in seconds. The valid range is from 16 to 256 in multiples of 16.

Defaults

parameter	default
value	16

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- If the primary server is unavailable and placed in the inactive mode the switch begins to poll the primary server in the background.
- In order to avoid overwhelming a primary server that becomes active again the switch will generate a random reconnect value. When the switch receives continuous keepalive responses equal to the random reconnect value it assumes the primary server is ready to takeover the active role.
- When the backup server is inactive this interval determines the frequncy at which the poll packets should be sent to backup server.
- Once the primary server becomes active, the backup server becomes inactive.

Examples

```
-> aaa hic redundancy background-poll-interval 32
```

Release History

Release 6.4.4; command was introduced.

Related Commands

show aaa hic	Displays the global Host Integrity Check (HIC) configuration for the switch.

MIB Objects

```
aaaHicConfigInfo
   aaaHicBgPollInterval
```

aaa hic server-failure mode

Configures the failure mode to be applied when both servers are unavailable.

aaa hic server-failure mode {hold | pass-through}

Syntax Definitions

hold	Places all new users in hold mode if the HIC servers are unavailable.
pass-through	Places all new users in pass-through mode if the HIC servers are unavailable.

Defaults

parameter	default
hold | pass-through	**hold**

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- The server failure mode has no affect on users that have already passed HIC successfully.
- In **hold** mode new users will stay in the HIC IN PROGRESS state while the servers are unavailable.
- In **pass-through** mode new users will be moved to HIC PASSTHROUGH mode and treated same as HIC SUCCESS.

Examples

```
-> aaa hic server-failure mode pass-through
```

Release History

Release 6.4.4; command was introduced.

Related Commands

show aaa hic server	Displays the HIC server configuration for the switch.

MIB Objects

```
aaaHicConfigInfoTable
   aaaHicSrvFailMode
```

aaa hic server-failure policy user-network-profile change

Configures which network profiles users will be moved to when both HIC servers are unavailable.

aaa hic server-failure policy user-network-profile change *unp1* **to** *unp2*

aaa hic server-failure policy user-network-profile no change

Syntax Definitions

unp1	Name of the original UNP from which the user will be moved if the servers are not reachable and the failure mode is set to Hold.
unp2	Name of the UNP that the HIC host will be moved to while the HIC servers are down.

Defaults

parameter	default
change | no change	**no change**

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- If the HIC failure mode is set to Hold and the HIC servers are not available this command allows users in the HIC-in-progress state to be moved from *unp1* to *unp2*. Once the HIC servers come back up, the user shall be moved back to the original *unp1* and the HIC-check will be restarted.
- A maximum of 8 server-failure policies can be configured.
- Use the **no** parameter to prevent users from moving out of their current UNP.

Examples

```
-> aaa hic server-failure policy user-network-profile change unp_orig to unp_temp
-> aaa hic server-failure policy user-network-profile no change
```

Release History

Release 6.4.4; command was introduced.

Related Commands

show aaa hic server	Displays the HIC server configuration for the switch.

MIB Objects

```
aaaHicSvrDownUnpMapTable
   aaaHicSvrDownUnpMapEntry
   aaaHicSvrDownUnpName
   aaaHicSvrDownMappedUnpName
   aaaHicSvrDownUnpRowStatus
```

aaa hic allowed-name

Configures a list of servers that are excluded from the Host Integrity Check (HIC) process. This list identifies servers that a host can communicate with during the verification process, when the host has limited access to the network.

aaa hic allowed-name *server* **ip-address** *ip_address* **[ip-mask** *subnet_mask***]**

aaa hic no allowed-name *server*

Syntax Definitions

server	The name of the server.
ip_address	The IP address of the primary HIC server.
subnet_mask	A valid IP address mask (for example, 255.0.0.0, 255.255.0.0) to identify the IP subnet for the download server.

Defaults

parameter	default
subnet_mask	255.255.255.255

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- Use the **no** form of the command to remove a server from the HIC exception list.
- Up to 16 server exception entries are allowed.
- If a host device requires access to the HIC server via a Web-based agent, make sure the Web agent download server is added to this list.
- Add any additional servers required for remediation to this list..

Examples

```
-> aaa hic allowed-name rem-srv1 ip-address 10.1.1.1
-> aaa hic allowed-name patch-srv1 ip-address 11.1.1.1
-> aaa hic allowed-name web-agent-srv1 ip-address 12.1.1.1
-> aaa hic no allowed-name rem-srv1
```

Release History

Release 6.3.4; command was introduced.
Release 6.4.5; allowed-name entries increased to a maximum of 16 servers.

Related Commands

show aaa server	Displays information about AAA servers.
aaa hic server-name	Configures a HIC server for use with the switch.
aaa hic	Globally enables and disables the HIC feature for the switch.

MIB Objects

```
aaaHicAllowedTable
   aaaHicAllowedName
   aaaHicAllowedIpAddr
   aaaHicAllowedIpMask
   aaaHicAllowedRowStatus
```

aaa hic

Globally enables or disables the Host Integrity Check (HIC) feature for the switch.

aaa hic {enable | disable}

Syntax Definitions

enable	Enables the HIC feature for the switch.
disable	Disables the HIC feature for the switch.

Defaults

HIC is disabled by default.

Platforms Supported

OmniSwitch 6400, 6855

Usage Guidelines

- This command requires the configuration of the HIC server information before HIC is enabled on the switch.
- When HIC is enabled for the switch, configuring HIC server parameters is not allowed.
- Note that the VLAN Stacking feature is not available when HIC is configured for the switch. These two features are mutually exclusive in that only one of them can run on the switch at any given time.

Examples

```
-> aaa hic enable
-> aaa hic disable
```

Release History

Release 6.3.4; command was introduced.

Related Commands

show aaa server	Displays information about AAA servers.
aaa hic server-name	Configures a HIC server for use with the switch.
aaa hic redundancy background-poll-interval	Configures a remediation, patch, or web agent download server as an exception to the Host Integrity Check (HIC) process.
aaa user-network-profile	Configures a User Network Profile (UNP) that is used to provide role-based access to the switch.

MIB Objects

```
aaaHicConfigInfo
   aaaHicStatus
```

aaa hic web-agent-url

Specifies the URL for the Web agent download server. The switch uses this information to redirect a host (client device) to a download server where the host can obtain the InfoExpress Web-based compliance agent. This agent provides the interaction between the switch, host device, and HIC server.

aaa hic web-agent-url *url*

Syntax Definitions

url	The URL address for the web agent download server.

Defaults

By default, no URL is configured.

Platforms Supported

OmniSwitch 6400, 6855

Usage Guidelines

- This command overwrites any URL information that was previously configured.
- Add the corresponding name and IP address for the web agent download server to the HIC allowed name exception list.

Examples

```
-> aaa hic web-agent-url http://10.10.10.10:2146
```

Release History

Release 6.3.4; command was introduced.

Related Commands

show aaa hic	Displays the global HIC configuration for the switch.
aaa hic server-name	Configures a HIC server for use with the switch.
aaa hic redundancy background-poll-interval	Configures a remediation, patch, or web agent download server as an exception to the Host Integrity Check (HIC) process.
aaa hic	

MIB Objects

```
aaaHicConfigInfo
   aaaHicWebAgentDownloadURL
```

aaa hic custom-proxy-port

Specifies the HTTP proxy port number used in the Web browser configuration of a host device. The HIC process uses this information when interacting with hosts using the InfoExpress Web-based compliance agent.

aaa hic custom-proxy-port *proxy_port*

Syntax Definitions

proxy_port	An HTTP proxy port number (1025–65535).

Defaults

The HTTP proxy port is set to 8080.

Platforms Supported

OmniSwitch 6400, 6855

Usage Guidelines

This command overwrites the existing proxy port number.

Examples

```
-> aaa hic custom-proxy-port 8878
```

Release History

Release 6.3.4; command was introduced.

Related Commands

show aaa server	Displays information about AAA servers.
aaa hic	Globally enables the HIC feature for the switch.

MIB Objects

```
aaaHicConfigInfo
   aaaHicCustomHttpProxyPort
```

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 6400, 6850E, 6855, 9000E
OmniSwitch 9000E, 6855-U24X; VRF supported.

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 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,

-> show aaa server rad1
Server name = rad1
  Server type           = RADIUS,
  IP Address 1          = 10.111.0.1,
  Retry number         = 3,
  Time out (sec)       = 2,
  Authentication port  = 1812,
  Accounting port      = 1813,
  VRF                  = "Management-vrf"
```

```
-> show aaa server TPub1
Server name = TPub1
   Server type          = TACACS+,
   IP Address 1         = 10.10.5.1,
   Port                 = 3,
   Timeout (in sec)     = 2,
   Encryption enabled   = no

-> 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, TACACS+, and LDAP parameters are configured through the **aaa radius-server**, **aaa tacacs+-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, TACACS+ or LDAP server name is defined through the **aaa radius-server, aaa tacacs+-server,** and **aaa ldap-server** commands respectively.
Server type	The type of server (ACE, LDAP, TACACS+, or RADIUS).
Host name	The name of the primary LDAP, TACACS+, 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 or TACACS+ server.
Encryption enabled	The status of the encryption.
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.
VRF	The VRF name assigned to the server.

Release History

Release 6.1; command was introduced.
Release 6.1.3; **Encryption enabled** field was added.
Release 6.4.2; added **VRF** ouput field.

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.
aaa tacacs+-server	Configures or modifies an TACACS+ server for Authenticated VLANs or Authenticated Switch Access.

MIB Objects

```
aaaServerTable
   aaasName
   aaasHostName
   aaasIpAddress
   aaasHostName2
   aaasIpAddress2
   aaasRadKey
   aaasRetries
   aaasTimeout
   aaasRadAuthPort
   aaasRadAcctPort
   aaasProtocol
   aaasTacacsKey
   aaasTacacsPort
   aaasLdapPort
   aaasLdapDn
   aaasLdapPasswd
   aaasLdapSearchBase
   aaasLdapServType
   aaasLdapEnableSsl
   aaasVrfName
```

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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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  = TacacsServer
   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 6.1; 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
   aaatsRowStatus
```

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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6855

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 6.1.2; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

Accounting servers are configured through the **aaa radius-server**, **aaa tacacs+-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 6.1; 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 mac

Displays information about accounting servers for 802.1X non-supplicant sessions.

show aaa authentication mac [statistics]

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Accounting servers are configured through the **aaa radius-server**, **aaa tacacs+-server**, and **aaa ldap-server** commands.

Examples

```
-> show aaa accounting mac
1rst authentication server = onyx,
2nd accounting server= odyssey
3rd accounting server= local

-> show aaa accounting mac statistics
NSA-users Logged in        = 1,
NSA-users Logged out      = 1,
NSA-users Failed info       = 0,
NSA-users IntermUpdate  = 0
```

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 6.4.4; command was introduced.

Related Commands

aaa accounting mac	Enables/disables accounting for 802.1X non-supplicant authentication sessions.

MIB Objects

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 6400, 6850E, 6855, 9000E

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 6.1; command was introduced.

Related Commands

aaa accounting mac	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 6400, 6850E, 6855, 9000E

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 6.1; 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

By default, all users are displayed if the *username* parameter is not specified with this command.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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.
- This command can be used to verify the SNMP level configured for the user when in FIPS mode.

Examples

```
-> show user
User name = Customer1,
  Password expiration     = 10/27/2007 11:01 (30 days from now),
  Password allow to be modified date     = 9/30/2007 10:59 (3 days from now),
  Account lockout     = Yes (Automatically unlocked after 19 minute(s)from now),
  Password bad attempts     = 3,
  Read Only for domains   = None,
  Read/Write for domains  = Admin System Physical Layer2 Services policy Security ,
  Read/Write for families = ip rip ospf bgp vrrp ip-routing ipx ipmr ipms ,
  Snmp allowed     = YES,
  Snmp authentication     = SHA,
  Snmp encryption     = DES
  Console-Only     = Disabled
User name = admin,
  Password expiration     = 10/27/2007 11:01 (30 days from now),
  Password allow to be modified date     = 9/30/2007 10:59 (3 days from now),
  Account lockout     = None,
  Password bad attempts     = 0,
  Read Only for domains   = None,
  Read/Write for domains  = All ,
  Snmp allowed     = NO
  Console-Only     = Disabled
User name = j_smith,
  Password expiration     = 10/27/2007 11:01 (30 days from now),
  Password allow to be modified date     = 9/30/2007 10:59 (3 days from now),
  Account lockout     = Yes (Automatically unlocked after 19 minute(s)from now),
  Password bad attempts     = 3,
```

```
  END user profile        = u_profile1,
  Snmp allowed     = YES,
  Snmp authentication     = SHA,
  Snmp encryption     = DES
  Console-Only     = Disabled
User name = public,
  Password expiration     = 10/27/2007 11:01 (30 days from now),
  Password allow to be modified date     = 9/30/2007 10:59 (3 days from now),
  Account lockout     = None,
  Password bad attempts     = 0,
  Read Only for domains   = None,
  Read/Write for domains  = All ,
  Snmp allowed     = NO,
  Console-Only     = Disabled
User name = default (*),
  Password expiration     = 10/27/2007 11:01 (30 days from now),
  Password allow to be modified date     = 9/30/2007 10:59 (3 days from now),
  Account lockout     = None,
  Password bad attempts     = 0,
  Read Only for domains   = None,
  Read/Write for domains  = System Physical Layer2 Services policy Security ,
  Read/Write for families = file telnet dshell debug ip rip ospf bgp vrrp ip-rout-
ing ipx ipmr ipms ,
  Snmp allowed     = NO,
  Console-Only     = Disabled
(*)Note:
  The default user is not an active user account.
  It contains the default user account settings,
  for new user accounts.

-> show user j_smith
User name = j_smith,
  Password expiration     = 10/27/2007 11:01 (30 days from now),
  Password allow to be modified date     = 9/30/2007 10:59 (3 days from now),
  Account lockout     = Yes (Automatically unlocked after 19 minute(s)from now),
  Password bad attempts     = 3,
  END user profile        = u_profile1,
  Snmp allowed     = YES,
  Snmp authentication     = SHA,
  Snmp encryption     = DES
  Console-Only     = Disabled
```

output definitions

User name	The user name for this account.
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.)
Password allow to be modified date	The earliest date and time on which the user may change the password. Configured through the **user password-min-age** command.

output definitions (continued)

Account lockout	Indicates if the user account is locked out (**Yes** or **No**) and how many minutes remain until the user account is automatically unlocked. If no remaining time is displayed, the **admin** user or a user with admin privileges must manually unlock the account. Configured through the **user lockout-duration** and **user lockout unlock** commands.
Password bad attempts	The number of failed password login attempts for this user account.
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. This field does not display if an end-user profile is associated with the user account.
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. This field does not display if an end-user profile is associated with the user account.
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. This field does not display if an end-user profile is associated with the user account.
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. This field does not display if an end-user profile is associated with the user account.
END user profile	The name of an end-user profile associated with the user account. Configured through the **end-user profile** command. This field only displays if an end-user profile is associated with the user account.
Snmp allowed	Indicates whether or not the user is authorized to use SNMP (**YES** or **NO**). SNMP is allowed for the user account when SNMP authentication is specified for the account.
Snmp authentication	The level of SNMP authentication, if any, configured for the user. This field only displays if the user is authorized to use SNMP.
Snmp encryption	The level of SNMP encryption, if any, configured for the user. This field only displays if the user is authorized to use SNMP.
Console-Only	Displays whether the ability for the admin user to access the switch using only the console connection is enabled or disabled.

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 6.1; command was introduced.
Release 6.3.1; fields added for password policy and lockout status.
Release 6.4.3; Console-only parameter added.

Related Commands

user	Configures user entries in the local user database.
show user password-policy	Displays the global password policy configuration for the switch.
show user lockout-setting	Displays the global user lockout settings for the switch.

MIB Objects

```
aaaUserTable
   aaauUserName
   aaauPasswordExpirationDate
   aaauPasswordExpirationInMinute
   aaauPasswordAllowModifyDate
   aaauPasswordLockoutEnable
   aaauBadAttempts
   aaauReadRight1
   aaauReadRight2
   aaauWriteRight1
   aaauWriteRight2
   aaauEndUserProfile
   aaauSnmpLevel
   aaauSnmpAuthkey
aaaAsaConfig
   aaaAsaAccessPolicyAdminConsoleOnly
```

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 6400, 6850E, 6855, 9000E

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 6.1; command was introduced.

Related Commands

user password-size min	Configures the minimum number of characters required when configuring a user password.
user	Configures or modifies user entries in the local user database.
password	Configures the current user's password.
show user password-policy	Displays the global password policy configuration for the switch.

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 6400, 6850E, 6855, 9000E

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 6.1; 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.
show user password-policy	Displays the global password policy configuration for the switch.

MIB Objects

```
aaaAsaConfig
   aaaAsaDefaultPasswordExpirationInDays
```

show user password-policy

Displays the global password settings configured for the switch.

show user password-policy

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

The password policy contains parameter values that define configuration requirements for all passwords that are created on the switch. Use this command to display the current parameter values for the password policy.

Examples

```
-> show user password-policy
Password Policy:
Contain username flag: Enable
Minimum number of English uppercase characters: 6
Minimum number of English lowercase characters: 4
Minimum number of base-10 digit: 2
Minimum number of non-alphanumeric: 3
Minimum size: 8
Password history: 4
Password minimum age: 20 (days)
Password expiration: 40 (days)
```

output definitions

Contain username flag	Indicates if the username is included with the password check (**Enable** or **Disable**). Configured through the **user password-policy cannot-contain-username** command.
Minimum number of English uppercase characters	The minimum number of uppercase characters required in a password. Configured through the **user password-policy min-uppercase** command.
Minimum number of English lowercase characters	The minimum number of lowercase characters required in a password. Configured through the **user password-policy min-lowercase**.
Minimum number of base-10 digit	The minimum number of digits required in a password. Configured through the **user password-policy min-digit** command.
Minimum number of non-alphanumeric	The minimum number of non-alphanumeric characters required in a password. Configured through the **user password-policy min-nonalpha** command.

output definitions

Minimum size	The minimum number of characters required for the password size. Configured through the **user password-size min** command.
Password history	The maximum number of old passwords retained in the password history. Configured through the **user password-history** command.
Password minimum age	The number of days a password is protected from any modification. Configured through the **user password-min-age** command.
Password expiration	The default expiration date applied to all passwords. Configured through the **user password-expiration** command.

Release History

Release 6.3.1; command was introduced.

Related Commands

show user password-size	Displays the minimum number of characters that are required for a user password.
show user password-expiration	Displays the expiration date for passwords configured for user accounts stored on the switch.

MIB Objects

```
aaaAsaConfig
   aaaAsaPasswordContainUserName
   aaaAsaPasswordMinUpperCase
   aaaAsaPasswordMinLowerCase
   aaaAsaPasswordMinDigit
   aaaAsaPasswordMinNonAlpha
   aaaAsaPasswordHistory
   aaaAsaPasswordMinAge
   aaaAsaPasswordSizeMin
   aaaAsaDefaultPasswordExpirationInDays
```

show user lockout-setting

Displays the global user lockout settings for the switch.

show user lockout-setting

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

The global lockout settings include parameter values that determine the length of a user observation window, the amount of time a locked user remains locked, and the number of failed password login attempts allowed.

Examples

```
-> show user lockout-setting
Lockout Setting:
Observation window: 30 (minutes)
Duration: 200 (minutes)
Threshold: 20
```

output definitions

Observation window	The amount of time, in minutes, during which the number of failed password login attempts are counted. Configured through the **user lockout-window** command.
Duration	The amount of time, in minutes, that a locked user account remains locked out of the switch. Configured through the **user lockout-duration** command.
Threshold	The maximum number of failed password login attempts allowed before the user is locked out of the switch. Configured through the **user lockout-threshold** command.

Release History

Release 6.3.1; command was introduced.

Related Commands

user lockout unlock	Manually locks or unlocks a user account on the switch.
show user	Displays information about all users or a particular user configured in the local user database on the switch.

MIB Objects

```
aaaAsaConfig
   aaaAsaLockoutWindow
   aaaAsaLockoutDuration
   aaaAsaLockoutThreshold
```

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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 **aaa accounting command** command.
port bounding	Whether or not port mobility rules are allowed on Authenticated VLANs. Configured through the **avlan port-bound** command.

Release History

Release 6.1; command was introduced.

Related Commands

aaa avlan dns	Configures a host name.
aaa avlan default dhcp	Configures the gateway address for a DHCP server.
aaa accounting command	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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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 user-network-profile

Displays the User Network Profile (UNP) configuration for the switch.

show aaa user-network-profile

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show aaa user-network-profile
                                          Max           Max        Max
Role Name  Vlan  HIC  Policy List Name  Ingress-BW   Egress-BW  Default-Depth
----------+----+----+-----------------+-----------+------------+---------------
100down10up 50   No   list1             10.0M         100.0M      128K
50down50up  40   Yes  list1, list2      50.0M         50.0M       256K
```

output definitions

Role Name	The user profile name.
Vlan	The VLAN ID number the profile assigns to the user device.
HIC	Whether Host Integrity Check is enabled or disabled for the profile.
Policy List Name	The name of one or more QoS policy lists that are applied to the device to which this profile is assigned.
Max Ingress-BW	Maximum ingress bandwidth associated to UNP.
Max Egress-BW	Maximum egress bandwidth associated to UNP.
Max Default Depth	Maximum default bandwidth associated to UNP.

Release History

Release 6.3.1; command was introduced.
Release 6.3.4; **HIC** and **Policy List Name** fields added.
Release 6.4.5; **Max Ingress-BW**, **Max Egress-BW,** and **Max Default-Depth** fields added.

Related Commands

aaa user-network-profile	Creates the user role in the user network profile table and maps the role to a VLAN ID.

MIB Objects

```
aaaUserNetProfileTable
   aaaUserNetProfileName
   aaaUserNetProfileVlanID
   aaaUserNetProfileHICflag
   aaaUserNetProfileQosPolicyListName
   aaaUserNetProfileMaxIngressBw
   aaaUserNetProfileMaxEgressBw
   aaaUserNetProfileMaxDefaultDepth
```

show aaa classification-rule

Displays the User Network Profile (UNP) mobile classification rule configuration for the switch.

show aaa classification-rule {mac-rule | mac-range-rule | ip-net-rule}

Syntax Definitions

mac-rule	Displays MAC address rules.
mac-range-rule	Displays MAC address range rules.
ip-net-rule	Displays IP network address rules.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855

Usage Guidelines

- Specifying a rule type parameter (**mac-rule**, **mac-range-rule**, **ip-net-rule**) is required with this command.
- UNP mobile rules take precedence over VLAN mobile rules.

Examples

```
-> show aaa classification-rule mac-rule

MAC Address        User Network Profile Name
------------------+-------------------------
00:1a:a0:b1:fa:e5  guest_user
00:b0:d0:2a:0e:2e  acct_user
00:b0:d0:2a:11:60  engr_user
```

output definitions

MAC Address	The source MAC address of the host device to which the UNP is applied.
User Network Profile Name	The name of the UNP applied to the host device.

```
-> show aaa classification-rule mac-range-rule

Low MAC Address    High MAC Address  User Network Profile Name
------------------+-----------------+------------------------
00:1a:a0:b1:fa:10  00:1a:0a:b1:fa:20  guest_user
00:b0:d0:2a:0e:2e  00:b0:d0:2a:0e:3a  acct_user
00:b0:d0:2a:11:60  00:b0:d0:2a:11:70  engr_user
```

output definitions

Low MAC Address	The MAC address that identifies the low end of the range of addresses.
High MAC Address	The MAC address that identifies the high end of the range of addresses.
User Network Profile Name	The name of the UNP applied to the host device.

```
-> show aaa classification-rule ip-net-rule

IP Addr             IP Mask           User Network Profile Name
--------------------+-----------------+-------------------------
198.4.21.1          255.255.0.0       guest_user
10.1.1.1            255.0.0.0         acct_user
20.2.2.1            255.0.0.0         engr_user
```

output definitions

IP Addr	The source IP address of the host device to which the UNP is applied.
IP Mask	The subnet mask for the IP address.
User Network Profile Name	The name of the UNP applied to the host device.

Release History

Release 6.3.4; command was introduced.

Related Commands

aaa classification-rule mac-address	Defines a MAC address classification rule and associates that rule with a user network profile.
aaa classification-rule mac-address-range	Defines a MAC address classification rule that specifies a range of MAC addresses for classification and associates the range of addresses with a user network profile.
aaa classification-rule ip-address	Defines an IP network address classification rule and associates the rule with a user network profile.

MIB Objects

```
aaaUNPMacRuleTable
   aaaUNPMacRuleAddr
   aaaUNPMacRule
   aaaUNPMacRuleProfileName
aaaUNPMacRangeRuleTable
   aaaUNPMacRangeRuleLoAddr
   aaaUNPMacRangeRuleHiAddr
   aaaUNPMacRangeRuleProfileName
aaaUNPIpNetRuleTable
   aaaUNPIpNetRuleAddr
   aaaUNPIpNetRuleMask
   aaaUNPIpNetRuleProfileName
```

show aaa hic

Displays the global Host Integrity Check (HIC) configuration for the switch.

show aaa hic

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

N/A

Examples

```
-> show aaa hic
HIC Global Status: Enabled
HIC Web Agent Download URL: http://100.100.100.100:8080/CGAgentLauncher.htm
HIC Host Custom HTTP Proxy Port: 8383
HIC Background Poll interval: 32
HIC Server-fail-mode: Hold
```

output definitions

HIC Status	The HIC status for the switch (**Enabled** or **Disabled**). Configured through the **aaa hic** command.
HIC Web Agent Download URL	The URL for the web agent download server. Configured through the **aaa hic web-agent-url** command.
HIC Host Custom HTTP Proxy Port	The proxy port number used when the web-based host is redirected to the HIC server. Configured through the **aaa hic custom-proxy-port** command.
HIC Background Poll Interval	The URL for the web agent download server. Configured through the **aaa hic redundancy background-poll-interval** command.
HIC Server-fail-mode	The server background poll interval. Configured through the **aaa hic server-failure mode** command.

Release History

Release 6.3.4; command was introduced.
Release 6.4.4; **Background Poll inteval** and **Server-fail-mode** added.

Related Commands

show aaa hic host	Displays a list of the learned host MAC addresses and the HIC status for each host.
show aaa hic server	Displays the HIC server configuration for the switch.
show aaa hic server-failure policy	Displays the list of servers allowed access to the switch and host device as part of the HIC process.

MIB Objects

```
aaaHicConfigInfo
   aaaHicStatus
   aaaHicWebAgentDownloadUrl
   aaaHicCustomHttpProxyPort
   aaaHicBgPollInterval
   aaaHicSrvFailMode
```

show aaa hic host

Displays a list of the learned host MAC addresses and the HIC status for each host.

show aaa hic host

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855

Usage Guidelines

N/A

Examples

```
-> show aaa hic host
  HIC Host MAC           Status
--------------------+--------------
00:1a:a0:b1:fa:e5      Successful
00:b0:d0:2a:0e:2e      Failed
00:b0:d0:2a:11:60      Successful
```

output definitions

HIC Host MAC	The MAC address for each learned host device.
Status	The HIC status for the host device (**In-Progress**, **Successful**, **Failed**, or **Timeout**).

Release History

Release 6.3.4; command was introduced.

Related Commands

show aaa hic	Displays the global HIC configuration for the switch.
show aaa hic server	Displays the HIC server configuration for the switch.
show aaa hic server-failure policy	Displays the list of servers allowed access to the switch and host device as part of the HIC process.

MIB Objects

```
aaaHicHostTable
   aaaHicHostMac
   aaaHicHostStatus
```

show aaa hic server

Displays the HIC server configuration for the switch.

show aaa hic server

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

A Primary and Backup HIC server can be configured per switch.

Examples

```
-> show aaa hic server

-> show aaa hic server
Server                                          Server   Server       Server
Name               IP Address      UDP Port     Role     Connection   Status
----------------+-----------------+---------+---------+------------+---------
           hic1     172.18.16.200     11707   Primary       Active     Down
           hic2     172.18.16.232     11707   Backup      Inactive     Down
```

output definitions

HIC Server Name	The name of the HIC server. Note that only one server is supported per switch. Configured through the **aaa hic server-name** command.
HIC Server IP Address	The IP address of the HIC server. Configured through the **aaa hic server-name** command.
HIC server UDP Port	The UDP port number. Configured through the **aaa hic server-name** command.
HIC Server Role	The role of this server; primary or backup. Configured through the **aaa hic server-name** command.
HIC Server Connection	The server connection status; active or inactive.
HIC Server Status:	The server status; up or down.

Release History

Release 6.3.4; command was introduced.
Release 6.4.4; **Role**, **Status**, and **Connection** parameters added.

Related Commands

show aaa hic	Displays the global HIC configuration for the switch.
show aaa hic host	Displays a list of the learned host MAC addresses and the HIC status for each host.
show aaa hic server-failure policy	Displays the list of servers allowed access to the switch and host device as part of the HIC process.

MIB Objects

```
aaaHicSvrTable
   aaaHicSvrName
   aaaHicSvrIpAddr
   aaaHicSvrRole
   aaaHicSvrConnection
   aaaHicSvrPort
```

show aaa hic server-failure policy

Displays the HIC server failure mode and UNP mapping.

show aaa hic server-failure policy

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

N/A

Examples

```
-> show aaa hic server-failure policy
    Mode: Hold
         UNP Source                      UNP Destination
-----------------------------------+-----------------------------------
unp1                               unp2
```

output definitions

Mode	The HIC Server Failure Mode; Hold or Pass-Through.
UNP Source	The current UNP of the users.
UNP Destination	The UNP that the users will be moved to if both HIC servers are unavailable.

Release History

Release 6.4.4; command was introduced.

Related Commands

aaa hic server-name	Configures the HIC server.

MIB Objects

```
aaaHicSvrDownUnpMapTable
   aaaHicSvrDownUnpMapEntry
   aaaHicSvrDownUnpName
   aaaHicSvrDownMappedUnpName
   aaaHicSvrDownUnpRowStatus
aaaHicConfigInfoTable
   aaaHicSrvFailMode
```

show aaa hic allowed

Displays the Host Integrity Check (HIC) server exception list. The servers included in this list are exempt from the HIC process. This allows a host device to access these servers for compliance and remediation purposes.

show aaa hic allowed

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855

Usage Guidelines

The HIC server exception list may contain up to 16 servers per switch.

Examples

```
-> show aaa hic allowed
          Allowed Name              IP Address         IP Mask
--------------------------------+----------------+-----------------
rem1_srv                         3.3.3.3           255.0.0.0
```

output definitions

Allowed Name	The name of the server that is allowed access to the switch and host as part of the HIC process. Configured through the **aaa hic redundancy background-poll-interval** command.
IP Address	The IP address of the allowed server. Configured through the **aaa hic redundancy background-poll-interval** command.
IP Mask	The IP subnet mask for the allowed server. Configured through the **aaa hic redundancy background-poll-interval** command.

Release History

Release 6.3.4; command was introduced.

Related Commands

show aaa hic	Displays the global HIC configuration for the switch.
show aaa hic host	Displays a list of the learned host MAC addresses and the HIC status for each host.
show aaa hic server	Displays the HIC server configuration for the switch.

MIB Objects

```
aaaHicAllowedTable
   aaaHicAllowedName
   aaaHicAllowedIpAddr
   aaaHicAllowedIpMask
```

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 6400, 6850E, 6855, 9000E

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 6.1; command was introduced.

Related Commands

user	Configures or modifies user entries in the local user database.

show aaa-device all-users

Displays the Access Guardian status of all users learned on 802.1x ports.

show aaa-device all-users [unp *profile_name* **| policy** *device_policy* **| authentication-status [success | fail]] [port** *slot/port***]**

Syntax Definitions

profile_name	The name of a user network profile.
device_policy	The type of Access Guardian device classification policy.
success	Display all users that have successfully authenticated.
fail	Display all users that have failed authentication.
slot/port	The slot and port number designation for a specific switch port.

Defaults

If none of the optional parameters are specified with this command, all users learned on all 802.1x ports are displayed by default.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **unp** *profile_name* parameter to display only those users associated with a specific user network profile.
- Use the **policy** *device_policy* parameter to display only those users authenticated with one of the device classification policy types. To specify which policy to use with this command, enter one of the following types for the *device_policy* parameter value:

policy type
vlan
user-network-profile
group mobility
default-vlan
captive-portal
authentication

- Use the **authentication success** or **authentication fail** parameters to display only those users that have either passed or failed authentication.
- Use the **port** *slot/port* parameter to display only those users learned on a specific port. Note that it is also possible to combine this parameter with any of the other **show aaa-device all-users** command parameters.

Examples

```
-> show aaa-device all-users

Slot  MAC               User            Addr IP       Authentication User Network
Port  Address           Name       VLAN Mode Address     Type Result Profile Name
---+-----------------+-----------+----+----+------------+---+----+-------------
1/1 00:11:50:a6:12:00  User101     100  Brdg 10.133.0.100 1X  Pass Marketing
1/1 00:11:50:a6:12:01  User101     100  Brdg 10.133.0.101 1X  Pass Marketing
1/1 00:11:50:a6:12:02  User101     100  Brdg 10.133.0.102 1X  Pass Marketing
1/1 00:11:50:a6:12:03  User101     100  Brdg 10.133.0.103 1X  Pass Marketing
1/1 00:1a:50:a6:12:50  --          100  Blk  10.133.2.128 None N/A engr_no_internet
1/1 00:1a:50:a6:12:51  --          100  Blk  10.133.2.129 None N/A engr_no_internet
1/1 00:1a:50:a6:12:52  --          100  Blk  10.133.2.130 None N/A engr_no_internet
1/1 00:1a:50:a6:12:53  --          100  Blk  10.133.2.131 None N/A engr_no_internet

Slot  MAC               User            Addr IP       Authentication User Network
Port  Address           Name       VLAN Mode Address     Type Result Profile Name
---+-----------------+-----------+----+----+------------+---+----+-------------
1/2 00:00:39:47:4f:0c  pc2006      1000 Brdg -            1X  Pass  Marketing
1/2 00:b0:d0:77:fa:72  --          1000 Brdg -            MAC Pass  Marketing

Slot  MAC               User            Addr IP       Authentication User Network
Port  Address           Name       VLAN Mode Address     Type Result Profile Name
---+-----------------+-----------+----+----+------------+---+----+-------------
5/9 00:90:27:17:91:a8  pc2006     1000  Brdg  -           1X  Pass  engr
5/9 00:00:39:93:46:0c  --            1  Blk   -           MAC Fail  -

-> show aaa-device all-users unp Marketing

Slot  MAC               User              Addr IP       Authentication User Network
Port  Address           Name         VLAN Mode Address     Type Result Profile Name
---+-----------------+-----------+----+----+------------+---+----+------------
1/1 00:11:50:a6:12:00  User101     100  Brdg 10.133.0.100 1X  Pass Marketing
1/1 00:11:50:a6:12:01  User101     100  Brdg 10.133.0.101 1X  Pass Marketing
1/1 00:11:50:a6:12:02  User101     100  Brdg 10.133.0.102 1X  Pass Marketing
1/1 00:11:50:a6:12:03  User101     100  Brdg 10.133.0.103 1X  Pass Marketing

Slot  MAC               User            Addr IP       Authentication User Network
Port  Address           Name       VLAN Mode Address     Type Result Profile Name
---+-----------------+-----------+----+----+------------+---+----+-------------
1/2 00:00:39:47:4f:0c  pc2006      1000 Brdg -            1X  Pass  Marketing
1/2 00:b0:d0:77:fa:72  --          1000 Brdg -            MAC Pass  Marketing

-> show aaa-device all-users unp Marketing port 1/2

Slot  MAC               User            Addr IP       Authentication User Network
Port  Address           Name       VLAN Mode Address     Type Result Profile Name
---+-----------------+-----------+----+----+------------+---+----+-------------
1/2 00:00:39:47:4f:0c  pc2006      1000 Brdg -            1X  Pass  Marketing
1/2 00:b0:d0:77:fa:72  --          1000 Brdg -            MAC Pass  Marketing

-> show aaa-device all-users port 5/9

Slot  MAC               User            Addr IP       Authentication User Network
Port  Address           Name       VLAN Mode Address     Type Result Profile Name
---+-----------------+-----------+----+----+------------+---+----+-------------
5/9 00:90:27:17:91:a8  pc2006     1000  Brdg  -           1X  Pass  engr
5/9 00:00:39:93:46:0c  --            1  Blk   -           MAC Fail  -
```

output definitions

Slot/Port	The slot and port number to which the user device is connected.
MAC Address	The MAC address of the user device.
User Name	The user login name used to access the switch.
VLAN	The VLAN ID the user device is authorized to access.
Addr Mode	The status of the MAC address for the user device.
Ip Address	The IP address of the user device.
Authentication Type	The type of authentication used to grant the device access to the switch (**1X**, **MAC**, or **none**).
Authentication Result	The result of the authentication process (**Pass**, **Fail**, or **N/A**).
User Network Profile Name	The name of the user network profile used to classify the user device. If **N/A** appears in this field, there is no user network profile associated with this device.

Release History

Release 6.3.4; command was introduced.

Related Commands

show aaa-device supplicant-users	Displays a list of all supplicant (802.1x) users learned on the switch.
show aaa-device non-supplicant-users	Displays a list of all non-supplicant (non-802.1X) users learned on the switch.
show aaa-device captive-portal-users	Displays a list of users that were classified using Captive Portal browser-based authentication.

MIB Objects

```
alaDot1xDeviceStatusTable
   alaDot1xDeviceStatusMacQueryType
   alaDot1xDeviceStatusSlotNumber
   alaDot1xDeviceStatusPortNumber
   alaDot1xDeviceStatusMacAddress
   alaDot1xDeviceStatusDeviceType
   alaDot1xDeviceStatusVlan
   alaDot1xDeviceStatusIpAddress
   alaDot1xDeviceStatusUserName
   alaDot1xDeviceStatusProfileUsed
   alaDot1xDeviceStatusAuthType
   alaDot1xDeviceStatusPolicyUsed
   alaDot1xDeviceStatusAuthResult
   alaDot1xDeviceStatusMacLearntState
   alaDot1xDeviceStatusTimeLearned
   alaDot1xDeviceStatusCaptivePortalUsed
```

show aaa-device supplicant-users

Displays the Access Guardian status of all supplicant (802.1x) users learned on the switch.

show aaa-device supplicant-users [unp *profile_name* **| policy** *device_policy* **| authentication-status [success | fail]] [port** *slot/port***]**

Syntax Definitions

profile_name	The name of a user network profile.
device_policy	The type of Access Guardian device classification policy.
success	Display all supplicant users that have successfully authenticated.
fail	Display all supplicant users that have failed authentication.
slot/port	The slot and port number designation for a specific switch port.

Defaults

If none of the optional parameters are specified with this command, all supplicant users are displayed by default.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **unp** *profile_name* parameter to display only those users associated with a specific user network profile.
- Use the **policy** *device_policy* parameter to display only those users authenticated with one of the device classification policy types. To specify which policy to use with this command, enter one of the following types for the *device_policy* parameter value:

policy type
vlan
user-network-profile
group mobility
default-vlan
captive-portal
authentication

- Use the **authentication success** or **authentication fail** parameters to display only those users that have either passed or failed authentication.
- Use the **port** *slot/port* parameter to display only those users learned on a specific port. Note that it is also possible to combine this parameter with any of the other **show aaa-device supplicant-users** command parameters.

Examples

```
-> show aaa-device supplicant-users

Slot  MAC               User            Addr IP       Authentication User Network
Port  Address           Name       VLAN Mode Address     Type Result Profile Name
---+-----------------+-----------+----+----+------------+---+----+--------------
1/1 00:11:50:a6:12:00  User101     100  Brdg 10.133.0.100 1X  Pass Marketing
1/1 00:11:50:a6:12:01  User101     100  Brdg 10.133.0.101 1X  Pass Marketing
1/1 00:11:50:a6:12:02  User101     100  Brdg 10.133.0.102 1X  Pass Marketing
1/1 00:11:50:a6:12:03  User101     100  Brdg 10.133.0.103 1X  Pass Marketing

Slot  MAC               User            Addr IP       Authentication User Network
Port  Address           Name       VLAN Mode Address     Type Result Profile Name
---+-----------------+-----------+----+----+------------+---+----+--------------
1/2 00:00:39:47:4f:0c  pc2006      1000 Brdg -            1X  Pass  Marketing

Slot  MAC               User            Addr IP       Authentication User Network
Port  Address           Name       VLAN Mode Address     Type Result Profile Name
---+-----------------+-----------+----+----+------------+---+----+--------------
5/9 00:90:27:17:91:a8  pc2006     1000  Brdg  -           1X  Pass engr
5/9 00:00:39:93:46:10  --            1  Blk   -           1X  Fail -

-> show aaa-device supplicant-users port 5/9

Slot  MAC               User            Addr IP       Authentication User Network
Port  Address           Name       VLAN Mode Address     Type Result Profile Name
---+-----------------+-----------+----+----+------------+---+----+--------------
5/9 00:90:27:17:91:a8  pc2006     1000  Brdg  -           1X  Pass engr
5/9 00:00:39:93:46:10  --            1  Blk   -           1X  Fail -

-> show aaa-device supplicant-users authentication-status fail

Slot  MAC               User            Addr IP       Authentication User Network
Port  Address           Name       VLAN Mode Address     Type Result Profile Name
---+-----------------+-----------+----+----+------------+---+----+------------
5/9 00:00:39:93:46:10  --            1  Blk   -           1X  Fail -
```

output definitions

Slot/Port	The slot and port number to which the user device is connected.
MAC Address	The MAC address of the user device.
User Name	The user login name used to access the switch.
VLAN	The VLAN ID the user device is authorized to access.
Addr Mode	The status of the MAC address for the user device.
Ip Address	The IP address of the user device.
Authentication Type	The type of authentication used to grant the device access to the switch (**1X**, **MAC**, or **none**).
Authentication Result	The result of the authentication process (**Pass**, **Fail**, or **N/A**).
User Network Profile Name	The name of the user network profile used to classify the user device. If **N/A** appears in this field, there is no user network profile associated with this device.

Release History

Release 6.3.4; command was introduced.

Related Commands

show aaa-device all-users	Displays a list of all users (supplicant and non-supplicant) learned on the switch.
show aaa-device non-supplicant-users	Displays a list of all non-supplicant (non-802.1X) users learned on the switch.
show aaa-device captive-portal-users	Displays a list of users that were classified using Captive Portal browser-based authentication.

MIB Objects

```
alaDot1xDeviceStatusTable
   alaDot1xDeviceStatusMacQueryType
   alaDot1xDeviceStatusSlotNumber
   alaDot1xDeviceStatusPortNumber
   alaDot1xDeviceStatusMacAddress
   alaDot1xDeviceStatusDeviceType
   alaDot1xDeviceStatusVlan
   alaDot1xDeviceStatusIpAddress
   alaDot1xDeviceStatusUserName
   alaDot1xDeviceStatusProfileUsed
   alaDot1xDeviceStatusAuthType
   alaDot1xDeviceStatusPolicyUsed
   alaDot1xDeviceStatusAuthResult
   alaDot1xDeviceStatusMacLearntState
   alaDot1xDeviceStatusTimeLearned
   alaDot1xDeviceStatusCaptivePortalUsed
```

show aaa-device non-supplicant-users

Displays the Access Guardian status of all non-supplicant (non-802.1x) users learned on the switch.

show aaa-device non-supplicant-users [unp *profile_name* **| policy** *device_policy* **| authentication-status [success | fail]] [port** *slot/port***]**

Syntax Definitions

profile_name	The name of a user network profile.
device_policy	The type of Access Guardian device classification policy.
authentication success	Display all non-supplicant users that have successfully authenticated.
authentication fail	Display all non-supplicant users that have failed authentication.
slot/port	The slot and port number designation for a specific switch port.

Defaults

If none of the optional parameters are specified with this command, all non-supplicant users are displayed by default.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **unp** *profile_name* parameter to display only those users associated with a specific user network profile.
- Use the **policy** *device_policy* parameter to display only those users authenticated with one of the device classification policy types. To specify which policy to use with this command, enter one of the following types for the *device_policy* parameter value:

policy type
vlan
user-network-profile
group mobility
default-vlan
captive-portal
authentication

- Use the **authentication success** or **authentication fail** parameters to display only those users that have either passed or failed authentication.
- Use the **port** *slot/port* parameter to display only those users learned on a specific port. Note that it is also possible to combine this parameter with any of the other **show aaa-device non-supplicant-users** command parameters.

Examples

```
-> show aaa-device non-supplicant-users

Slot  MAC               User            Addr IP       Authentication User Network
Port  Address           Name       VLAN Mode Address     Type Result Profile Name
---+-----------------+-----------+----+----+------------+---+----+-------------
1/1 00:1a:50:a6:12:50  --          100  Blk  10.133.2.128 None N/A engr_no_internet
1/1 00:1a:50:a6:12:51  --          100  Blk  10.133.2.129 None N/A engr_no_internet
1/1 00:1a:50:a6:12:52  --          100  Blk  10.133.2.130 None N/A engr_no_internet
1/1 00:1a:50:a6:12:53  --          100  Blk  10.133.2.131 None N/A engr_no_internet

Slot  MAC               User            Addr IP       Authentication User Network
Port  Address           Name       VLAN Mode Address     Type Result Profile Name
---+-----------------+-----------+----+----+------------+---+----+-------------
1/2 00:b0:d0:77:fa:72  --          1000 Brdg -            MAC Pass  Marketing

Slot  MAC               User            Addr IP       Authentication User Network
Port  Address           Name       VLAN Mode Address     Type Result Profile Name
---+-----------------+-----------+----+----+------------+---+----+-------------
5/9 00:90:27:17:91:20  pc2006     1000  Brdg  -           MAC Pass  engr
5/9 00:00:39:93:46:0c  --            1  Blk   -           MAC Fail  -

-> show aaa-device non-supplicant-users unp engr_no_internet

Slot  MAC               User              Addr IP       Authentication User Network
Port  Address           Name         VLAN Mode Address     Type Result Profile Name
---+-----------------+-----------+----+----+------------+---+----+------------
1/1 00:1a:50:a6:12:50  --          100  Blk  10.133.2.128 None N/A engr_no_internet
1/1 00:1a:50:a6:12:51  --          100  Blk  10.133.2.129 None N/A engr_no_internet
1/1 00:1a:50:a6:12:52  --          100  Blk  10.133.2.130 None N/A engr_no_internet
1/1 00:1a:50:a6:12:53  --          100  Blk  10.133.2.131 None N/A engr_no_internet

-> show aaa-device non-supplicant-users authentication-status success

Slot  MAC               User            Addr IP       Authentication User Network
Port  Address           Name       VLAN Mode Address     Type Result Profile Name
---+-----------------+-----------+----+----+------------+---+----+-------------
1/2 00:b0:d0:77:fa:72  --          1000 Brdg -            MAC Pass  Marketing

Slot  MAC               User            Addr IP       Authentication User Network
Port  Address           Name       VLAN Mode Address     Type Result Profile Name
---+-----------------+-----------+----+----+------------+---+----+-------------
5/9 00:90:27:17:91:20  pc2006     1000  Brdg  -           MAC Pass  engr
```

output definitions

Slot/Port	The slot and port number to which the user device is connected.
MAC Address	The MAC address of the user device.
User Name	The user login name used to access the switch.
VLAN	The VLAN ID the user device is authorized to access.
Addr Mode	The status of the MAC address for the user device.
Ip Address	The IP address of the user device.
Authentication Type	The type of authentication used to grant the device access to the switch (**1X**, **MAC**, or **none**).

output definitions

Authentication Result	The result of the authentication process (**Pass**, **Fail**, or **N/A**).
User Network Profile Name	The name of the user network profile used to classify the user device. If **N/A** appears in this field, there is no user network profile associated with this device.

Release History

Release 6.3.4; command was introduced.

Related Commands

show aaa-device all-users	Displays a list of all users (supplicant and non-supplicant) learned on the switch.
show aaa-device supplicant-users	Displays a list of all supplicant (802.1X) users learned on the switch.
show aaa-device captive-portal-users	Displays a list of users that were classified using Captive Portal browser-based authentication.

MIB Objects

```
alaDot1xDeviceStatusTable
   alaDot1xDeviceStatusMacQueryType
   alaDot1xDeviceStatusSlotNumber
   alaDot1xDeviceStatusPortNumber
   alaDot1xDeviceStatusMacAddress
   alaDot1xDeviceStatusDeviceType
   alaDot1xDeviceStatusVlan
   alaDot1xDeviceStatusIpAddress
   alaDot1xDeviceStatusUserName
   alaDot1xDeviceStatusProfileUsed
   alaDot1xDeviceStatusAuthType
   alaDot1xDeviceStatusPolicyUsed
   alaDot1xDeviceStatusAuthResult
   alaDot1xDeviceStatusMacLearntState
   alaDot1xDeviceStatusTimeLearned
   alaDot1xDeviceStatusCaptivePortalUsed
```

show aaa-device captive-portal-users

Displays the Access Guardian status of all users that attempted network access through the switch using Captive Portal web-based authentication.

show aaa-device captive-portal-users [unp *profile_name* **| policy** *device_policy* **| authentication-status [success | fail]] [port** *slot/port***]**

Syntax Definitions

profile_name	The name of a user network profile.
device_policy	The type of Access Guardian device classification policy.
authentication success	Display all non-supplicant users that have successfully authenticated.
authentication fail	Display all non-supplicant users that have failed authentication.
slot/port	The slot and port number designation for a specific switch port.

Defaults

If none of the optional parameters are specified with this command, all Captive Portal users are displayed by default.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **unp** *profile_name* parameter to display only those users associated with a specific user network profile.
- Use the **policy** *device_policy* parameter to display only those users authenticated with one of the device classification policy types. To specify which policy to use with this command, enter one of the following types for the *device_policy* parameter value:

policy type
vlan
user-network-profile
group mobility
default-vlan
captive-portal
authentication

- Use the **authentication success** or **authentication fail** parameters to display only those users that have either passed or failed authentication.
- Use the **port** *slot/port* parameter to display only those users learned on a specific port. Note that it is also possible to combine this parameter with any of the other **show aaa-device captive-portal-users** command parameters.

Examples

```
-> show aaa-device captive-portal-users

Slot  MAC               User            Addr IP       Authentication User Network
Port  Address           Name       VLAN Mode Address     Type Result Profile Name
---+-----------------+-----------+----+----+------------+---+----+-------------
1/1 00:11:50:a6:12:00  User101     100  Brdg 10.133.0.100 1X  Pass Marketing
1/1 00:11:50:a6:12:01  User101     100  Brdg 10.133.0.101 1X  Pass Marketing
1/1 00:11:50:a6:12:02  User101     100  Brdg 10.133.0.102 1X  Pass Marketing
1/1 00:11:50:a6:12:03  User101     100  Brdg 10.133.0.103 1X  Pass Marketing

Slot  MAC               User            Addr IP       Authentication User Network
Port  Address           Name       VLAN Mode Address     Type Result Profile Name
---+-----------------+-----------+----+----+------------+---+----+-------------
1/2 00:00:39:47:4f:0c  pc2006      1000 Brdg -            1X  Pass  Marketing
1/2 00:b0:d0:77:fa:72  --          1000 Brdg -            MAC Pass  Marketing

Slot  MAC               User            Addr IP       Authentication User Network
Port  Address           Name       VLAN Mode Address     Type Result Profile Name
---+-----------------+-----------+----+----+------------+---+----+-------------
5/9 00:90:27:17:91:a8  pc2006      1000 Brdg  -           1X  Pass  engr
5/9 00:00:39:93:46:0c  --            1  Blk   -           MAC Fail  -

-> show aaa-device captive-portal-users unp Marketing

Slot  MAC               User              Addr IP       Authentication User Network
Port  Address           Name       VLAN Mode Address     Type Result Profile Name
---+-----------------+-----------+----+----+------------+---+----+------------
1/1 00:11:50:a6:12:00  User101     100  Brdg 10.133.0.100 1X  Pass Marketing
1/1 00:11:50:a6:12:01  User101     100  Brdg 10.133.0.101 1X  Pass Marketing
1/1 00:11:50:a6:12:02  User101     100  Brdg 10.133.0.102 1X  Pass Marketing
1/1 00:11:50:a6:12:03  User101     100  Brdg 10.133.0.103 1X  Pass Marketing

Slot  MAC               User            Addr IP       Authentication User Network
Port  Address           Name       VLAN Mode Address     Type Result Profile Name
---+-----------------+-----------+----+----+------------+---+----+-------------
1/2 00:00:39:47:4f:0c  pc2006      1000 Brdg -            1X  Pass  Marketing
1/2 00:b0:d0:77:fa:72  --          1000 Brdg -            MAC Pass  Marketing

-> show aaa-device captive-portal-users policy vlan

Slot  MAC               User            Addr IP       Authentication User Network
Port  Address           Name       VLAN Mode Address     Type Result Profile Name
---+-----------------+-----------+----+----+------------+---+----+-------------
1/2 00:00:39:47:4f:0c  pc2006      1000 Brdg -            1X  Pass  Marketing
1/2 00:b0:d0:77:fa:72  --          1000 Brdg -            MAC Pass  Marketing

Slot  MAC               User            Addr IP       Authentication User Network
Port  Address           Name       VLAN Mode Address     Type Result Profile Name
---+-----------------+-----------+----+----+------------+---+----+-------------
5/9 00:90:27:17:91:a8  pc2006      1000 Brdg  -           1X  Pass  engr
5/9 00:00:39:93:46:0c  --            1  Blk   -           MAC Fail  -
```

output definitions

Slot/Port	The slot and port number to which the user device is connected.
MAC Address	The MAC address of the user device.

output definitions

User Name	The user login name used to access the switch.
VLAN	The VLAN ID the user device is authorized to access.
Addr Mode	The status of the MAC address for the user device.
Ip Address	The IP address of the user device.
Authentication Type	The type of authentication used to grant the device access to the switch (**1X**, **MAC**, or **none**).
Authentication Result	The result of the authentication process (**Pass**, **Fail**, or **N/A**).
User Network Profile Name	The name of the user network profile used to classify the user device. If **N/A** appears in this field, there is no user network profile associated with this device.

Release History

Release 6.3.4; command was introduced.

Related Commands

show aaa-device all-users	Displays a list of all users (supplicant and non-supplicant) learned on the switch.
show aaa-device supplicant-users	Displays a list of all supplicant (802.1X) users learned on the switch.
show aaa-device non-supplicant-users	Displays a list of all non-supplicant (non-802.1X) users learned on the switch.

MIB Objects

```
alaDot1xDeviceStatusTable
   alaDot1xDeviceStatusMacQueryType
   alaDot1xDeviceStatusSlotNumber
   alaDot1xDeviceStatusPortNumber
   alaDot1xDeviceStatusMacAddress
   alaDot1xDeviceStatusDeviceType
   alaDot1xDeviceStatusVlan
   alaDot1xDeviceStatusIpAddress
   alaDot1xDeviceStatusUserName
   alaDot1xDeviceStatusProfileUsed
   alaDot1xDeviceStatusAuthType
   alaDot1xDeviceStatusPolicyUsed
   alaDot1xDeviceStatusAuthResult
   alaDot1xDeviceStatusMacLearntState
   alaDot1xDeviceStatusTimeLearned
   alaDot1xDeviceStatusCaptivePortalUsed
```

802.1x kerberos

Enable or disable Kerberos snooping on an 802.1x port.

802.1x *slot/port* **kerberos {enable | disable}**

Syntax Definitions

enable	Enable Kerberos snooping on the specified 802.1x port .
disable	Disable Kerberos snooping on the specified 802.1x port.
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).

Defaults

By default, Kerberos is disabled on 802.1x ports.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Kerberos snooping is supported only on 802.1x ports with non-supplicant users.
- Kerberos can be enabled only when at least one authentication server and one Kerberos enabled port is configured on the switch.
- All Kerberos parameters are configurable irrespective of the per port status (enable/disable) of Kerberos snooping.
- If Kerberos is disabled on a specific 802.1x port, then all the Kerberos users learned on that port are removed from Kerberos user database and the corresponding QoS policies are also removed.
- If 802.1x is disabled on the Kerberos enabled port, then Kerberos is disabled and all the Kerberos users learned on that port are removed from the switch. If 802.1 x is enabled on the same port, then Kerberos has to be enabled on that port explicitly. Kerberos is not automatically enabled on the port.
- Maximum number of Kerberos users that can be learned on sthe witch is 1000.

Examples

```
-> 802.1x 1/1 kerberos enable
-> 802.1x 1/1 kerberos disable
```

Release History

Release 6.4.5; command introduced.

Related Commands

show aaa kerberos configuration	Displays Kerberos global configuration.
show aaa kerberos port	Displays Kerberos status of a port or range of ports.
show aaa kerberos users	Displays the learnt Kerberos users information.
show aaa kerberos statistics	Displays the global Kerberos statistics.
show aaa kerberos port statistics	Displays the Kerberos statistics on a port.
clear aaa kerberos statistics	Clears global Kerberos statistics.
clear aaa kerberos port statistics	Clears port level Kerberos statistics.

MIB Objects

```
alaKerberosPortTable
   alaKerberosPortIfIndex
   alaKerberosPortStatus
```

aaa kerberos mac-move

Enable or disable MAC move globally on the switch.

aaa kerberos mac-move {enable | disable}

Syntax Definitions

enable	Enable MAC move globally on the switch.
disable	Disable MAC move globally on the switch.

Defaults

By default, MAC move is enabled.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

There is no support for multiple users on the same MAC address. For the same MAC address, a new Kerberos authentication will overwrite the existing entry in the Kerberos Database.

Examples

```
-> aaa kerberos mac-move enable
-> aaa kerberos mac-move disable
```

Release History

Release 6.4.5; command introduced.

Related Commands

802.1x kerberos	Enable or disable Kerberos snooping on a 802.1x port.
aaa kerberos inactivity-timer	Configures global inactivity timer on the switch for Kerberos users.
show aaa kerberos configuration	Displays Kerberos global configuration.

MIB Objects

```
alaKerberosGlobalMacMoveStatus
```

aaa kerberos inactivity-timer

Configures global inactivity timer on the switch for Kerberos users.

aaa kerberos inactivity-timer *num*

Syntax Definitions

mins	Time interval in minutes in the range 10 minutes to 600 minutes.

Defaults

By default, inactivity timer is set to 300 minutes.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> aaa kerberos inactivity-timer 30
```

Release History

Release 6.4.5; command introduced.

Related Commands

802.1x kerberos	Enable or disable Kerberos snooping on a 802.1x port.
aaa kerberos mac-move	Enable or disable MAC move globally on the switch.
show aaa kerberos configuration	Displays Kerberos global configuration.

MIB Objects

```
alaKerberosGlobalInactivityTimer
```

aaa kerberos ip-address

Configures IP address of the Kerberos server (Key Distribution Centre - KDC) and UDP or TCP port number.

aaa kerberos ip-address *ip_address* **[udp-port** *num***]**

no aaa kerberos ip-address *ip_address*

Syntax Definitions

ip_address	The IP address of the Kerberos server.
num	UDP or TCP port number of the Kerberos application running on the Kerberos server. UDP port range is 1 to 65535.

Defaults

Default value of UDP port is 88.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Atleast one Kerberos server and one Kerberos enabled port must be configured on the switch for Kerberos snooping to function.
- A maximum of four Kerberos server IP addresses can be configured on a switch
- Server IP address cannot be configured as 0.0.0.0, and the octet value in the IP address cannot be greater than 255 (for example, 1.256.2.3).
- Use the ‘udp-port’ keyword to configure both UDP and TCP protocol port number.
- Use the **no** form of this command to delete the Kerberos server IP address. Only one server can be deleted at a time.
- If all the authentication servers are removed from the switch, then all the Kerberos users learned so far on all the ports are not removed from the database.

Examples

```
-> aaa kerberos ip-address 172.21.160.102 udp-port 2001
-> aaa kerberos ip-address 172.21.160.103 udp-port 2003
-> no aaa kerberos ip-address 172.21.160.102
```

Release History

Release 6.4.5; command introduced.

Related Commands

802.1x kerberos	Enable or disable Kerberos snooping on a 802.1x port.
aaa kerberos mac-move	Enable or disable MAC move globally on the switch.
aaa kerberos inactivity-timer	Configures global inactivity timer on the switch for Kerberos users.
aaa kerberos ip-address	Configures IP address of the Kerberos server (Key Distribution Centre - KDC) and UDP or TCP port number.
aaa kerberos server-timeout	Configures global server reply time-out timer value on the switch for Kerberos users.
show aaa kerberos configuration	Displays Kerberos global configuration.

MIB Objects

```
alaKerberosServerTable
   alaKerberosIpAddress
   alaKerberosRowStatus
```

aaa kerberos server-timeout

Configures global server reply time-out timer value on the switch for Kerberos users.

aaa kerberos kerberos server-timeout *num*

Syntax Definitions

secs	Server reply time-out time interval in seconds in the range 1 second to 30 seconds.

Defaults

By default, reply-timeout is 2 seconds.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

All the users trying to get authenticated from a specific server will have the same value for reply-timeout timer. Whenever a Kerberos request packet is sent to the server, the server reply time-out starts. If the timer expires before receiving the reply from the server, the user authentication is marked as server-time-out and a trap is generated.

Examples

```
-> aaa kerberos server-timeout 20
```

Release History

Release 6.4.5; command introduced.

Related Commands

802.1x kerberos	Enable or disable Kerberos snooping on a 802.1x port.
show aaa kerberos configuration	Displays Kerberos global configuration.

MIB Objects

```
alaKerberosGlobalServerTimeoutTimer
```

aaa kerberos authentication-pass policy-list-name

Configures global classification QoS policy list on the switch for Kerberos users.

aaa kerberos authentication-pass policy-list-name *string*

no aaa kerberos authentication-pass policy-list-name

Syntax Definitions

string	Name of the QoS policy list.

Defaults

By default, global policy list name is ‘none’, that is, there is no Kerberos global QoS policy list configured.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- QoS policy list must be created prior to this configuration.
- Per user Kerberos policy list configuration is not supported.
- Use the **no** form of this command to remove the global classification QoS policy list from the switch.
- If a domain level policy list is configured in the switch and any user belonging to that domain gets authenticated from the Kerberos server, then the domain level policy list is applied to the user over the global policy list.
- If a user gets authenticated from the Kerberos server and the domain level policy list is not configured on the switch for the authenticated user, then the global policy list is applied to the user if the global policy list is configured on the switch.
- If a user gets authenticated from the Kerberos server and neither the domain level policy list (for that user domain) nor the global policy list is configured, then the user traffic is classified on the basis of already applied non-supplicant authentication classification.

Examples

```
-> aaa kerberos authentication-pass policy-list-name p2
```

The following example shows that the **p2** is configured as the global classification QoS policy list on the switch for Kerberos users.

```
-> show aaa kerberos configuration
Mac-Move                    :disabled,
Inactivity Timer            :30 (mins),
Server Timeout              :20 (secs),
Global QoS Policy List      :p2,
Global QoS Policy Status    :Active,

Servers                     :
IP-Address            UDP Port
------------------+----------------
1.1.1.1               88

Per Domain QoS policy List  :
Domain-Name                                Policy-List-Name         Status
---------------------------------+------------------------------+----------
EXAMPLE.COM                          p11                            Active
```

When the QoS policy list **p2** is removed from the system, the corresponding configuration in Kerberos is is shown as below.

```
-> no policy list p2
-> qos apply

-> show aaa kerberos configuration
Mac-Move                    :disabled,
Inactivity Timer            :30 (mins),
Server Timeout              :20 (secs),
Global QoS Policy List      :p2,
Global QoS Policy Status    :Inactive,

Servers                     :
IP-Address            UDP Port
------------------+----------------
1.1.1.1               88

Per Domain QoS policy List  :
Domain-Name                                Policy-List-Name         Status
---------------------------------+------------------------------+----------
EXAMPLE.COM                          pl1                            active
```

The following command removes the global classification QoS policy list from the switch.

```
-> no aaa kerberos authentication-pass policy-list-name
```

Release History

Release 6.4.5; command introduced.

Related Commands

802.1x kerberos	Enable or disable Kerberos snooping on a 802.1x port.
aaa kerberos ip-address	Configures IP address of the Kerberos server (Key Distribution Centre - KDC) and UDP or TCP port number.
aaa kerberos authentication-pass domain	Configures "per domain" classification policy for the Kerberos users.
show aaa kerberos configuration	Displays Kerberos global configuration.

MIB Objects

```
alaKerberosGlobalPolicy
```

aaa kerberos authentication-pass domain

Configures "per domain" classification policy for the Kerberos users.

aaa kerberos authentication-pass domain *domain_name* **policy-list-name** *policy_list*

no aaa kerberos authentication-pass domain *domain_name*

Syntax Definitions

domain_name	Domain name on which the QoS policy is applied. Domain name length can be a maximum of 32 characters. Domain name is case sensitive.
policy_list	Name of the QoS policy list already configured.

Defaults

By default, global policy list name is ‘none’, that is, there is no Kerberos global QoS policy list configured.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the **no** form of this command to remove the "per domain" classification policy for Kerberos users.

Examples

```
-> aaa kerberos authentication-pass domain EXAMPLE.COM policy-list-name p11
```

The following example shows that the **p11** is configured as the policy list associated with the domain EXAMPLE.COM

```
-> show aaa kerberos configuration
Mac-Move                    :disabled,
Inactivity Timer            :30 (mins),
Server Timeout              :20 (secs),
Global QoS Policy List      :p2,
Global QoS Policy Status    :Active,

Servers                     :
IP-Address            UDP Port
------------------+----------------
1.1.1.1               88

Per Domain QoS policy List  :
Domain-Name                              Policy-List-Name         Status
---------------------------------+------------------------------+----------
EXAMPLE.COM                          pl1                          Active
```

When the QoS policy list **p11** is remeoved from the system, the corresponding configuration in Kerberos is shown as below.

```
-> no policy list pl1
-> qos apply

-> show aaa kerberos configuration
Mac-Move                    :disabled,
Inactivity Timer            :30 (mins),
Server Timeout              :20 (secs),
Global QoS Policy List      :p2,
Global QoS Policy Status    :Active,

Servers                     :
IP-Address            UDP Port
------------------+---------------
1.1.1.1               88

Per Domain QoS policy List  :
Domain-Name                              Policy-List-Name         Status
---------------------------------+-----------------------------+----------
EXAMPLE.COM                          pl1                         Inactive
```

The following command removes the “per domain" classification policy for Kerberos users.

```
-> no aaa kerberos authentication-pass domain EXAMPLE.COM
```

Release History

Release 6.4.5; command introduced.

Related Commands

802.1x kerberos	Enable or disable Kerberos snooping on a 802.1x port.
aaa kerberos authentication-pass policy-list-name	Configures global classification QoS policy list on the switch for Kerberos users.
show aaa kerberos configuration	Displays Kerberos global configuration.

MIB Objects

```
alaKerberosPolicyConfigTable
   alaKerberosPolicyDomainName
   alaKerberosPolicyName
   alaKerberosPolicyRowStatus
```

show aaa kerberos configuration

Displays Kerberos global configuration.

show aaa kerberos configuration

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show aaa kerberos configuration
Mac-Move                    :disabled,
Inactivity Timer            :30 (mins),
Server Timeout              :9 (secs),
Global QoS Policy List      :p2,
Global QoS Policy Status    :Active

Servers                     :
IP-Address            UDP Port
------------------+----------------
1.2.3.5               90
4.5.6.7               88
11.22.33.55           80

Per Domain QoS policy List  :
Domain-Name                          Policy-List-Name              Status
---------------------------------+------------------------------+----------
EXAMPLE.COM                          pl1                           Active
```

output definitions

Mac-Move	MAC-move status on the switch: Enabled or Disabled
Inactivity Timer	Global inactivity timer configured on the switch for Kerberos users.
Server Timeout	Global server reply time-out timer value configured on the switch for Kerberos users.
Global QoS Policy List	Global classification QoS policy list associated with the Kerberos users.

output definitions (continued)

Global QoS Policy Status	The global QoS policy status: Active or Inactive 'Inactive' status indicates that the policy list does not exist in the switch or the policy list exists, but not applied.
Servers	**IP Address:** IP address configured of the Kerberos server. **UDP Port:** UDP or TCP port of the Kerberos application running on the Kerberos server
Per Domain QoS policy List	**Domain-Name:** Per domain classification policy configured for Kerberos users. **Policy-List-Name:** Name of the QoS policy list associated with the domain. **Status:** Per domain QoS policy list status: Active or Inactive 'Inactive' status indicates that the policy list does not exist in the switch or the policy list exists, but not applied.

Release History

Release 6.4.5; command introduced.

Related Commands

802.1x kerberos	Enable or disable Kerberos snooping on a 802.1x port.
aaa kerberos mac-move	Enable or disable MAC move globally on the switch.
aaa kerberos inactivity-timer	Configures global inactivity timer on the switch for Kerberos users.
aaa kerberos ip-address	Configures IP address of the Kerberos server (Key Distribution Centre - KDC) and UDP or TCP port number.
aaa kerberos server-timeout	Configures global server reply time-out timer value on the switch for Kerberos users.
aaa kerberos authentication-pass policy-list-name	Configures global classification QoS policy list on the switch for Kerberos users.
aaa kerberos authentication-pass domain	Configures "per domain" classification policy for the Kerberos users.
show aaa kerberos port	Displays Kerberos status of a port or range of ports.
show aaa kerberos users	Displays the learnt Kerberos users information.
show aaa kerberos statistics	Displays the global Kerberos statistics.
show aaa kerberos port statistics	Displays the Kerberos statistics on a port.
clear aaa kerberos statistics	Clears global Kerberos statistics.
clear aaa kerberos port statistics	Clears port level Kerberos statistics.

MIB Objects

```
alaKerberosGlobalMacMoveStatus
   alaKerberosGlobalInactivityTimer
   alaKerberosGlobalServerTimeoutTimer
   alaKerberosGlobalPolicy
   alaKerberosServerTable
```

```
   alaKerberosIpAddress
alaKerberosPolicyConfigTable
   alaKerberosPolicyDomainName
   alaKerberosPolicyName
```

show aaa kerberos port

Displays Kerberos status of a port or range of ports.

show aaa kerberos port [enabled | disabled| <*slot/port* [-*port2*]>]

Syntax Definitions

enabled | **disabled**	Displays the Kerberos status: enabled or disabled
slot/port[-*port2*]	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3). Use a hyphen to specify a range of ports (3/1-10, 5/10-20).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- If a slot/port is not specified, then the information for all the ports are displayed.
- Aggregable and mirroring destination ports are not displayed in the show output.

Examples

```
-> show aaa kerberos port
Slot/Port   Status
----------+---------
    2/1    enabled
    2/2    disabled
    2/3    disabled
    2/4    disabled
    2/5    enabled
    2/6    disabled
    2/7    disabled
    2/8    disabled
```

output definitions

Slot/Port	The Kerberos slot and the port number.
Status	Kerberos status on a port or ports: Enabled or Disabled

Release History

Release 6.4.5; command introduced.

Related Commands

802.1x kerberos	Enable or disable Kerberos snooping on a 802.1x port.
show aaa kerberos configuration	Displays Kerberos global configuration.
show aaa kerberos users	Displays the learnt Kerberos users information.
show aaa kerberos statistics	Displays the global Kerberos statistics.
show aaa kerberos port statistics	Displays the Kerberos statistics on a port.
clear aaa kerberos statistics	Clears global Kerberos statistics.
clear aaa kerberos port statistics	Clears port level Kerberos statistics.

MIB Objects

```
alaKerberosPortTable
   alaKerberosPortIfIndex
   alaKerberosPortStatus
```

show aaa kerberos users

Displays the learnt Kerberos users information.

show aaa kerberos users [port <*slot/port*> **| <mac-address>]**

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
mac-address	MAC address of the Kerberos user.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- If a slot/port is specified, the Kerberos users learnt on that port are displayed.
- If MAC address is specified, then the information related to that Kerberos user is displayed.
- If none of the parameters are specified (slot/port, MAC address), then the information related to all the Kerberos users learnt on the switch is displayed.

Examples

```
-> -> show aaa kerberos users
Slot/         MAC          Authentication       QOS
Port       Address           Status           Policy
-----+-----------------+-----------------+-------------------
 2/18 00:11:22:33:44:55  tgs-authenticated    pl1
 2/19 00:01:02:03:04:05  tgs-timeOut


-> show aaa kerberos users port 2/18
Slot/         MAC          Authentication       QOS
Port       Address           Status           Policy
-----+-----------------+-----------------+-------------------
 2/18 00:11:22:33:44:55  tgs-authenticated    pl1


-> show aaa kerberos users 00:11:22:33:44:55
Detail User Information:
  MAC Address            : 00:11:22:33:44:55
  Port                   : 2/18
  Authentication Status  : tgs-authenticated
  QoS Policy             : pl1
  Domain Name            : EXAMPLE.COM
  User Name              : root\admin
```

```
User Entry State       : active
Inactivity Timer Left  : -1
```

output definitions

Slot/Port	The Kerberos slot and the port number.
MAC Address	MAC address of the Kerberos user.
Authentication Status	Kerberos authentication process involve exchange of two requests (AS_REQ and AS_REP) and two response (AS_REP and TGS_REP). This field indicates up to which level the authentication has reached. On successful authentication, "tgs-authenticated" is displayed.
QoS Policy	QoS policy list configured on the switch for the Kerberos user.
Domain Name	Per domain classification policy configured for the Kerberos user.
User Name	User name of the client

Release History

Release 6.4.5; command introduced.

Related Commands

802.1x kerberos	Enable or disable Kerberos snooping on a 802.1x port.
aaa kerberos authentication-pass policy-list-name	Configures global classification QoS policy list on the switch for Kerberos users.
aaa kerberos authentication-pass domain	Configures "per domain" classification policy for the Kerberos users.
show aaa kerberos configuration	Displays Kerberos global configuration.
clear aaa kerberos statistics	Clears global Kerberos statistics.
clear aaa kerberos port statistics	Clears port level Kerberos statistics.

MIB Objects

```
alaKerberosUserTable
   alaKerberosUserMac
   alaKerberosUserPort
   alaKerberosUserName
   alaKerberosUserDomain
   alaKerberosUserAuthState
   alaKerberosUserPolicy
   alaKerberosUserLeftTime
   alaKerberosUserState
```

show aaa kerberos statistics

Displays the global Kerberos statistics.

show aaa kerberos statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show aaa kerberos statistics
Total Client Packet Rx         :  52
Total Server Packet Rx         :  13
Total KRB-AS-REQ Packet Rx     :  47
Total KRB-AS-REP Packet Rx     :  8
Total KRB-TGS-REQ Packet Rx    :  5
Total KRB-TGS-REP Packet Rx    :  5
Total KRB-ERROR Packet Rx      :  0
Total Client Packet Sw Discard :  0
Total Server Packet Sw Discard :  2
Total Client Packet Hw Discard :  0
Total Server Packet Hw Discard :  0
```

output definitions

Total Client Packet Rx	Total client request packets received.
Total Server Packet Rx	Total server response packets received.
Total KRB-AS-REQ Packet Rx	Total AS-REQ request packets received.
Total KRB-AS-REP Packet Rx	Total AS-REP response packets received.
Total KRB-TGS-REQ Packet Rx	Total TGS-REQ request packets received.
Total KRB-TGS-REP Packet Rx	Total TGS-REP response packets received.
Total KRB-ERROR Packet Rx	Total error packets received from the server.
Total Client Packet Sw Discard	Total client's request packets discarded at software by kerberos module.
Total Server Packet Sw Discard	Total server's response packets discarded at software by kerberos module.

output definitions (continued)

Total Client Packet Hw Discard	Total client's request packets discarded at hardware.
Total Server Packet Hw Discard	Total server's response packets discarded at hardware.

Release History

Release 6.4.5; command introduced.

Related Commands

802.1x kerberos	Enable or disable Kerberos snooping on a 802.1x port.
show aaa kerberos configuration	Displays Kerberos global configuration.
show aaa kerberos port statistics	Displays the Kerberos statistics on a port.
clear aaa kerberos statistics	Clears global Kerberos statistics.
clear aaa kerberos port statistics	Clears port level Kerberos statistics.

MIB Objects

```
alaKerberosClientPktHwDiscardStats
alaKerberosServerPktHwDiscardStats
alaKerberosTotalClientPktRxStats
alaKerberosTotalServerPktRxStats
alaKerberosClientPktSwDiscardStats
alaKerberosServerPktSwDiscardStats
alaKerberosTotalASREQRxStats
alaKerberosTotalASREPRxStats
alaKerberosTotalTGSREQRxStats
alaKerberosTotalTGSREPRxStats
alaKerberosTotalErrorRxStats
```

show aaa kerberos port statistics

Displays the Kerberos statistics on a port.

show aaa kerberos port *slot/port***[**-*port2***] statistics**

Syntax Definitions

*slot/port***[**-*port2***]**	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3). Use a hyphen to specify a range of ports (3/1-10).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- If only port is specified, then the statistics for all the ports is displayed.
- If the slot/port option is specified along with the port, then the statistics for the given port is displayed.
- If the slot/port1-port2 (range of port) is specified, then the statistics for the given port range is displayed.

Examples

```
-> show aaa kerberos statistics

-> show aaa kerberos port statistics
Slot/  Client  Server     Client           Server     KRB-AS-REQ KRB-AS-REP  KRB-TGS-REQ  KRB-TGS-REP KRB-RROR
Port   Pkt Rx  Pkt Rx  Pkt Sw Discard  Pkt Sw Discard   Pkt Rx     Pkt Rx      Pkt Rx       Pkt Rx     Pkt Rx
------+-------+------+---------------+---------------+----------+-----------+-----------+-----------+----------
2/1      0       0         0              0            0            0           0           0           0
2/2      0       0         0              0            0            0           0           0           0
2/3      0       0         0              0            0            0           0           0           0
2/4      0       0         0              0            0            0           0           0           0
2/5      0       0         0              0            0            0           0           0           0
2/6      0       0         0              0            0            0           0           0           0
2/7      0       0         0              0            0            0           0           0           0
2/8      0       0         0              0            0            0           0           0           0
2/9      0       0         0              0            0            0           0           0           0
2/10     0       0         0              0            0            0           0           0           0
2/11     0       0         0              0            0            0           0           0           0
2/12     0       0         0              0            0            0           0           0           0
2/13     0       0         0              0            0            0           0           0           0
2/14     0       0         0              0            0            0           0           0           0
2/15     0       0         0              0            0            0           0           0           0
2/16     0       13        0              2            0            8           0           5           0
2/17     0       0         0              0            0            0           0           0           0
2/18     52      0         0              0            47           0           5           0           0
.
.
.
.
.
```

```
    -> show aaa kerberos port 2/16 statistics
Slot/  Client  Server     Client           Server     KRB-AS-REQ KRB-AS-REP  KRB-TGS-REQ  KRB-TGS-REP KRB-RROR
Port   Pkt Rx  Pkt Rx  Pkt Sw Discard  Pkt Sw Discard   Pkt Rx     Pkt Rx      Pkt Rx       Pkt Rx     Pkt Rx
------+-------+------+---------------+---------------+----------+-----------+-----------+-----------+----------
2/16     0       13         0              2            0           8           0           5           0
```

output definitions

Slot/Port	The Kerberos slot and the port number.
Client Pkt Rx	Client request packets received.
Server Pkt Rx	Server response packets received.
Client Pkt Sw Discard	Client's request packets discarded by kerberos module.
Server Pkt Sw Discard	Server's response packets discarded at the sofware by kerberos module.
KRB-AS-REQ Pkt Rx	AS-REQ request packets received.
KRB-AS-REP Pkt Rx	AS-REP response packets received.
KRB-TGS-REQ Pkt Rx	TGS-REQ request packets received.
KRB-TGS-REP Pkt Rx	TGS-REP response packets received.
KRB-ERROR Pkt Rx	Error packets received from the server.

Release History

Release 6.4.5; command introduced.

Related Commands

802.1x kerberos	Enable or disable Kerberos snooping on a 802.1x port.
show aaa kerberos configuration	Displays Kerberos global configuration.
show aaa kerberos statistics	Displays the global Kerberos statistics.
clear aaa kerberos statistics	Clears global Kerberos statistics.
clear aaa kerberos port statistics	Clears port level Kerberos statistics.

MIB Objects

```
alaKerberosPortStatsTable
   alaKerberosStatsIfIndex
   alaKerberosPortClientPktRxStats
   alaKerberosPortServerPktRxStats
   alaKerberosPortClientPktSwDiscardStats
   alaKerberosPortServerPktSwDiscardStats
   alaKerberosPortASREQRxStats
   alaKerberosPortASREPRxStats
   alaKerberosPortTGSREQRxStats
   alaKerberosPortTGSREPRxStats
   alaKerberosPortErrorRxStats
```

clear aaa kerberos statistics

Clears global Kerberos statistics.

clear aaa kerberos statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> clear aaa kerberos statistics
```

Release History

Release 6.4.5; command introduced.

Related Commands

show aaa kerberos configuration	Displays Kerberos global configuration.
clear aaa kerberos port statistics	Clears port level Kerberos statistics.

MIB Objects

```
alaKerberosGlobalClearStats
```

clear aaa kerberos port statistics

Clears port level Kerberos statistics.

clear aaa kerberos port *slot/port***[**-*port2***] statistics**

Syntax Definitions

*slot/port***[**-*port2***]**	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3). Use a hyphen to specify a range of ports (3/1-10).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> clear aaa kerberos port 2/1 statistics
-> clear aaa kerberos port 2/1-10 statistics
```

Release History

Release 6.4.5; command introduced.

Related Commands

show aaa kerberos configuration	Displays Kerberos global configuration.
show aaa kerberos port	Displays Kerberos status of a port or range of ports.
show aaa kerberos port statistics	Displays the Kerberos statistics on a port.
clear aaa kerberos statistics	Clears global Kerberos statistics.

MIB Objects

```
alaKerberosPortStatsTable
   alaKerberosPortClearStats
```

42 UNP Commands

The Universal Network Profile (UNP) feature provides administrators with the ability to define and apply network access control to specific types of devices by grouping such devices according to specific matching profile criteria. This allows network administrators to create virtual machine network profiles (VNPs) *and* profiles for user devices from a unified framework of operation and administration.

UNP is not limited to creating profiles to classify only certain types of devices. However, the following classification methods implemented through UNP functionality and profile criteria provide the ability to tailor profiles for specific devices (physical or virtual):

- MAC-based authentication using a RADIUS-capable server.
- Switch-wide classification rules to classify on source MAC or IP address (no authentication required).
- VLAN tag classification to create VLAN port associations based on the VLAN ID contained in device packets.
- Default UNP classification for untagged traffic or traffic not classified through other methods.

Basically, UNP provides a method for dynamically assigning network devices to VLAN domains. A profile consists of configurable attributes. When a device sends traffic that matches such attributes, the device is then assigned to a VLAN associated with the UNP. The UNP may also specify a QoS/ACL policy list that is subsequently applied to device traffic associated with the UNP VLAN.

Dynamic assignment of devices using UNP is achieved through port-based functionality that provides the ability to authenticate and classify device traffic. Authentication verifies the device identity and provides a UNP name. In the event authentication is not available or is unsuccessful, classification rules associated with the UNPs are applied to the traffic to determine the UNP VLAN assignment.

This chapter provides information about configuring UNP port parameters and profile attributes through the Command Line Interface (CLI).

MIB information for the UNP commands is as follows:

Filename: ALCATEL-IND1-DA-MIB
Module: alcatelIND1DaMIB

A summary of the available commands is listed here:

UNP commands	**unp name** **unp port** **unp port default-unp** **unp port mac-authentication** **unp port mac-authentication pass-alternate** **unp port classification** **unp port trust-tag** **unp classification mac-address** **unp classification mac-range** **unp classification ip-address** **unp classification vlan-tag** **unp dynamic-vlan-configuration** **unp dynamic-profile-configuration** **unp auth-server-down-unp** **unp auth-server-down-timeout**
UNP show commands	**show unp** **show unp global configuration** **show unp classification** **show unp port** **show unp user**

unp name

Configures a Universal Network Profile (UNP) that is used to provide role-based access to the switch. The UNP determines the VLAN ID a device can join and if any QoS policy rules are applied to control access to network resources.

unp name *unp_name* **vlan** *vlan_id* **[qos-policy-list** *list_name***]**

no unp name *unp_name*

Syntax Definitions

unp_name	The name of the UNP.
vlan_id	The VLAN ID number to associate with the specified UNP. Devices classified with the UNP are assigned to the associated VLAN.
list_name	The name of a policy list to associate with the specified UNP. The policy list contains QoS policy rules/ACLs that are applied to devices clasified with the UNP.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- Use the **no** form of this command to remove a UNP from the switch configuration.
- Specifying a QoS policy list name that is inactive or does not already exist in the switch configuration is allowed. However, the list remains inactive for the UNP until the list is enabled or configured using the QoS policy list commands.
- If the UNP dynamic VLAN configuration capability is enabled, a VLAN specified with this command that does not exist in the switch configuration is automatically created when the UNP is created.

Note. Dynamic VLANs are not saved in the VLAN section of the **boot.cfg** file. However, the **unp** commands to enable dynamic VLAN configuration and create a UNP are saved in the UNP section of the **boot.cfg** file. As a result, the VLAN is created again on the next switch bootup.

Examples

```
-> unp name unp1 vlan 100 qos-policy-list “list1”
-> unp name unp2 vlan 200 qos-policy-list “bad-list”
-> no unp name unp1
```

Release History

Release 6.4.5; command was introduced.

Related Commands

unp port	Enables UNP on a port.
unp dynamic-vlan-configuration	Configures the status of dynamic VLAN configuration for profiles created with a VLAN ID that does not exist.
policy rule	Configures a QoS policy rule.
policy list	Configures a QoS policy list.
show unp	Displays the profile configuration for the switch.

MIB Objects

```
alaDaUserNetProfileTable
   alaDaUserNetProfileName
   alaDaUserNetProfileVlanID
   alaDaUserNetProfileRowStatus
   alaDaUserNetProfileQosPolicyListName
```

unp port

Configures the status of UNP for the specified port. Enabling UNP makes the port eligible for dynamic assignment to a VLAN based on UNP authentication and classification.

unp {port *slot/port1***[**-*port2***] | linkagg** *agg_id***}**

no unp {port *slot/port1***[**-*port2***] | linkagg** *agg_id***}**

Syntax Definitions

*slot/port***[**-*port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
agg_id	The link aggregate ID number.

Defaults

By default, UNP functionality is disabled on all switch ports and link aggregates.

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- Use the **no** form of this command to remove the UNP configuration for the specified port or link aggregate.
- Any configuration change to a UNP-enabled port will flush all MAC addresses learned on that port. This applies only to CLI commands used to configure UNP port parameters.
- Enabling UNP is *not* supported on the following port types:
  - 802.1q-tagged ports.
  - MVRP ports.
  - Port Mirroring destination ports (MTP).
  - Port Mapping network ports.
  - STP and ERP ports.
  - Ports on which a static MAC address is configured.
  - Ports on which dynamic Source Learning is disabled.

Note. If source learning is disabled on UNP Vlan, ensure that the UNP is also disabled to prevent UNP users from getting learnt.

  - VLAN Stacking (Ethernet Services NNI or UNI) ports.

- The UNP and Learned Port Security (LPS) features are supported on the same port with the following conditions:
  - > When LPS is enabled or disabled on a UNP port, MAC addresses already learned on that port are flushed.
  - > When both LPS and UNP are enabled on the same port, UNP first authenticates and classifies any MAC addresses received, then LPS rules are applied. If a MAC address violates any of the LPS rules for the port, the address may get filtered or the port violated even if UNP initially determined the address was valid. In other words, LPS rules take precedence over UNP to determine if a MAC address is bridged or filtered on the port.
  - > If UNP classifies a MAC address as learning but LPS learns the address as filtering, an untagged packet will show as filtering in the default VLAN for the port and a tagged packet MAC will show as filtering in the specific tagged VLAN.
  - > When a MAC address is filtered by LPS, the **show unp user** command will display "LPS-Blocked" as the classification source for that MAC address.
  - > The LPS **port-security chassis** command and some options of the **port-security learning-window** command are not supported on UNP ports. For more information about these exceptions and other conditions for using UNP and LPS on the same port, see Chapter 46, "Learned Port Security Commands," in this guide and the UNP and LPS chapters in the *OmniSwitch AOS Release 6 Network Configuration Guide*.
- There is no limit to the number of switch ports that can have UNP enabled.

Examples

```
-> unp port 1/1
-> unp port 1/1-3
-> no unp port 1/1
-> unp linkagg 5
-> no linkagg 8
```

Release History

Release 6.4.5; command was introduced.

Related Commands

unp name	Configures a UNP in the switch configuration.
unp port default-unp	Associates a default UNP to a port.
show unp port	Displays the UNP configuration for the port.
show unp user	Displays information about the devices learned on a UNP port.

MIB Objects

```
alaDaUNPPortTable
   alaDaUNPPortIfIndex
   alaDaUNPPortDefaultProfileName
   alaDaUNPPortPassAltProfileName
   alaDaUNPPortRowStatus
   alaDaUNPPortMacAuthFlag
   alaDaUNPPortClassificationFlag
```

```
alaDaUNPPortTrustTagStatus
```

unp port default-unp

Configures the name of an existing UNP to serve as the default UNP for the specified port or link aggregate.

unp {port *slot/port1***[**-*port2***] | linkagg** *agg_id***} default-unp** *unp_name*

no unp {port *slot/port1***[**-*port2***] | linkagg** *agg_id***} default-unp**

Syntax Definitions

*slot/port***[**-*port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
agg_id	The link aggregate ID number.
unp_name	The name of the UNP.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- Use the **no** form of the command to remove the default UNP from the port configuration.
- This command is allowed only on UNP-enabled ports.
- The UNP specified with this command must already exist in the switch configuration.
- The default UNP is used to classify devices on the port when one of the following conditions occur:
  - UNP authentication and classification are not enabled on the port.
  - MAC authentication fails.
  - Device traffic does not match UNP classification rules.
  - The UNP trust VLAN tag option (see **unp port trust-tag**) is enabled for the port, but the VLAN ID specified in the tag field of the device traffic does not exist.
  - Untagged device traffic is not classified.

Examples

```
-> unp port 1/1 default-unp “Sales”
-> no unp port 1/1 default-unp
-> unp port 1/1-4 default-unp “Sales”
ERROR: Port 1/2 is not a unp port
ERROR: Port 1/3 is not a unp port
-> unp port 1/1 default-unp “BAD-UNP”
ERROR: UNP doesn't exist
```

```
-> no unp port 1/1-4 default-unp
-> unp linkagg 5 default-unp “VM1-Server1”
-> no unp linkagg 5 default-unp
```

Release History

Release 6.4.5; command was introduced.

Related Commands

unp name	Configures a UNP in the switch configuration.
unp port	Configures the status of UNP functionality on the port.
unp port trust-tag	Configures whether or not a device is classified into an existing VLAN that matches the VLAN ID tag of the packets received from the device.
show unp port	Displays the UNP configuration for the port.

MIB Objects

```
alaDaUNPPortTable
   alaDaUNPPortIfIndex
   alaDaUNPPortDefaultProfileName
   alaDaUNPPortPassAltProfileName
   alaDaUNPPortMacAuthFlag
   alaDaUNPPortClassificationFlag
   alaDaUNPPortTrustTagStatus
   alaDaUNPPortRowStatus
```

unp port mac-authentication

Configures the status of MAC authentication for the specified UNP port. Enable this functionality to invoke MAC-based authentication for devices connected to the UNP port.

unp {port *slot/port1***[-***port2***] | linkagg** *agg_id***} mac-authentication {enable | disable}**

Syntax Definitions

*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
agg_id	Link aggregate ID number.
enable	Enables MAC authentication.
disable	Disables MAC authentication.

Defaults

By default, MAC authentication is disabled.

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- This command is allowed only on UNP-enabled ports.
- MAC-based authentication is supported only through a RADIUS server.
- An option exists to classify a device into an alternate UNP in the event successful MAC authentication does not return a UNP name. This option is configured through the **unp port mac-authentication pass-alternate** command.
- If MAC authentication fails, any classification rules configured for the UNP port are applied.
- If both UNP MAC authentication and classification (see **unp port classification**) are not enabled on the UNP port, all MAC addresses received on that port are blocked unless a default UNP is configured and/or trust VLAN tag is enabled for the port.

Examples

```
-> unp port 1/1 mac-authentication enable
-> unp port 1/1 mac-authentication disable
-> unp linkagg 2 mac-authentication enable
-> unp linkagg 2 mac-authentication disable
```

Release History

Release 6.4.5; command was introduced.

Related Commands

unp name	Configures a UNP in the switch configuration.
unp port	Configures the status of UNP functionality on the port.
unp port mac-authentication pass-alternate	Assigns the device to another UNP when successful MAC authentication does not return a UNP name.
unp port classification	Configures the classification status for the UNP port.
show unp port	Displays the UNP configuration for the port.

MIB Objects

```
alaDaUNPPortTable
   alaDaUNPPortIfIndex
   alaDaUNPPortDefaultProfileName
   alaDaUNPPortPassAltProfileName
   alaDaUNPPortMacAuthFlag
   alaDaUNPPortClassificationFlag
   alaDaUNPPortTrustTagStatus
   alaDaUNPPortRowStatus
```

unp port mac-authentication pass-alternate

Configures the name of an existing UNP to use as an alternate UNP. A device is assigned to the alternate UNP when successful MAC authentication does not return a UNP name.

unp {port *slot/port1***[**-*port2***] | linkagg** *agg_id***} mac-authentication pass-alternate unp-name** *unp_name*

no unp {port *slot/port1***[**-*port2***] | linkagg** *agg_id***} mac-authentication pass-alternate**

Syntax Definitions

*slot/port***[**-*port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
agg_id	Link aggregate ID number.
unp_name	The name of the UNP.

Defaults

By default, no alternate UNP is configured.

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- Use the **no** form of this command to remove the alternate UNP from the UNP port configuration.
- This command is allowed only on UNP-enabled ports or link aggregates.
- The UNP name specified with this command must exist in the switch configuration.

Examples

```
-> unp port 1/1 mac-authentication pass-alternate unp-name Finance
-> unp port 1/1-3 mac-authentication pass-alternate unp-name Finance
-> no unp port 1/1-3 mac-authentication pass-alternate
-> unp linkagg 5 mac-authentication pass-alternate unp-name AltUNP
-> no linkagg 5 mac-authentication pass-alternate
```

Release History

Release 6.4.5; command was introduced.

Related Commands

unp name	Configures a UNP in the switch configuration.
unp port	Configures the status of UNP functionality on the port.
unp port mac-authentication	Configures the MAC authentication status for the UNP port.
show unp port	Displays the UNP port parameter configuration.

MIB Objects

```
alaDaUNPPortTable
   alaDaUNPPortIfIndex
   alaDaUNPPortDefaultProfileName
   alaDaUNPPortPassAltProfileName
   alaDaUNPPortMacAuthFlag
   alaDaUNPPortClassificationFlag
   alaDaUNPPortTrustTagStatus
   alaDaUNPPortRowStatus
```

unp port classification

Configures the classification status for the specified UNP port. When enabled and MAC authentication is disabled or fails, UNP classification rules (MAC address, MAC address range, IP network address, or VLAN tag) are applied to the traffic received on the UNP port.

unp {port *slot/port1***[-***port2***] | linkagg** *agg_id***} classification {enable | disable}**

Syntax Definitions

*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
agg_id	Link aggregate ID.
enable	Enables classification.
disable	Disables classification.

Defaults

By default, classification is disabled on the UNP port.

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- This command is allowed only on UNP-enabled ports.
- UNP classification rules are applied if MAC authentication is disabled on the port, is enabled on the port but the RADIUS server is not configured, or MAC authentication fails.
- If untagged device traffic does not match any of the classification rules, the device is assigned to the default UNP configured for the port.
- If tagged device traffic does not match any of the classification rules and the trust VLAN tag option (see **unp port trust-tag**) is enabled for the port, the device is classified based on the VLAN tag is a VLAN matching the tag exists in the switch configuration.
- If both UNP MAC authentication and classification (see **unp port mac-authentication**) are not enabled on the UNP port, all MAC addresses received on that port are blocked unless a default VLAN is specified and/or trust VLAN tag is enabled for the port.
- When classification is enabled for the port, UNP classification rules are applied in the following order of precedence:
  - MAC address + VLAN tag
  - MAC address
  - MAC address range + VLAN tag
  - MAC address range
  - IP address + VLAN tag
  - IP address
  - VLAN tag

Examples

```
-> unp port 1/1 classification enable
-> unp port 1/1 classification disable
-> unp port 1/1-4 classification enable
ERROR: Port 1/3 is not a unp-port
-> unp linkagg 5 classification enable
-> unp linkagg 5 classification disable
```

Release History

Release 6.4.5; command was introduced.

Related Commands

show unp classification	Displays the UNP classification rule configuration for the switch.
show unp port	Displays the UNP configuration for the port.

MIB Objects

```
alaDaUNPPortTable
   alaDaUNPPortIfIndex
   alaDaUNPPortDefaultProfileName
   alaDaUNPPortPassAltProfileName
   alaDaUNPPortMacAuthFlag
   alaDaUNPPortClassificationFlag
   alaDaUNPPortTrustTagStatus
```

unp port trust-tag

Configures the option of whether or not to trust the VLAN ID of a tagged packet when the VLAN specified also exists in the switch configuration. If the VLAN tag is trusted, the device is assigned to the VLAN ID on the switch that matches the VLAN tag.

unp port {port *slot/port1***[**-*port2***] | linkagg** *agg_id***} trust-tag {enable | disable}**

Syntax Definitions

*slot/port***[**-*port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
agg_id	Link aggregate ID.
enable	Trust the VLAN ID tag.
disable	Do not trust the VLAN ID tag.

Defaults

By default, the VLAN tag is not trusted.

Platforms Supported

OmniSwitch 6900

Usage Guidelines

- When this option is enabled and the VLAN ID tag matches an existing VLAN in the system, the device is classified into the VLAN when one of the following conditions occur:
  - MAC authentication passes, but the RADIUS server returns a UNP that does not exist in the switch configuration.
  - MAC authentication passes, but the RADIUS server does not return a UNP and the alternate UNP option is disabled for the port.
  - Device traffic does not match any of the classification rules configured for the UNP port.
  - The UNP VLAN obtained from the matching classification rule does not exist in the switch configuration.
  - Auth-Server-Down UNP option is used, but the VLAN associated with that UNP does not exist in the switch configuration.
- When the trust tag option is triggered by one of the above conditions, a VLAN-port-association (VPA) is created between the UNP port and the matching VLAN even if the matching VLAN is *not* associated with a UNP.
- Enabling the trust VLAN ID tag option provides an implicit method of VLAN tag classification that will accept tagged traffic matching any of the existing UNPs without the need to create specific classification rules for those profiles.

Examples

```
-> unp port 1/1 trust-tag enable
-> unp port 1/1 trust-tag disable
-> unp port 1/1-4 trust-tag enable
```

Release History

Release 6.4.5; command was introduced.

Related Commands

unp port default-unp	Associates a default UNP to a port.
unp port classification	Configures the classification status for the UNP port.
show unp port	Displays the UNP configuration for the port.
show unp user	Displays information about the devices learned on a UNP port.

MIB Objects

```
alaDaUNPPortTable
   alaDaUNPPortIfIndex
   alaDaUNPPortDefaultProfileName
   alaDaUNPPortPassAltProfileName
   alaDaUNPPortMacAuthFlag
   alaDaUNPPortClassificationFlag
   alaDaUNPPortTrustTagStatus
   alaDaUNPPortRowStatus
```

unp classification mac-address

Defines a MAC address classification rule for the specified Universal Network Profile (UNP). If the source MAC address of the device traffic matches the MAC address defined for the rule, the specified UNP is applied to the device. An optional VLAN ID tag parameter is available to specify a VLAN tag that device traffic must also match in addition to the source MAC address.

unp classification mac-address *mac_address* **[vlan-tag** *vlan_id***] unp-name** *unp_name*

no unp classification mac-address *mac_address*

Syntax Definitions

mac_address	MAC address (for example, 00:00:39:59:f1:0c).
vlan_id	A VLAN ID.
unp_name	The name of a UNP.

Defaults

By default, no classification rules are defined for a UNP.

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- Use the **no** form of this command to remove the MAC address rule. When a classification rule is removed or modified, all MAC addresses classified with that rule are flushed.
- Adding a rule does not cause a MAC address flush. If necessary, use the **no mac-learning** command to clear and re-learn any addresses after the rule is added.
- If a VLAN ID tag is specified with this command, the UNP is only applied to tagged packets containing the specified source MAC address *and* the VLAN ID tag.
- Untagged packets are only classified using the specified MAC address; the VLAN ID tag is ignored if it is specified with this rule.

Examples

```
-> unp classification mac-address 00:11:22:33:44:55 unp-name Finance
-> unp classification mac-address 00:11:22:33:44:55 vlan-tag 100 unp-name Finance
```

Release History

Release 6.4.5; command was introduced.

Related Commands

unp port classification	Configures the classification status for the UNP port. Rules are not applied when classification is disabled for the port.
show unp classification	Displays the UNP classification rule configuration.

MIB Objects

```
alaDaUNPMacRuleTable
   alaDaUNPMacRuleAddr
   alaDaUNPMacRuleProfileName
   alaDaUNPMacRuleVlanTag
```

unp classification mac-range

Defines a MAC address range classification rule for the specified Universal Network Profile (UNP). If the source MAC address of the device traffic matches any address within the range of MAC addresses, the specified UNP is applied to the device. An optional VLAN ID tag parameter is available to specify a VLAN tag that device traffic must also match in addition to the source MAC address.

unp classification mac-range *low_mac_address high_mac_address* **[vlan-tag** *vlan_id***] unp-name** *unp_name*

no unp classification mac-range *low_mac_address high_mac_address*

Syntax Definitions

low_mac_address	MAC address that defines the low end of the range (for example, 00:00:39:59:f1:00).
high_mac_address	MAC address that defines the high end of the range (for example, 00:00:39:59:f1:90).
vlan_id	A VLAN ID.
unp_name	The name of a UNP.

Defaults

By default, no classification rules are defined for a UNP.

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- Use the **no** form of this command to remove a MAC address range rule. When a classification rule is removed or modified, all MAC addresses classified with that rule are flushed.
- Adding a rule does not cause a MAC address flush. If necessary, use the **no mac-learning** command to clear and re-learn any addresses after the rule is added.
- If a VLAN ID tag is specified with this command, the UNP is only applied to tagged packets containing a source MAC address within the specified range *and* the VLAN ID tag.
- Untagged packets are only classified using the specified MAC address range; the VLAN ID tag is ignored if it is specified with this rule.

Examples

```
-> unp classification mac-range 00:11:22:33:44:66 00:11:22:33:44:77 unp-name Sales
-> unp classification mac-range 00:11:22:33:44:88 00:11:22:33:44:99 vlan-tag 200
unp-name
```

Release History

Release 6.4.5; command was introduced.

Related Commands

unp port classification	Configures the classification status for the UNP port. Rules are not applied when classification is disabled for the port.
show unp classification	Displays the UNP classification rule configuration.

MIB Objects

```
alaDaUNPMacRangeRuleTable
   alaDaUNPMacRangeRuleLoAddr
   alaDaUNPMacRangeRuleHiAddr
   alaDaUNPMacRangeRuleProfileName
   alaDaUNPMacRangeRuleVlanTag
```

unp classification ip-address

Defines an IP address classification rule for the specified Universal Network Profile (UNP). If the source IP address of the device traffic matches the IP address defined for the rule, the specified UNP is applied to the device. An optional VLAN ID tag parameter is available to specify a VLAN tag that device traffic must also match in addition to the source MAC address.

unp classification ip-address *ip_address* **mask** *subnet_mask* **[vlan-tag** *vlan_id***] unp-name** *unp_name*

no unp classification ip-address *ip_address* **mask** *subnet_mask*

Syntax Definitions

ip_address	IPv4 network address (for example, 10.0.0.0, 171.15.0.0, 196.190.254.0).
subnet_mask	An IP address mask to identify the IP subnet for the interface (supports class-less masking).
vlan_id	A VLAN ID.
unp_name	The name of a UNP.

Defaults

- By default, the subnet mask is set to the default subnet mask value for the IP address class.
- By default, no classification rules defined for a UNP.

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- Use the **no** form of this command to remove an IP address rule. When a classification rule is removed or modified, all MAC addresses classified with that rule are flushed.
- Adding a rule does not cause a MAC address flush. If necessary, use the **no mac-learning** command to clear and re-learn any addresses after the rule is added.
- If a VLAN ID tag is specified with this command, the UNP is only applied to tagged packets containing the specified source IP address *and* the VLAN ID tag.
- Untagged packets are only classified using the specified IP address; the VLAN ID tag is ignored if it is specified with this rule.

Examples

```
-> unp classification ip-address 10.1.1.1 unp-name Engg
-> unp classification ip-address 20.1.1.1 255.255.0.0 unp-name Admin
-> unp classification ip-address 50.1.1.1 vlan-tag 300 unp-name HR
```

Release History

Release 6.4.5; command was introduced.

Related Commands

unp port classification	Configures the classification status for the UNP port. Rules are not applied when classification is disabled for the port.
show unp classification	Displays the UNP classification rule configuration.

MIB Objects

```
alaDaUNPIpNetRuleTable
   alaDaUNPIpNetRuleAddr
   alaDaUNPIpNetRuleMask
   alaDaUNPIpNetRuleProfileName
   alaDaUNPIpNetRuleVlanTag
```

unp classification vlan-tag

Defines VLAN tag classification rule for the specified Universal Network Profile (UNP). If the VLAN ID tag of the device traffic matches the VLAN ID defined for the rule, the specified UNP is applied to the device.

unp classification vlan-tag *vlan_id* **unp-name** *unp_name*

no unp classification vlan-tag *vlan_id*

Syntax Definitions

vlan_id	A VLAN ID.
unp_name	The name of a UNP.

Defaults

By default, no classification rules are defined for a UNP.

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- Use the **no** form of this command to remove a VLAN tag rule. When a classification rule is removed or modified, all MAC addresses classified with that rule are flushed.
- Adding a rule does not cause a MAC address flush. If necessary, use the **no mac-learning** command to clear and re-learn any addresses after the rule is added.
- Untagged packets are not classified with this rule if a VLAN ID tag is specified with this command.

Examples

```
-> unp classification vlan-tag 400 unp-name Admin
-> unp classification vlan-tag 300 unp-name HR
```

Release History

Release 6.4.5; command was introduced.

Related Commands

unp port classification	Configures the classification status for the UNP port. Rules are not applied when classification is disabled for the port.
show unp classification	Displays the UNP classification rule configuration.

MIB Objects

```
alaDaUNPVlanTagRuleTable
   alaDaUNPVlanTagRuleVlan
   alaDaUNPVlanTagRuleProfileName
```

unp dynamic-vlan-configuration

Configures the UNP status for dynamic VLAN configuration. When this functionality is enabled and the UNP is created with a VLAN that does not exist, the switch will dynamically create the VLAN at the time the UNP is created.

unp dynamic-vlan-configuration {enable | disable}

Syntax Definitions

enable	Enables dynamic VLAN configuration for UNPs.
disable	Disables dynamic VLAN configuration for UNPs**.**

Defaults

By default, dynamic VLAN configuration is disabled.

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

Note. Dynamic VLANs are not saved in the VLAN section of the **boot.cfg** file. However, the **unp** commands to enable dynamic VLAN configuration and create a UNP are saved in the UNP section of the **boot.cfg** file. As a result, the VLAN is created again on the next switch bootup.

- When dynamic VLAN configuration is disabled, creating a UNP with a VLAN that does not exist in the switch configuration is not allowed.
- The VLAN status and other port (non-UNP port) assignments for a dynamic UNP VLAN are configurable using standard VLAN commands. In addition, the STP status is configurable and enabled by default when the dynamic VLAN is created.
- A dynamic VLAN cannot be deleted using standard VLAN commands (**no vlan** *vlan_id*).
- UNP dynamic VLANs are identified as a separate type of VLAN. The **vlan show** commands will display this type with the default name of “UNP-DYN-VLAN” and the designated type as “UNP Dynamic Vlan”.

Examples

```
-> unp dynamic-vlan-configuration enable
-> unp dynamic-vlan-configuration disable
```

Release History

Release 6.4.5; command was introduced.

Related Commands

unp name	Configures a UNP in the switch configuration.
show unp global configuration	Displays the dynamic VLAN configuration status for the switch.

MIB Objects

```
alaDaUNPGlobalConfiguration
   alaDaUNPDynamicVlanConfigFlag
```

unp dynamic-profile-configuration

Configures the UNP status for dynamic profile configuration. When this functionality is enabled, a UNP profile is dynamically created based on specific traffic conditions.

unp dynamic-profile-configuration {enable | disable}

Syntax Definitions

enable	Enables dynamic profile configuration for UNPs.
disable	Disables dynamic profile configuration for UNPs**.**

Defaults

By default, dynamic profile configuration is disabled.

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- When dynamic profile configuration is enabled, a UNP profile is dynamically created when the trust VLAN tag option is enabled on the UNP port or link aggregate and one of the following conditions occurs:
  - A tagged packet received on the UNP port contains a VLAN tag that matches an existing MVRP VLAN in the switch configuration that is not assigned to a profile.
  - There is no matching VLAN in the switch configuration.
- Dynamically created profiles are saved in the **boot.cfg** file for the switch.
- By default, dynamically created profiles are automatically named **dynamic_profile_***vlan_id*, where the VLAN ID is the ID of the VLAN contained in the packet tag.
- After the dynamic profile is created, changing the profile name, associated VLAN ID, or the QoS policy list is allowed. To avoid any confusion, change the profile name if the VLAN ID associated with the profile has changed.
- If the dynamic profile configuration option is enabled along with the dynamic VLAN configuration option, if the dynamic creation of a profile refers to a VLAN that is a MVRP VLAN, then the MVRP VLAN is automatically converted to a dynamic UNP VLAN (UNP-DYN-VLAN).

Examples

```
-> unp dynamic-profile-configuration enable
-> unp dynamic-profile-configuration disable
```

Release History

Release 6.4.5; command was introduced.

Related Commands

unp name	Configures a UNP in the switch configuration.
unp dynamic-vlan-configuration	Configures the status of dynamic VLAN configuration. When enabled, UNP will create a VLAN at the time a profile is created that specifies a VLAN ID that does not exist in the switch configuration.
show unp global configuration	Displays the dynamic profile configuration status for the switch.

MIB Objects

```
alaDaUNPGlobalConfiguration
   alaDaUNPDynamicVlanConfigFlag
```

unp auth-server-down-unp

Configures a UNP to which a device is classified if MAC authentication fails because the RADIUS server is unreachable.

unp auth-server-down-unp *unp_name*

no auth-server-down unp

Syntax Definitions

unp_name	The name of the UNP.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- Use the **no** form of this command to remove the authentication server down UNP.
- When a device is classified into the UNP created with this command, a configurable authentication down timer is started. When the timer runs out, the device is removed from the UNP and the authentication and classification process is performed again for that same device.
- If the authentication server down UNP is removed, the authentication server down timer is also removed.

Examples

```
-> unp auth-server-down-unp unp1
-> no unp auth-server-down-unp
```

Release History

Release 6.4.5; command was introduced.

Related Commands

unp auth-server-down-timeout	Configures the value for the authentication server down timer.
show unp global configuration	Displays the profile designated as the authentication server down UNP for the switch.

MIB Objects

```
alaDaUNPGlobalConfiguration
   alaDaUNPAuthServerDownUnp
```

unp auth-server-down-timeout

Configures the authentication server down timer value. This timer value is applied to devices that were learned in the authentication server down UNP.

unp auth-server-down-timeout *seconds*

Syntax Definitions

seconds	The number of seconds the authentication server down timer is active.The valid range is 10 to 1000 seconds.

Defaults

By default, the timeout value is set to 60 seconds.

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- When this timer expires, devices learned in the authentication server down UNP are cleared from that UNP and authenticated and classified again.
- When the authentication server down UNP is removed, the authentication server down timer is also cleared.

Examples

```
-> unp auth-server-down-timeout 500
-> unp auth-server-down-timeout 60
```

Release History

Release 6.4.5; command was introduced.

Related Commands

unp auth-server-down-unp	Configures a UNP to which a device is classified if MAC authentication fails because the RADIUS server is unreachable.
show unp global configuration	Displays the authentication server down timeout value for the switch.

MIB Objects

```
alaDaUNPGlobalConfiguration
   alaDaUNPAuthServerDownTimeout
```

show unp

Displays the Universal Network Profile (UNP) configuration for the switch.

show unp [*unp_name* **| sync | out-of-sync | local**

Syntax Definitions

unp_name	The name of the UNP to display.
sync	Displays the UNP configurations that are the same on both MCLAG peer switches.
out-of-sync	Displays the UNP configurations that are not the same on both MCLAG peer switches.
local	Displays the UNP configurations that are local to the switch.

Defaults

By default, the configuration for all UNPs is displayed.

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- Enter a UNP name with this command to display information for a specific UNP.
- Configuring a UNP setup in a Multi-Chassis Link Aggregation (MCLAG) configuration is supported, but the UNP configuration must be the same on both MCLAG peer switches. The “MC Conf Status” field contents indicates whether or not the UNP configuration is consistent on both peer switches.
- Use the **sync**, **out-of-sync**, or **local** parameters with this command to specify which profiles to display based on the MCLAG consistency of the UNP configuration. The following table indicates under which conditions the UNP configuration is considered in sync, out-of-sync, or local.

Sync	Out of Sync	Local
Profile name is the same on both peer switches, and profiles are configured with the same parameters.	• Profile names are the same on both peer switches, but profile parameters are different. • Profile is configured on only one peer switch and is assigned to an MCLAG aggregate as a default UNP or a Pass Alternate UNP. • Profile is configured on only one peer switch and is assigned to a device ingressing on an MCLAG aggregate.	• Profile is configured on only one peer switch and is not assigned to an MCLAG aggregate as a default UNP or a Pass Alternate UNP. • Profile is configured on only one peer switch and is not assigned to a device ingressing on an MCLAG aggregate.

Examples

```
-> show unp
Name               Vlan   Policy List Name  Status   MC Conf Status
-----------------+------+-----------------+--------+-------------
Sales               100   list1             Active    Sync
Finance             1000  list2             Inactive  Out Of Sync

-> show unp sync
Name               Vlan   Policy List Name  Status   MC Conf Status
-----------------+------+-----------------+--------+-------------
Sales               100   list1             Active    Sync

-> show unp Finance
Name               Vlan   Policy List Name  Status   MC Conf Status
-----------------+------+-----------------+--------+-------------
Finance             1000  list2             Inactive  Out Of Sync
```

output definitions

Name	The name of the profile. Configured through the **unp name** command.
Vlan	The VLAN ID associated with the profile. Configured through the **unp name** command.
Policy List Name	The name of the QoS policy list associated with the profile. Configured through the **unp name** command.
Status	The status of the profile (**Active** or **Inactive**). An active profile indicates devices are assigned to the profile VLAN.
MC Conf Status	The MCLAG consistency check status of the UNP configuration (**Sync, Out-Of-Sync**, or **Local**).

Release History

Release 6.4.5; command was introduced.

Related Commands

show unp classification	Displays the UNP classification rule configuration for the switch.
show unp global configuration	Displays the UNP global parameter values configured for the switch.
show unp port	Displays the UNP configuration for the port.
show unp user	Displays information about the devices learned on a UNP port.

MIB Objects

```
alaDaUserNetProfileTable
   alaDaUserNetProfileName
   alaDaUserNetProfileVlanID
   alaDaUserNetProfileRowStatus
   alaDaUserNetProfileQosPolicyListName
   alaDaUserNetProfileMCLagConfigStatus
```

show unp global configuration

Displays the configuration for global Universal Network Profile (UNP) parameter settings.

show unp global configuration

Syntax Definitions

N/A

Defaults

N/A.

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- Configuring a UNP setup in a Multi-Chassis Link Aggregation (MCLAG) configuration is supported, but the UNP configuration must be the same on both MCLAG peer switches. The “MC Conf Status” field contents (Sync or Out Of Sync) indicates whether or not the UNP configuration is consistent on both peer switches.
- The following table indicates under which conditions the UNP global configuration is considered in sync or out-of-sync (the Local status does not apply to global UNP parameters).

	Sync	Out of Sync	Local
Dynamic VLAN Configuration	Enabled on both peer switches or disabled on both peer switches.	Enabled on one peer switch, but disabled on the other peer switch.	N/A
Dynamic Profile Configuration	Enabled on both peer switches or disabled on both peer switches.	Enabled on one peer switch, but disabled on the other peer switch.	N/A
Authentication Server Down UNP	• The same authentication server down UNP name is configured on both peer switches. • There is no authentication server down UNP configured on either one of the two peer switches.	• The authentication server down UNP name is different on each peer switch. • The authentication server down UNP is configured on only one of the peer switches.	N/A
Authentication Server Down Timeout	• The timer value is the same on both peer switches. • There is no timer value configured on either one of the two peer switches (the default value was not changed).	• The time value is different on each peer switch • The timer value is configured on only one of the peer switches.	N/A

Examples

```
-> show unp global configuration
Dynamic Vlan Configuration        : Enabled,
MC Conf Status                    : Sync,
Dynamic Profile Configuration     : Enabled,
MC Conf Status                    : Sync,
Auth Server Down UNP              : SrvDownUNP,
MC Conf Status                    : Sync,
Auth Server Down Timeout (Sec)    : 60
MC Conf Status                    : Sync,

-> show unp global configuration
Dynamic Vlan Configuration        : Disabled,
MC Conf Status                    : Sync,
Dynamic Profile Configuration     : Disabled,
MC Conf Status                    : Sync,
Auth Server Down UNP              : -,
MC Conf Status                    : Out Of Sync,
Auth Server Down Timeout (Sec)    : -,
MC Conf Status                    : Out Of Sync,
```

output definitions

Dynamic Vlan Configuration	The status (**Enabled** or **Disabled**) of dynamic VLAN configuration. Configured through the **unp dynamic-vlan-configuration** command.
MC Conf Status	The MCLAG consistency check status for the global UNP configuration of this parameter (**Sync** or **Out Of Sync**). The status is displayed for each global UNP parameter option.
Dynamic Profile Configuration	The status (**Enabled** or **Disabled**) of dynamic profile configuration. Configured through the **unp dynamic-profile-configuration** command.
Auth Server Down UNP	The name of a UNP that a device is assigned to in the event the RADIUS server is unreachable. This feature is not configured if a UNP name does not appear in this field. Configured through the **unp auth-server-down-unp** command.
Auth Server Down Timeout	The amount of time, in seconds, that devices remain in the VLAN associated with the authentication server down UNP. Configured through the **unp auth-server-down-timeout** command.

Release History

Release 6.4.5; command was introduced.

Related Commands

show unp	Displays the UNP configuration for the switch.
show unp port	Displays the UNP configuration for the port.
show unp user	Displays information about the devices learned on a UNP port.

MIB Objects

```
alaDaUNPGlobalConfiguration
   alaDaUNPDynamicVlanConfigFlag
   alaDaUNPDynamicVlanMCLagConfigStatus
   alaDaUNPDynamicProfileConfigFlag
   alaDaUNPDynamicProfileConfigMCLagConfigStatus
   alaDaUNPAuthServerDownUnp
   alaDaUNPAuthServerDownUNPMCLagConfigStatus
   alaDaUNPAuthServerDownTimeout
   alaDaUNPAuthServerDownTimeoutMCLagConfigStatus
```

show unp classification

Displays the UNP classification rule configuration for the switch.

show unp classification {mac-rule | mac-range-rule | ip-rule | vlan-tag-rule} [sync | out-of-sync | local]

Syntax Definitions

mac-rule	Display the MAC address rule configuration.
mac-range-rule	Displays the MAC address range rule configuration.
ip-rule	Displays the IP network address rule configuration.
vlan-tag-rule	Displays the VLAN tag rule configuration.
sync	Displays the UNP configurations that are the same on both MCLAG peer switches.
out-of-sync	Displays the UNP configurations that are not the same on both MCLAG peer switches.
local	Displays the UNP configurations that are local to the switch.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- Specifying one of the classification rule type parameters is required with this command.
- Configuring a UNP setup in a Multi-Chassis Link Aggregation (MCLAG) configuration is supported, but the UNP configuration must be the same on both MCLAG peer switches. The “MC Conf Status” field contents (Sync, Out Of Sync, or Local) indicates whether or not the UNP configuration is consistent on both peer switches.
- Use the **sync**, **out-of-sync**, or **local** parameters with this command to specify which profiles to display based on the MCLAG consistency of the UNP configuration. The following table indicates under which conditions the UNP configuration is considered in sync, out-of-sync, or local.

Sync	Out of Sync	Local
The classification rule, rule attributes, and the UNP name for the rule are the same on both peer switches.	• Classification rule and attributes are the same on both peer switches, but the UNP name for the rule is different. • Classification rule is configured on only one peer switch, but a device ingressing on an MCLAG aggregate is classified with the rule.	Classification rule is configured on only one peer switch but UNP has not classified any device ingressing on an MCLAG aggregate with this rule.

Examples

```
-> show unp classification mac-rule
MAC Address        UNP Name       VLAN Tag   MC Conf Status
-----------------+--------------+---------+----------------
00:11:22:33:44:55  Sales           100        Sync
00:0f:b5:46:d7:56  Finance          -         Out Of Sync

-> show unp classification mac-rule out-of-sync
MAC Address        UNP Name       VLAN Tag   MC Conf Status
-----------------+--------------+---------+----------------
00:0f:b5:46:d7:56  Finance          -         Out Of Sync

-> show unp classification mac-range-rule
Low MAC Address    High MAC Address   UNP Name   VLAN Tag   MC Conf Status
-----------------+-----------------+----------+---------+----------------
00:11:22:33:44:66  00:11:22:33:44:77  Sales       100       Out Of Sync
00:11:22:33:44:88  00:11:22:33:44:99  Sales       100       Local

-> show unp classification mac-range-rule Local
Low MAC Address    High MAC Address   UNP Name   VLAN Tag   MC Conf Status
-----------------+-----------------+----------+---------+----------------
00:11:22:33:44:88  00:11:22:33:44:99  Sales       100       Local

-> show unp classification ip-rule
IP Address      IP Mask         UNP Name  VLAN Tag   MC Conf Status
---------------+---------------+---------+---------+---------------
10.1.1.1        255.0.0.0       Engg        -        Sync
20.1.1.1        255.255.0.0     Admin       -        Sync
50.1.1.1        255.0.0.0       HR          300      Local
60.1.1.1        255.0.0.0       HR          -        Local

-> show unp classification ip-rule sync
IP Address      IP Mask         UNP Name  VLAN Tag   MC Conf Status
---------------+---------------+---------+---------+---------------
10.1.1.1        255.0.0.0       Engg        -        Sync
20.1.1.1        255.255.0.0     Admin       -        Sync
```

```
-> show unp classification vlan-tag-rule
VLAN Tag  UNP Name    MC Conf Status
---------+----------+---------------------
400       Admin       Sync
300       HR          Out Of Sync

-> show unp classification vlan-tag-rule out-of-sync
VLAN Tag  UNP Name    MC Conf Status
---------+----------+---------------------
300       HR          Out Of Sync
```

output definitions

MAC Address	The MAC address value to match for this profile rule. Configured through the **unp classification mac-address** command.
Low MAC Address **High MAC Address**	The lowest and highest MAC address values used to specify a range of addresses to match for this rule. Configured through the **unp classification mac-range** command.
IP Address IP Mask	The IP network address and mask values to match for this rule. Configured through the **unp classification ip-address**
UNP Name	The name of the profile. Configured through the **unp name** command.
VLAN Tag	The VLAN ID value to match for this profile rule. This rule is also supported in combination with each of the other classification rules. Configured through the **unp classification vlan-tag** or as a parameter with the other classification rule commands.
MC Conf Status	The MCLAG consistency check status for the UNP configuration (**Sync, Out-Of-Sync**, or **Local**).

Release History

Release 6.4.5; command was introduced.

Related Commands

show unp	Displays the UNP configuration for the switch.
show unp port	Displays the UNP configuration for the port.
show unp user	Displays information about the devices learned on a UNP port.

MIB Objects

```
alaDaUNPMacRuleTable
   alaDaUNPMacRuleAddr
   alaDaUNPMacRuleProfileName
   alaDaUNPMacRuleVlanTag
   alaDaUNPMacRuleMCLagConfigStatus
alaDaUNPMacRangeRuleTable
   alaDaUNPMacRangeRuleLoAddr
   alaDaUNPMacRangeRuleHiAddr
   alaDaUNPMacRangeRuleProfileName
   alaDaUNPMacRangeRuleVlanTag
```

```
   alaDaUNPMacRangeRuleMCLagConfigStatus
alaDaUNPIpNetRuleTable
   alaDaUNPIpNetRuleAddrType
   alaDaUNPIpNetRuleAddr
   alaDaUNPIpNetRuleMask
   alaDaUNPIpNetRuleProfileName
   alaDaUNPIpNetRuleVlanTag
   alaDaUNPIpNetRuleMCLagConfigStatus
alaDaUNPVlanTagRuleTable
   alaDaUNPVlanTagRuleVlan
   alaDaUNPVlanTagRuleProfileName
   alaDaUNPVlanTagRuleMCLagConfigStatus
```

show unp port

Displays the UNP configuration for the port. Includes only ports and link aggregates for which UNP is enabled.

show unp {port *slot/port1***[**-*port2***] | linkagg** *agg_id***} [sync | out-of-sync | local]**

Syntax Definitions

*slot/port***[**-*port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
agg_id	Link aggregate ID.
sync	Displays the UNP configurations that are the same on both MCLAG peer switches.
out-of-sync	Displays the UNP configurations that are not the same on both MCLAG peer switches.
local	Displays the UNP configurations that are local to the switch.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- Configuring a UNP setup in a Multi-Chassis Link Aggregation (MCLAG) configuration is supported, but the UNP configuration must be the same on both MCLAG peer switches. The “MC Conf Status” field contents (Sync, Out Of Sync, or Local) indicates whether or not the UNP configuration is consistent on both peer switches.
- Use the **sync**, **out-of-sync**, or **local** parameters with this command to specify which profiles to display based on the MCLAG consistency of the UNP configuration. The following table indicates under which conditions the UNP configuration is considered in sync, out-of-sync, or local.

Show Command	Sync	Out of Sync	Local
show unp port	MCLAG aggregates: the UNP configuration is the same on both peer switches.	MCLAG aggregates: the UNP configuration is not the same on both peer switches.	All ports; all link aggregates that are not MCLAG.
show unp port *slot/port*	N/A - ports always Local.	N/A - ports always local.	All ports.

Show Command	Sync	Out of Sync	Local
show unp linkagg *agg_id*	MCLAG aggregates: the UNP configuration is the same on both peer switches.	• MCLAG aggregates: the UNP configuration is not the same on both peer switches. • MCLAG aggregates: UNP is enabled on only one of the peer switches.	Link aggregates are not MCLAG.

Examples

```
-> show unp port
Port Mac-Auth Classification Default Pass-Alternate Trust-Tag  MC Conf Status
----+--------+--------------+-------+--------------+----------+---------------
1/1  Enabled   Enabled        Sales  Finance         Enabled     Local
1/2  Enabled   Disabled       Engg   Accouting       Disabled    Local
1/3  Disabled  Disabled       Engg   -               Enabled     Local
1/4  Disabled  Disabled       -      -               Disabled    Local
0/10 Enabled   Enabled        Sales  Finance         Enabled     Sync
0/11 Enabled   Disabled       Engg   Accouting       Disabled    Out Of Sync

-> show unp port sync
Port Mac-Auth Classification Default Pass-Alternate Trust-Tag  MC Conf Status
----+--------+--------------+-------+--------------+----------+---------------
0/10 Enabled   Enabled        Sales  Finance         Enabled     Sync

-> show unp linkagg
Port Mac-Auth Classification Default Pass-Alternate Trust-Tag  MC Conf Status
----+--------+--------------+-------+--------------+----------+---------------
0/10 Enabled   Enabled        Sales  Finance         Enabled    Sync
0/11 Enabled   Disabled       Engg   Accouting       Disabled   Out Of Sync
0/12 Enabled   Enabled        Sales  Finance         Enabled    Sync
0/13 Enabled   Disabled       Engg   Accouting       Disabled   Out Of Sync

-> show unp linkagg out-of-sync
Port Mac-Auth Classification Default Pass-Alternate Trust-Tag  MC Conf Status
----+--------+--------------+-------+--------------+----------+---------------
0/11 Enabled   Disabled       Engg   Accouting       Disabled   Out Of Sync
0/13 Enabled   Disabled       Engg   Accouting       Disabled   Out Of Sync

-> show unp port 1/2-4
Port Mac-Auth Classification Default Pass-Alternate Trust-Tag  MC Conf Status
----+--------+--------------+-------+--------------+----------+---------------
1/2  Enabled   Disabled       Engg   Accouting       Enabled    Local
1/3  Disabled  Disabled       Engg   -               Disabled   Local
1/4  Disabled  Disabled       -      -               Enabled    Local

-> show unp port 1/1
Port Mac-Auth Classification Default Pass-Alternate Trust-Tag  MC Conf Status
----+--------+--------------+-------+--------------+----------+---------------
1/1  Enabled  Enabled        Sales   Finance         Enabled    Local
```

output definitions

Port	The port or link aggregate on which UNP is enabled. Configured through the **unp port** command.
Mac-Auth	The status of MAC authentication (Enabled or Disabled) for the UNP port or link aggregate. Configured through the **unp port mac-authentication** command.
Classification	The status of classification (Enabled or Disabled) for the UNP port or link aggregate. Configured through the **unp port classification** command.
Default	The name of the default UNP assigned to the port or link aggregate. Configured through the **unp port default-unp** command.
Pass-Alternate	The name of the MAC authentication pass alternate UNP assigned to the port or link aggregate. Configured through the **unp port mac-authentication pass-alternate** command.
Trust-Tag	The status of the trust VLAN tag option for the UNP port or link aggregate. Configured through the **unp port trust-tag** command.
MC Conf Status	The MCLAG consistency check status for the UNP port or link aggregate. The status for ports is always set to **Local**, but the status for link aggregates is set to **Sync**, **Out Of Sync**, or **Local**.

Release History

Release 6.4.5; command was introduced.

Related Commands

show unp	Displays the UNP configuration for the switch.
show unp user	Displays information about the devices learned on a UNP port.

MIB Objects

```
alaDaUNPPortTable
   alaDaUNPPortIfIndex
   alaDaUNPPortDefaultProfileName
   alaDaUNPPortPassAltProfileName
   alaDaUNPPortMacAuthFlag
   alaDaUNPPortClassificationFlag
   alaDaUNPPortTrustTagStatus
   alaDaUNPPortMCLagConfigStatus
```

show unp user

Displays information about the MAC addresses learned on a UNP port or link aggregate.

show unp user [*mac_address***] [***slot/port***[-***port2***] | linkagg** *agg_id***] [count]**

Syntax Definitions

mac_address	The device MAC address.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
agg_id	Link aggregate ID.
count	Displays the number of UNP users.

Defaults

By default, information is displayed for all learned devices on all UNP ports and link aggregates.

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- The **count** parameter is used on its own or in combination with a specified port or link aggregate.
- Enter a slot and port number to display devices learned on a specific port.
- Use the **linkagg** parameter and an aggregate ID number to display devices learned on a specific link aggregate.
- A zero is displayed instead of a slot number to designate a link aggregate. For example “0/10” specifies the device was learned on aggregate ID number 10.

Examples

```
-> show unp user
Total users: 3
                                        User                            Learning
Port Username           Mac address     IP       Vlan  UNP     Status   Source
----+----------------+----------------+---------+-----+-------+-------+----------
1/1  00:00:00:00:00:01 00:00:00:00:00:01 10.0.0.1  10    Sales   Active   Local
1/1  00:80:df:00:00:02 00:80:df:00:00:02 10.0.0.2  20    Finance Active   Local
1/2  00:80:df:00:00:03 00:80:df:00:00:03 20.0.0.5  30     -      Block    Local
0/10 00:80:df:00:00:04 00:80:df:00:00:04 30.0.0.5  30     -      Block    Remote
0/11 00:80:df:00:00:05 00:80:df:00:00:05 40.0.0.5  30     -      Active   Local
```

output definitions

Port	The port or link aggregate on which the MAC address was learned.
User Name/MAC Address	The MAC address of the device.
User IP	The IP network address of the device.

output definitions

VLAN	The UNP VLAN ID in which the device was classified.
UNP	The name of the UNP to which the device was assigned.
Status	The status of the device (**Active** or **Blocked**)
Learning Source	Indicates in an MCLAG configuration if the device was classified on the local switch (**Local**) or learned on the peer switch (**Remote**).

```
-> show unp user 00:00:00:00:00:01
Port                        : 01/20,
Mac-address                 : 00:00:00:00:00:01,
IP                          : 14.15.16.17,
Vlan                        : 300,
UNP                         : UNP3,
Login Timestamp             : 04/01/1970 18:45:26,
Authentication Type         : Mac authentication,
Authentication Status       : Authenticated,
Classification Source       : RADIUS - Server UNP
Learning source             : Local

-> show unp user 00:11:11:00:00:12
Port                        : 01/20,
Mac-address                 : 00:11:11:00:00:12,
IP                          : 14.15.16.17,
Vlan                        : 100,
UNP                         : UNP1,
Login Timestamp             : 04/01/1970 18:49:04,
Authentication Type         : Mac authentication,
Authentication Status       : Authenticated,
Classification Source       : RADIUS - Default UNP
Learning source             : Local

-> show unp user 00:11:22:33:44:93
Port                        : 01/20,
Mac-address                 : 00:11:22:33:44:93,
IP                          : 14.15.16.17,
Vlan                        : 400,
UNP                         : UNP4,
Login Timestamp             : 04/01/1970 18:43:11,
Authentication Type         : Mac authentication,
Authentication Status       : Failed,
Classification Source       : Auth Fail - MAC Range Rule UNP
Learning source             : Local

-> show unp user 00:11:22:33:44:99
Port                        : 01/20,
Mac-address                 : 00:11:22:33:44:99,
IP                          : 14.15.16.17,
Vlan                        : 500,
UNP                         : UNP5,
Login Timestamp             : 04/01/1971 18:50:01,
Authentication Type         : - ,
Authentication Status       : - ,
Classification Source       : Tag - MAC Rule UNP
Learning source             : Local
```

```
-> show unp user 00:11:22:33:44:99
Port                         : 01/20,
Mac-address                  : 00:11:22:33:44:99,
IP                           : 14.15.16.17,
Vlan                         : 500,
UNP                          : UNP5,
Login Timestamp              : 04/01/1971 18:50:01,
Authentication Type          : Mac Authentication,
Authentication Status        : Failed,
Classification Source        : Auth-Server-Down UNP
Learning source              : Local

-> show unp user 00:11:22:33:44:9A
Port                         : 01/21,
Mac-address                  : 00:11:22:33:44:9A,
IP                           : 14.15.16.19,
Vlan                         : 1,
UNP                          : - ,
Login Timestamp              : - ,
Authentication Type          : Mac Authentication,
Authentication Status        : Failed,
Classification Source        : Auth-Server-Down UNP - Blocked
Learning source              : Local

-> show unp user 00:11:22:33:44:9A
Port                         : 0/10,
Mac-address                  : 00:11:22:33:44:9A,
IP                           : 14.15.16.19,
Vlan                         : 1,
UNP                          : - ,
Login Timestamp              : - ,
Authentication Type          : Mac Authentication,
Authentication Status        : Failed,
Classification Source        : Auth-Server-Down UNP - Blocked
Learning source              : Remote

-> show unp user 1/1-5 count
Total users: 3

-> show unp user count
Total users: 3

-> show unp user linkagg 11 count
Total users: 2
```

output definitions

Port	The port or link aggregate on which the MAC address was learned.
MAC Address	The MAC address of the device.
IP	The IP network address of the device.
VLAN	The UNP VLAN ID in which the device was classified.
UNP	The name of the UNP to which the device was assigned.
Login Timestamp	The date and time the device was learned.
Authentication Type	The type of authentication used (only MAC authentication supported).

output definitions

Authentication Status	The status of the authentication process (**blank** "–", **Authenticated**, **Failed**, or **In Progress**).
Classification Source	Indicates how the device was classified.
Learning Source	Indicates in an MCLAG configuration if the device was classified on the local switch (**Local**) or learned on the peer switch (**Remote**).

The following is a list of possible values for the "Classification Source" field:

- Pass alternate UNP
- Pass alternate UNP - Blocked
- Default UNP
- Default UNP - Blocked
- Server UNP
- Server UNP - Blocked
- Auth Fail - Default UNP
- Auth Fail - Default UNP - Blocked
- Auth Fail - MAC Rule UNP
- Auth Fail - MAC Rule UNP - Blocked
- Auth Fail - MAC Range Rule UNP
- Auth Fail - MAC Range Rule UNP - Blocked
- Auth Fail - IP Rule UNP
- Auth Fail - IP Rule UNP - Blocked
- MAC Rule UNP
- MAC Rule UNP - Blocked
- MAC + Vlan Tag UNP
- MAC + Vlan Tag UNP - Blocked
- MAC Range rule UNP
- MAC Range rule UNP - Blocked
- MAC Range + Vlan Tag UNP
- MAC Range + Vlan Tag UNP - Blocked
- IP Rule UNP
- IP Rule UNP - Blocked
- IP + Vlan Tag UNP
- IP + Vlan Tag UNP - Blocked
- Vlan Tag Rule UNP
- Vlan Tag Rule UNP - Blocked
- Trust Tag
- No UNP Match – Blocked
- Auth-Server Down UNP
- Auth-Server Down UNP – Blocked.
- LPS - Blocked.

Release History

Release 6.4.5; command was introduced.

Related Commands

show unp	Displays the UNP configuration for the switch.
show unp port	Displays the UNP configuration for the port.

MIB Objects

```
alaDaMacUserTable
   alaDaMacVlanUserIntfNum,
   alaDaMacVlanUserAuthVlan
   alaDaMacVlanUserMACAddress
```

43 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
vlan binding port-protocol
vlan mac
vlan mac range
vlan ip
vlan ipx
vlan protocol
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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 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 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 6.1; 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

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 6400, 6850E, 6855, 9000E

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 6.1; 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 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 43-18).
- 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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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** 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 6400, 6850E, 6855, 9000E

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 6.1; 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 | 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.
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 6400, 6850E, 6855, 9000E

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 6.1; 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 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; command was introduced.

Related Commands

show vlan port	Displays VLAN port assignments for all VLANs, a specific VLAN, or for a specific port.

44 Network Security Commands

Network Security (also known as Alcatel-Lucent's Traffic Anomaly Detection feature) detects anomalies in network traffic through statistical analysis of a port's ingress and egress packets. Anomalies occur when traffic patterns of a port do not meet expectations. Network Security detects such anomalies in real time and upon detection can log and/or generate an SNMP trap and/or disable the anomalous port automatically.

Network Security provides the following capabilities:

- Real time network traffic monitoring.
- Dynamic anomaly detection.
- Dynamic anomalous port quarantining.

Note. The Network Security feature is supported only on the OmniSwitch 6850E, 6855, and 9000E series.

MIB information for the Network Security commands is as follows:

Filename: AlcatelIND1Ns.mib
Module: ALCATEL-IND1-NETSEC-MIB

A summary of available commands is listed here:

---

netsec group port
netsec group anomaly
show netsec summary
show netsec traffic
show netsec statistics
show netsec config
show netsec operation
show netsec group port

Configuration procedures for Network Security are explained in the "Configuring Network Security" chapter of the *OmniSwitch AOS Release 6 Network Configuration Guide*.

netsec group port

Creates a monitoring-group and configures port associations for that group.

netsec group *grp_name* **port** *slot/port***[**-*port2***]**

no netsec group *grp_name* **port** *slot/port***[**-*port2***]**

Syntax Definitions

grp_name	The name of the monitoring-group (up to 32 characters).
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).
port2	The last port number in a range of ports that you want to associate on the same slot (e.g, 3/1-4 specifies ports 1-4 on slot 3).

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a port or a range of ports from the monitoring-group.
- A port-range cannot be a subset of any other port-range which is already configured.
- The word ‘all’ cannot be used as a group name (*grp_name).*

Examples

```
-> netsec group ad-port port 1/1
-> netsec group ad-port port 1/3-10
-> no netsec group ad-port port 1/1
```

Release History

Release 6.3.1; command was introduced.

Related Commands

netsec group anomaly	Configures the monitoring period of an anomaly for a port-group, packet count configuration for triggering anomaly detection, anomaly detection algorithm’s sensitivity to discrepancy in standard and observed traffic pattern.
show netsec summary	Displays the anomaly check summary.

MIB Objects

```
alaNetSecPortRangeGroupTable
   alaNetSecPortRangeGroupStartIfId
   alaNetSecPortRangeGroupEndIfId
   alaNetSecPortRangeGroupName
   alaNetSecPortRangeGroupRowStatus
```

netsec group anomaly

Configures various anomaly parameters of a monitoring-group and specifies the anomaly to monitor for the monitoring-group.

netsec group {*grp_name* **| all} anomaly {***anomaly_name* **| all} {{{state | log | trap | quarantine} {enable | disable}} | {period** *seconds***} | {count** *num***} | {sensitivity** *num***}}**

no netsec group *grp_name* **anomaly {***anomaly_name* **| all} {state | log | trap | quarantine | period | count | sensitivity}**

Syntax Definitions

grp_name	The name of the monitoring-group (up to 32 characters).
group all	Specifies all the monitoring-groups.
anomaly_name	The type of the anomaly to be enabled or disabled. (Refer to the table in the "Usage Guidelines" section below for a list of supported anomalies).
anomaly all	Monitors all anomalies.
state	Specifies the status of anomaly detection.
log	Logs detected anomalies.
trap	Sends a trap when an anomaly is detected.
quarantine	Quarantines the port on which an anomaly is detected.
period *seconds*	The time duration to observe traffic pattern, in seconds. The valid range is 5-3600
count *num*	The number of packets that must be seen during the period to trigger anomaly detection. The valid range is 1-100000.
sensitivity *num*	Sensitivity of anomaly detection to deviation from the expected traffic pattern. The valid range is 1-100.
enable	Enables the status of the state, log, trap, and quarantine parameters for the anomaly.
disable	Disables the status of the state, log, trap, and quarantine parameters for the anomaly.

Defaults

parameter	default
state enable | disable	**disable**
log enable | disable	**disable**
trap enable | disable	**disable**
quarantine enable | disable	**disable**
period *seconds*	30
sensitivity *num*	50

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to reset to default value.
- Use the parameter **period** to set the time to observe traffic on a port to detect anomalies. Accuracy and latency of algorithm is proportional to the time period.
- Use the parameter **count** to configure the minimum traffic required to activate anomaly detection. Accuracy of detection is proportional to count.
- Use the parameter **sensitivity** to check anomaly sensitivity of deviation from the expected traffic pattern. Accuracy of detection is proportional to sensitivity.
- The following table lists the **netsec anomaly** command options for specifying anomalies:

anomaly name	count defaults
arp-addr-scan	50
arp-flood	90
arp-failure	6
icmp-addr-scan	30
icmp-flood	90
icmp-unreachable	20
tcp-port-scan	20
tcp-addr-scan	30
syn-flood	90
syn-failure	10
syn-ack-scan	2
fin-scan	6
fin-ack-diff	5
rst-count	50

Examples

```
-> netsec group ad anomaly tcp-port-scan period 30
-> netsec group add anomaly arp-poisoning count 40
-> netsec group al anomaly tcp-port-scan sensitivity 90
-> netsec group ala anomaly arp-addr-scan log enable
-> netsec group a anomaly tcp-port-scan trap disable
-> no netsec group ad anomaly tcp-port-scan period
-> no netsec group al anomaly tcp-port-scan sensitivity
-> no netsec group ala anomaly arp-addr-scan quarantine
```

Release History

Release 6.3.1; command was introduced.

Related Commands

netsec group port	Associates or disassociates port-range with monitoring-group.
show netsec config	Displays the current network security configurations.

MIB Objects

```
alaNetSecMonitoringGroupTable
   alaNetSecMonitoringGroupName
   alaNetSecMonitoringGroupAnomaly
   alaNetSecMonitoringGroupAnomalyState
   alaNetSecMonitoringGroupAnomalyLog
   alaNetSecMonitoringGroupAnomalyTrap
   alaNetSecMonitoringGroupAnomalyQuarantine
   alaNetSecMonitoringGroupAnomalyCount
   alaNetSecMonitoringGroupAnomalySensitivity
   alaNetSecMonitoringGroupAnomalyPeriod
   alaNetSecMonitoringGroupRowStatus
```

show netsec summary

Displays the anomaly check summary.

show netsec [group {*grp_name* **| all} | port** *slot/port***[-***port2***]] [anomaly {***anomaly_name* **| all}] summary**

Syntax Definitions

grp_name	The name of the monitoring-group whose member-ports statistics are required.
group all	Specifies all the monitoring-groups.
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).
-port2	The last port number in a range of ports that you want to display on the same slot (e.g, 3/1-4 specifies ports 1-4 on slot 3).
anomaly_name	The type of the anomaly.
anomaly all	Monitors all anomalies.

Defaults

By default, a list of all anomalies is displayed.

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

- Use the **anomaly** and **group** parameters to list the summary of a particular anomaly that belongs to the specified monitoring-group.
- The following table show the list of anomalies:

anomaly name
arp-addr-scan
arp-flood
arp-failure
icmp-addr-scan
icmp-flood
icmp-unreachable
tcp-port-scan
tcp-addr-scan
syn-flood
syn-failure

anomaly name
syn-ack-scan
fin-scan
fin-ack-diff
rst-count

Examples

```
-> show netsec anomaly all summary
Slot
Port  Anomaly          Observed  Detected
----+---------------+-----------+-----------
2/5   arp-addr-scan           82        0
2/5   arp-flood               82        0
2/5   arp-failure             88        6
2/5   icmp-addr-scan          82        0
2/5   icmp-flood              82        0
2/5   icmp-unreachable        82        0
2/5   tcp-port-scan           82        0
2/5   tcp-addr-scan           82        0
2/5   syn-flood               82        0
2/5   syn-failure             82        0
2/5   syn-ack-scan            82        0
2/5   fin-scan                82        0
2/5   fin-ack-diff            82        0
2/5   rst-count               82        0

-> show netsec port 2/1 anomaly arp-addr-scan summary
Slot
Port  Anomaly          Observed  Detected
----+---------------+-----------+-----------
2/1   arp-addr-scan    7         1
```

output definitions

Slot/Port	Slot number for the module and physical port number on that module.
Anomaly	The type of anomaly.
Observed	The number of times an anomaly was checked for this port since monitoring was enabled.
Detected	The number of times an anomaly was detected on this port since monitoring was enabled.

Release History

Release 6.3.1; command was introduced.

Related Commands

netsec group port	Associates or disassociates port-range with monitoring-group.
netsec group anomaly	Configures the monitoring period of an anomaly for a port-group, packet count configuration for triggering anomaly detection, anomaly detection algorithm's sensitivity to discrepancy in standard and observed traffic pattern.

MIB Objects

```
alaNetSecPortAnomalySummaryTable
   alaNetSecPortAnomalySummaryIfId
   alaNetSecPortAnomalySummaryAnomaly
   alaNetSecPortAnomalySummaryObserved
   alaNetSecPortAnomalySummaryDetected
```

show netsec traffic

Displays anomaly specific traffic statistics.

show netsec [group {*group-name* **| all} | port** *slot/port1***[-***port2***]] [anomaly {***anomaly_name* **| all}] traffic**

Syntax Definitions

group-name	The name of the monitoring-group.
group all	Specifies all the monitoring-groups.
slot/port1	The slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
-port2	The last port number in a range of ports that you want to configure on the same slot (e.g, 3/1-4 specifies ports 1-4 on slot 3).
anomaly_name	The type of the anomaly.
anomaly all	Monitors all anomalies.

Defaults

By default, a list of all anomalies traffic is displayed.

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

To display trafffic for a particular monitoring-group, specify only the **group** parameter.

Examples

```
-> show netsec anomaly all traffic
Slot
Port   Anomaly          Packet     Curr-in    Curr-out    Last-in    Last-out
----+---------------+-----------+---------+------------+----------+-----------
2/5   arp-addr-scan    arp-rep      -          0           -          0
2/5   arp-addr-scan    arp-req      0          -           0          -
2/5   arp-flood        arp-rep      0          0           0          0
2/5   arp-flood        arp-req      0          -           0          -
2/5   arp-failure      arp-rep      -          0           -          0
2/5   arp-failure      arp-req      0          -           0          -
2/5   icmp-addr-scan   icmp-rep     -          0           -          0
2/5   icmp-addr-scan   icmp-req     0          -           0          -
2/5   icmp-flood       icmp-rep     -          0           -          0
2/5   icmp-flood       icmp-req     0          0           0          0
2/5   icmp-unreachable icmp-dnr     0          0           0          0
2/5   tcp-port-scan    syn-only     0          0           0          0
2/5   tcp-port-scan    syn-ack      0          0           0          0
2/5   tcp-port-scan    rst          0          0           0          0
2/5   tcp-addr-scan    syn-only     0          -           0          -
2/5   tcp-addr-scan    syn-ack      -          0           -          0
```

```
2/5   tcp-addr-scan    rst          -          0          -          0
2/5   syn-flood        syn-only     0          0          0          0
2/5   syn-flood        syn-ack      0          0          0          0
2/5   syn-failure      syn-only     0          -          0          -
2/5   syn-failure      syn-ack      -          0          -          0
2/5   syn-ack-scan     syn-ack      0          0          0          0
2/5   syn-ack-scan     syn-nack     0          0          0          0
2/5   fin-scan         fin-nack     0          0          0          0
2/5   fin-ack-diff     fin-ack      0          0          0          0
2/5   rst-count        rst          0          0          0          0
```

```
-> show netsec group test1 anomaly arp-addr-scan traffic
Slot
Port  Anomaly          Packet      Curr-in    Curr-out   Last-in    Last-out
----+----------------+-----------+----------+----------+----------+-----------
2/1   arp-addr-scan    arp-rep     -          0          -          0
2/1   arp-addr-scan    arp-req     1500       -          1746       -
2/2   arp-addr-scan    arp-rep     -          0          -          0
2/2   arp-addr-scan    arp-req     0          -          0          -
```

output definitions

Slot/Port	Slot number for the module and physical port number on that module.
Anomaly	The type of anomaly.
Packet	The packet being monitored.
Curr-in	The number of incoming packets during the current monitoring period.
Curr-out	The number of outgoing packets during the current monitoring period.
Last-in	The number of incoming packets during the last monitoring period.
Last-out	The number of outgoing packets during the last monitoring period.

Release History

Release 6.3.1; command was introduced.

Related Commands

netsec group port	Associates or disassociates port-range with monitoring-group.
netsec group anomaly	Configures the monitoring period of an anomaly for a port-group, packet count configuration for triggering anomaly detection, anomaly detection algorithm's sensitivity to discrepancy in standard and observed traffic pattern.
show netsec statistics	Displays the pattern counts on ports.

MIB Objects

```
alaNetSecPortAnomalyStatsTable
   alaNetSecPortAnomalyStatsIfId
   alaNetSecPortAnomalyStatsAnomaly
   alaNetSecPortAnomalyStatsPacket
   alaNetSecPortAnomalyStatsCurrentIngress
   alaNetSecPortAnomalyStatsCurrentEgress
   alaNetSecPortAnomalyStatsLastIngress
   alaNetSecPortAnomalyStatsLastIngress
```

show netsec statistics

Displays the pattern counts on ports.

show netsec [group {*grp_name* **| all} | port** *slot/port***[-***port2***]] statistics**

Syntax Definitions

grp_name	The name of the port-group (up to 16 characters).
group all	Specifies all the monitoring-groups.
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).
port2	The last port number in a range of ports that you want to configure on the same slot (e.g, 3/1-4 specifies ports 1-4 on slot 3).

Defaults

By default, a list of all pattern counts is displayed.

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

To display statistics for a particular monitoring-group, specify only the **group** parameter.

Examples

```
-> show netsec statistics
Slot
Port       Packet       Last-In       Last-Out      Total-In      Total-Out
-------+------------+------------+-------------+-------------+------------
2/5        arp-rep        0              0             0            0
2/5        arp-req        0              -             0            -
2/5        icmp-rep       0              0             0            0
2/5        icmp-req       0              0             0            0
2/5        icmp-dnr       0              0             0            0
2/5        syn-only       0              0             0            0
2/5        syn-ack        0              0             0            0
2/5        syn-nack       0              0             0            0
2/5        fin-ack        0              0             0            0
2/5        fin-nack       0              0             0            0
2/5        rst            0              0             0            0
2/7        arp-rep        0              0             0            0
2/7        arp-req        0              -             0            -
2/7        icmp-rep       0              0             0            0
2/7        icmp-req       0              0             0            0
2/7        icmp-dnr       0              0             0            0
2/7        syn-only       0              0             0            0
2/7        syn-ack        0              0             0            0
2/7        syn-nack       0              0             0            0
```

```
2/7        fin-ack        0              0              0            0
2/7        fin-nack       0              0              0            0
2/7        rst            0              0              0            0


-> show netsec group test1 statistics
Slot
Port  Packet         Last-In  Last-Out  Total-In   Total-Out
-----+--------------+--------+---------+---------+-----------
2/5   arp-rep           0         0         0         0
2/5   arp-req           0         -         0         -
2/5   icmp-rep          0         0         0         0
2/5   icmp-req          0         0         0         0
2/5   icmp-dnr          0         0         0         0
2/5   syn-only          0         0         0         0
2/5   syn-ack           0         0         0         0
2/5   syn-nack          0         0         0         0
2/5   fin-ack           0         0         0         0
2/5   fin-nack          0         0         0         0
2/5   rst               0         0         0         0

-> show netsec port 2/7 statistics

Slot
Port  Packet         Last-In  Last-Out  Total-In   Total-Out
-----+--------------+--------+---------+---------+-------------
2/7   arp-rep           0         0         0         0
2/7   arp-req           0         -         0         -
2/7   icmp-rep          0         0         0         0
2/7   icmp-req          0         0         0         0
2/7   icmp-dnr          0         0         0         0
2/7   syn-only          0         0         0         0
2/7   syn-ack           0         0         0         0
2/7   syn-nack          0         0         0         0
2/7   fin-ack           0         0         0         0
2/7   fin-nack          0         0         0         0
2/7   rst               0         0         0         0
```

output definitions

Slot/Port	Slot number for the module and physical port number on that module.
Packet	The packet being monitored.
Last-In	The number of incoming packets observed during the last 5 seconds.
Last-Out	The number of outgoing packets observed during the last 5 seconds.
Total-In	The total number of incoming packets observed since monitoring was enabled.
Total-Out	The total number of outgoing packets observed since monitoring was enabled.

Release History

Release 6.3.1; command was introduced.

Related Commands

netsec group port	Associates or disassociates port-range with monitoring-group.
netsec group anomaly	Configures the monitoring period of an anomaly for a port-group, packet count configuration for triggering anomaly detection, anomaly detection algorithm's sensitivity to discrepancy in standard and observed traffic pattern.
show netsec traffic	Displays anomaly specific traffic statistics.

MIB Objects

```
alaNetSecPortStats
   alaNetSecPortStatsIfId
   alaNetSecPortStatsPacket
   alaNetSecPortStatsLastIngress
   alaNetSecPortStatsLastEgress
   alaNetSecPortStatsTotalIngress
   alaNetSecPortStatsTotalEgress
```

show netsec config

Displays the current network security configurations.

show netsec [group {*grp_name* **| all}] [anomaly {***anomaly_name* **| all}] config**

Syntax Definitions

group-name	The name of the monitoring-group whose member-ports statistics are required.
group all	Specifies all the monitoring-groups.
anomaly_name	The type of the anomaly.
anomaly all	Monitors all anomalies.

Defaults

By default, a list of all anomalies configuration is displayed.

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

To display the security configuration for a particular monitoring-group, specify only the **group** parameter.

Examples

```
-> show netsec config
Group                  Anomaly          S  L  T  Q     Per     Cnt      Sen
---------------------+---------------+----+--+--+---+-------+---------+------------
h                      arp-addr-scan    E  E  -  -       -       -          -
h                      arp-flood        E  E  -  -       -       -          -
h                      arp-failure      E  E  -  -       -       -          -
h                      icmp-addr-scan   E  E  -  -       -       -          -
h                      icmp-flood       E  E  -  -       -       -          -
h                      icmp-unreachable E  E  -  -       -       -          -
h                      tcp-port-scan    E  E  -  -       -       -          -
h                      tcp-addr-scan    E  E  -  -       -       -          -
h                      syn-flood        E  E  -  -       -       -          -
h                      syn-failure      E  E  -  -       -       -          -
h                      syn-ack-scan     E  E  -  -       -       -          -
h                      fin-scan         E  E  -  -       -       -          -
h                      fin-ack-diff     E  E  -  -       -       -          -
h                      rst-count        E  E  -  -       -       -          -
test1                  tcp-addr-scan    E  E  E  -      10       -          -
```

```
-> show netsec group test1 anomaly arp-addr-scan config
Group                          Anomaly          S L T Q  Per   Cnt     Sen
-----------------------------+----------------+---+-+-+--+-----+-----+----------
test1                          arp-addr-scan    E E E -   -     -       -
```

output definitions

Group	The name of the monitoring-group.
Anomaly	The anomaly type of the monitoring group.
S	The current state (- indicates Not configured, E indicates enabled, and D indicates disabled).
L	Log (- indicates Not configured, E indicates enabled, and D indicates disabled).
T	Trap (- indicates Not configured, E indicates enabled, and D indicates disabled).
Q	Quarantine (- indicates Not configured, E indicates enabled, and D indicates disabled).
Per	Anomaly monitoring period (- indicates Not configured)
Cnt	Anomaly detection threshold (- indicates Not configured)
Sen	Anomaly sensitivity (- indicates Not configured)

Release History

Release 6.3.1; command was introduced.

Related Commands

netsec group anomaly	Configures the monitoring period of an anomaly for a port-group, packet count configuration for triggering anomaly detection, anomaly detection algorithm's sensitivity to discrepancy in standard and observed traffic pattern.
show netsec operation	Displays the network security operational conditions at per port anomaly level.

MIB Objects

```
alaNetSecMonitoringGroupConfig
   alaNetSecMonitoringGroupName
   alaNetSecMonitoringGroupAnomaly
   alaNetSecMonitoringGroupAnomalyState
   alaNetSecMonitoringGroupAnomalyLog
   alaNetSecMonitoringGroupAnomalyTrap
   alaNetSecMonitoringGroupAnomalyQuarantine
   alaNetSecMonitoringGroupAnomalyCount
   alaNetSecMonitoringGroupAnomalySensitivity
   alaNetSecMonitoringGroupAnomalyPeriod
```

show netsec operation

Displays the network security operational conditions.

show netsec [group {*grp_name* **| all} | port** *slot/port***[-***port2***]] [anomaly {***anomaly_name* **| all}] operation**

Syntax Definitions

grp_name	The name of the port-group (up to 16 characters).
group all	Specifies all the monitoring-groups.
slot/port1	The slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
-port2	The last port number in a range of ports that you want to configure on the same slot (e.g, 3/1-4 specifies ports 1-4 on slot 3).
anomaly_name	The type of the anomaly.
anomaly all	Monitors all anomalies.

Defaults

By default, the network security operational condition of all the anomalies is displayed.

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

To display the network security operational condition for a particular monitoring-group, specify only the **group** parameter.

Examples

```
-> show netsec operation
Port-Range
Group            Anomaly           S   L   T   Q     Per       Cnt         Sen
-------------+------------------+---+---+---+---+-------+----------+----------
h              arp-addr-scan       E   E   D   D      30        30         50
h              arp-flood           E   E   D   D      30        90         50
h              arp-failure         E   E   D   D      30        6          50
h              icmp-addr-scan      E   E   D   D      30        30         50
h              icmp-flood          E   E   D   D      30        90         50
h              icmp-unreachable    E   E   D   D      30        20         50
h              tcp-port-scan       E   E   D   D      30        20         50
h              tcp-addr-scan       E   E   D   D      30        30         50
h              syn-flood           E   E   D   D      30        90         50
h              syn-failure         E   E   D   D      30        10         50
h              syn-ack-scan        E   E   D   D      30        2          50
h              fin-scan            E   E   D   D      30        6          50
h              fin-ack-diff        E   E   D   D      30        5          50
h              rst-count           E   E   D   D      30        50         50
```

```
test1          arp-addr-scan       D   D   D   D      30        30         50
test1          arp-flood           D   D   D   D      30        90         50
test1          arp-failure         D   D   D   D      30        6          50
test1          icmp-addr-scan      D   D   D   D      30        30         50
test1          icmp-flood          D   D   D   D      30        90         50
test1          icmp-unreachable    D   D   D   D      30        20         50
test1          tcp-port-scan       D   D   D   D      30        20         50
test1          tcp-addr-scan       E   E   E   D      10        30         50
test1          syn-flood           D   D   D   D      30        90         50
test1          syn-failure         D   D   D   D      30        10         50
test1          syn-ack-scan        D   D   D   D      30        2          50
test1          fin-scan            D   D   D   D      30        6          50
test1          fin-ack-diff        D   D   D   D      30        5          50
test1          rst-count           D   D   D   D      30        50         50
default        arp-addr-scan       E   E   D   D      30        30         50
default        arp-flood           E   E   D   D      30        90         50
default        arp-failure         E   E   D   D      30        6          50
default        icmp-addr-scan      E   E   D   D      30        30         50
default        icmp-flood          E   E   D   D      30        90         50
default        icmp-unreachable    E   E   D   D      30        20         50
default        tcp-port-scan       E   E   D   D      30        20         50
default        tcp-addr-scan       E   E   D   D      30        30         50
default        syn-flood           E   E   D   D      30        90         50
default        syn-failure         E   E   D   D      30        10         50
default        syn-ack-scan        E   E   D   D      30        2          50
default        fin-scan            E   E   D   D      30        6          50
default        fin-ack-diff        E   E   D   D      30        5          50
default        rst-count           E   E   D   D      30        50         50

-> show netsec group test1 operation
Port-Range
Group                           Anomaly          S L T Q Per  Cnt        Sen
--------------------------------+----------------+---+-+-+--+---+-------+--------
test1                           arp-addr-scan    E E E D 30   30         50
test1                           arp-flood        D D D D 30   90         50
test1                           arp-poisoning    D D D D 30   6          50
test1                           arp-failure      D D D D 30   6          50
test1                           icmp-addr-scan   D D D D 30   30         50
test1                           icmp-flood       D D D D 30   90         50
test1                           icmp-unreachable D D D D 30   20         50
test1                           tcp-port-scan    D D D D 30   20         50
test1                           tcp-addr-scan    D D D D 30   30         50
test1                           syn-flood        D D D D 30   90         50
test1                           syn-failure      D D D D 30   10         50
test1                           syn-ack-scan     D D D D 30   2          50
test1                           fin-scan         D D D D 30   6          50
test1                           fin-ack-diff     D D D D 30   5          50
test1                           rst-count        D D D D 30   50         50
```

output definitions

Slot/Port	Slot number for the module and physical port number on that module.
Port-Range group	Range of ports or name of the monitoring-group.
Anomaly-Type	The anomaly type of the monitoring group.
S	The current state (- indicates Not configured, E indicates enabled, and D indicates disabled).

output definitions (continued)

L	Log (- indicates Not configured, E indicates enabled, and D indicates disabled).
T	Trap (- indicates Not configured, E indicates enabled, and D indicates disabled).
Q	Quarantine (- indicates Not configured, E indicates enabled, and D indicates disabled).
Per	Anomaly monitoring period (- indicates Not configured)
Cnt	Anomaly detection threshold (- indicates Not configured)
Sen	Anomaly sensitivity (- indicates Not configured)

Release History

Release 6.3.1; command was introduced.

Related Commands

netsec group anomaly	Configures the monitoring period of an anomaly for a port-group, packet count configuration for triggering anomaly detection, anomaly detection algorithm's sensitivity to discrepancy in standard and observed traffic pattern.
show netsec config	Displays the current network security configurations.

MIB Objects

```
alaNetSecPortOp
   alaNetSecPortOpIfId
   alaNetSecPortOpAnomaly
   alaNetSecPortOpState
   alaNetSecPortOpLog
   alaNetSecPortOpTrap
   alaNetSecPortOpQuarantine
   alaNetSecPortOpCount
   alaNetSecPortOpSensitivity
   alaNetSecPortOpPeriod
```

show netsec group port

Displays the group membership of ports.

show netsec {group {*grp_name* **| all} | port** *slot/port* **[-***port2***]}**

Syntax Definitions

grp_name	The name of the port-group (up to 16 characters).
all	Specifies all the monitoring-groups.
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).
port2	The last port number in a range of ports that you want to configure on the same slot (e.g, 3/1-4 specifies ports 1-4 on slot 3).

Defaults

N/A

Platforms Supported

OmniSwitch 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show netsec group all
Slot/Port Port-RangeGroup
---------+----------------------------
2/5                 a
2/7                 b

-> show netsec group a
Slot/Port Port-RangeGroup
---------+----------------------------
2/5             a

-> show netsec port 2/7
Slot/Port Port-RangeGroup
---------+-----------------------------
2/7             b

-> show netsec group a port 2/5
Slot/Port Port-RangeGroup
---------+-----------------------------
2/5             a
```

output definitions

Slot/Port	Slot number for the module and physical port number on that module.
Group	The name of the monitoring-group.

Release History

Release 6.3.1; command was introduced.

Related Commands

netsec group port	Associates or disassociates port-range with monitoring-group.

MIB Objects

```
alaNetSecPortRangeGroup
   alaNetSecPortRangeGroupStartfId
   alaNetSecPortRangeGroupEndfId
   alaNetSecPortRangeGroupName
```

45 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)
port mapping unknown-unicast-flooding
port mapping dynamic-proxy-arp
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 6400, 6850E, 6855, 9000E

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 6.1.2; 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 6400, 6850E, 6855, 9000E

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 6.1.2; 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.
port mapping dynamic-proxy-arp	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 6400, 6850E, 6855, 9000E

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 6.1.2; 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
```

port mapping unknown-unicast-flooding

Enables or disables flooding of unknown unicast traffic from all ports to user ports for a particular session.

port mapping *session id* **unknown-unicast-flooding {enable | disable}**

Synatax Definitions

session id	The port mapping session for which the unknown unicast flooding status is to be configured.
enable	Enables the flooding of unknown unicast traffic from all ports to the user ports for a particular session.
disable	Disables the flooding of unknown unicast traffic from all ports to the user ports for a particular session.

Defaults

parameter	default
enable | disable	**enable**

Platform Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Flooding of unknown unicast traffic is enabled by default.
- Unknown unicast flooding for the user ports will be enabled if port mapping is disabled on a session.
- Configuring unknown unicast flooding will create a new port mapping session if there is no existing session.
- When a link aggregate is configured as a user port, the unknown unicast flooding configuration will be applied to all the member ports of the aggregate.
- Enabling this command affects unicast flooding to the user ports from all the switch ports, not just the network ports for the session.

Examples

```
-> portmapping 1 unknown-unicast-flooding enable
-> portmapping 2 unknown-unicast-flooding disable
```

Release History

Release 6.3.4; 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.
port mapping dynamic-proxy-arp	Displays the status of one or more port mapping sessions.

MIB Objects

```
portMappingSessionTable
   pmapSessionUnknownUnicastFloodStatus
```

port mapping dynamic-proxy-arp

Enables or disables the dynamic proxy arp functionality for the port mapping session.

port mapping *session id* **dynamic-proxy-arp {enable | disable}**

Synatax Definitions

session id	The port mapping session for which the dynamic proxy arp status is to be configured.
enable	Enables the dynamic proxy arp status.
disable	Disables the dynamic proxy arp status.

Defaults

parameter	default
enable | disable	**disable**

Platform Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Clients must be connected to the user-ports and the head end routers connected to the network-ports of the port mapping session for dynanic proxy arp to function properly.
- DHCP snooping must be enabled for dynamic proxy arp to function.
- Using dynamic-proxy-arp in conjunction with DHCP snooping allows for the configuation of the MAC Forced Forwarding feature.

Examples

```
-> portmapping 1 dynamic-proxy-arp enable
-> portmapping 1 dynamic-proxy-arp disable
```

Release History

Release 6.4.3; 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.
show port mapping status	Displays the status of one or more port mapping sessions.

MIB Objects

```
portMappingSessionTable
   pmapSessionDynProxyARP
```

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 6400, 6850E, 6855, 9000E

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          Unknown Unicast    DPA Status
------------+-----------------+--------------+-----------------+------------
     1            uni           enable          flood               disable
     2            uni           enable          drop                enable
     3            bi            disable         drop                disable
     4            bi            enable          flood               disable
     7            bi            disable         flood               enable
     8            bi            disable         flood               enable
```

output definitions

SessionID	Displays the port mapping session ID.
Direction	Displays the direction of a port mapping session.
Status	Displays the status of a port mapping session.
Unknown unicast	Displays the status of unknown unicast flooding
DPA Status	Displays the status of Dynamic Proxy ARP.

Release History

Release 6.1.2; command was introduced.
Release 6.3.4; **unknown unicast** field added.
Release 6.4.3; DPA Status field added

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.
port mapping unknown-unicast-flooding	Enables or disables flooding of unknown unicast traffic from all ports to user ports for a particular session.

MIB Objects

```
portMappingSessionTable
   pmapSessionNumber
   pmapSessionDirection
   pmapSessionStatus
   pmapSessionUnknownUnicastFloodStatus
   pmapSessionDynProxyARP
```

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 6400, 6850E, 6855, 9000E

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 6.1.2; 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
   pmapSessionUnknownUnicastFloodStatus
```

46 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 max-filtering
port-security convert-to-static
port-security mac
port-security mac-range
port-security violation
port-security release
port-security learn-trap-threshold
show port-security
show port-security shutdown
show port-security brief

port-security

Enables or disables Learned Port Security (LPS) on the switch port(s). When LPS is enabled, only devices that have a source MAC address that complies with LPS restrictions are learned on the port(s).

port-security *slot/port***[**-*port2***] [admin-status {enable | disable | locked}]**

port-security chassis {convert-to-static | disable}

no port security *slot/port***[**-*port2***]**

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
-port2	The last port number in a range of ports you want to configure on the same slot (for example, 3/1-4 specifies ports 1-4 on slot 3).
enable	Enables LPS on the specified port(s).
disable	Disables LPS on the specified port(s).
locked	Disables source learning on the specified LPS port(s).
chassis disable	Disables all LPS-eligible ports on the chassis.
chassis convert-to-static	Converts the learned bridge MAC address on all LPS port(s) into static MAC address. This does not apply to filtering MAC addresses.

Defaults

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

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove LPS and clear all entries from the table. This command enables the switch port to learn new MAC addresses.
- Use the **locked** parameter to disable the learning on the port. All MAC addresses are flushed and the packets are dropped.
- The **port-security chassis disable** command disables all the LPS-eligible ports on the chassis. Disabling port security restricts a port from learning new MAC addresses.
- Use the **port-security chassis convert-to-static** command to stop the aging-out of MAC address learned on the LPS ports.
- LPS is supported on 10/100 and Gigabit Ethernet fixed, mobile, authenticated, 802.1Q tagged ports, and 802.1x ports.

- LPS is not supported on 10 Gigabit Ethernet, link aggregate, or 802.1Q tagged link aggregate (trunked) ports.
- 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 admin-status enable
-> port-security 2/1-10 admin-status enable
-> port-security 2/11-15 admin-status disable
-> port-security 4/3 admin-status locked
-> no port-security 1/1-12
-> port-security chassis disable
-> port-security chassis convert-to-static
```

Release History

Release 6.1; command was introduced.
Release 6.1.5; **chassis** parameter was added.
Release 6.4.4; **admin-status**, **locked** and **convert-to-static** parameters added.

Related Commands

port-security mac	Configures a single authorized source MAC address for a port that belongs to a specified VLAN.
port-security mac-range	Configures a list of authorized MAC addresses by defining a range of addresses allowed on the port.
port-security maximum	Specifies the maximum number of source MAC addresses that an LPS port(s) is allowed to learn.
port-security shutdown	Configures 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(s).

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. 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. This command also enables or disables the conversion of dynamic MAC addresses to static MAC addresses on LPS ports.

port-security shutdown *num* **[convert-to-static {enable | disable}] [no-aging {enable | disable}] [boot-up {enable | disable}] [learn-as-static {enable | disable}] [mac-move {enable | disable}] default**

Syntax Definitions

num	The number of minutes during which LPS allows source learning across all LPS ports. This amount of time defines the LPS learning window. Learning window value can range from 0-65535 (in minutes).
convert-to-static enable	Converts dynamically learned MAC addresses to static MAC addresses.
convert-to-static disable	Disables conversion of dynamically learned MAC addresses to static MAC addresses.
no-aging enable	Prevents dynamically learned MAC addresses from aging out or getting flushed during the LPS learning window time period.
no-aging disable	Allows dynamically learned MAC addresses to age out or get flushed during the LPS learning window time period.
boot-up enable	Enables the automatic start of the LPS learning window timer when the switch restarts.
boot-up disable	Disables the start of the LPS learning window timer when the switch restarts.
learn-as-static enable	All MACs will be learnt as static directly during the learning window(finite/infinite).
learn-as-static disable	All dynamic MACs will be learnt as pseudo-static or bridge during the learning window based on the no-aging option.
mac-move enable	Allows movement of pseudo-static MAC.
mac-move disable	Movement of pseudo-static MAC is not allowed.
default	All parameters related to the shutdown window will be set to default values. To use this option, shutdown option should be set to zero.

Defaults

By default, the LPS source learning time limit is not set for the switch.

parameter	default
convert-to-static	disable
no-aging	disable

parameter	default
boot-up	**enable**
learn-as-static	**disable**
mac-move	**disable**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The LPS source learning time window is started and/or reset each time the **port-security shutdown** command is issued or when the **port-security shutdown boot-up** option is enabled and the switch restarts.
- When "no-aging" is enabled on an LPS port, the MAC addresses are automatically learned as pseudo static MAC addresses during the LPS learning window time period. (Pseudo static MAC addresses are the MAC addresses that are learned dynamically in the system and are converted to static in the hardware). These learned MAC addresses are not affected by aging and flushing operations that occur during the learning window. Once the learning window expires, if the "convert-to-static" option is disabled, these MAC addresses remain as pseudo static. Else if "convert-to-static" is enabled, MAC is converted to static address.
- The MAC addresses entering the LPS enabled port is learnt as filtered MAC after the learning window expires in the system. The maximum number of filtered MAC addresses that can be learned is limited by a configurable parameter ‘max-filtering’.
- For example, consider a scenario where maximum number of MAC addresses allowed is set to 30 and maximum filtering allowed is 7. If the learning window expires, then only the filtering MAC addresses up to “seven" is learned. After learning seven filtering MAC addresses, the port goes to violation state.
- For example, consider a scenario where maximum MAC address is set to 5, and the max-filtering value is set to 10. If the learning window is running, and if five MAC addresses are learned on the port, then the other ten new MAC addresses is learned as filtering MAC addresses. The 11th MAC puts the port in violation state.
- If the **convert-to-static** parameter is enabled and the LPS source learning time window expires, then all the dynamic MAC addresses are converted to static MAC addresses. This stops the MAC addresses from aging out.
- The conversion of dynamic MAC addresses to static does not apply to LPS mobile and authenticated ports.
- With ‘**learn-as-static**’ option enabled the MAC addresses will be directly learnt as static during learning window, without manually enabling the 'convert-to-static' option. This can be used only when 'no-aging' option is enabled.
- With ‘**mac-move**’ option enabled, a pseudo static MAC is allowed to move from one port to another. Unlike duplicate static mac, no information will be retained on the old port upon pseudo-static mac movement. This can be used only when 'no-aging' option is enabled.
- Infinite learning window will be allowed on boot-up, no-aging, learn-as-static, mac-move, and shutdown. With the shutdown time set to ‘0’ all the option for the learning window can be used.

- The **port-security shutdown 0 default** option can be used to set all the options for learning window to their default values.

Examples

```
-> port-security shutdown 25
-> port-security shutdown 60 no-aging enable
-> port-security shutdown 2 convert-to-static enable no-aging enable
-> port-security shutdown 2 convert-to-static enable no-aging enable boot-up enable
-> port-security shutdown 20 no-aging enable learn-as-static enable
-> port-security shutdown 20 no-aging enable mac-move enable
-> port-security shutdown 0 no-aging enable convert-to-static enable boot-up enable
-> port-security shutdown 0 default
```

Release History

Release 6.1; command was introduced.
Release 6.1.5; **convert-to-static** parameter added.
Release 6.4.4; **no-aging** and **boot-up** parameters added.
Release 6.4.5; **learn-as-static**, **mac-move**, and **default** parameters added.

Related Commands

port-security	Enables or disables Learned Port Security (LPS) on the switch port(s).
port-security mac	Configures a single authorized source MAC address for a port that belongs to a specified VLAN.
port-security mac-range	Configures a list of authorized MAC addresses by defining a range of addresses allowed on the port.
port-security maximum	Specifies the maximum number of source MAC addresses that an LPS port(s) is allowed to learn.
port-security violation	Selects the method for handling traffic that does not comply with LPS restrictions for the specified port.

MIB Objects

```
learnedPortSecurityGlobalGroup
   lpsLearningWindowTime
   lpsLearningWindowTimeWithStaticConversion
   lpsLearningWindowNoAging
   lpsLearningWindowBootupStatus
   lpsLearningWindowLearnAsStatic
   lpsLearningWindowPseudoMacMove
```

port-security maximum

Configures the maximum number of source MAC addresses that an LPS port(s) is allowed to learn.

port-security *slot/port***[**-*port2***]** **maximum** *num*

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
-port2	The last port number in a range of ports you want to configure on the same slot (for example, 3/1-4 specifies ports 1-4 on slot 3).
maximum *num*	The number of source MAC addresses that are allowed on this port. Valid range is 1-1000.

Defaults

By default, the number of MAC addresses allowed is set to 1.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 the LPS port will handle violating traffic.
- If an LPS port is in a violation state and the maximum number of MAC addresses allowed is changed, the port transitions out of the violation state.
- 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
-> port-security 1/2 maximum 5 learn-trap-threshold 4
```

Release History

Release 6.1; command was introduced.

Related Commands

port-security	Enables or disables Learned Port Security (LPS) on the switch port(s).
port-security mac	Configures a single authorized source MAC address for a port that belongs to a specified VLAN.
port-security mac-range	Configures a list of authorized MAC addresses by defining a range of addresses allowed on the port.
port-security shutdown	Configures the amount of time in minutes to allow source learning on all LPS ports. Also, enables or disables the conversion of dynamic MAC addresses to static MAC addresses on 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 max-filtering

Configures the maximum number of filtered MAC addresses that can be learned on an LPS port.

port-security *slot/port***[**-*port2***]** **max-filtering** *num*

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
-port2	The last port number in a range of ports you want to configure on the same slot (for example, 3/1-4 specifies ports 1-4 on slot 3).
max-filtering *num*	The maximum number of filtered MAC addresses that can be learned on an LPS port. Valid range is 0–100.

Defaults

By default, the maximum number of filtered MAC addresses that can be learned on an LPS port is set to 5.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- When the LPS learning window time expires, MAC addresses are learned in a filtering state up to the maximum filtering value set with this command. For example, if the maximum filtering value is set to five, when the learning window time expires, the switch will learn up to five filtering MAC addresses.
- If an LPS port is in a violation state and the maximum number of filtering MAC addresses allowed is changed, the port transitions out of the violation state.
- The maximum filtering value is separate from the maximum bridged MAC address value.
- When the number of filtered MAC addresses learned on the port reaches the maximum, either the port is disabled (Shutdown Violation mode) or MAC address learning is disabled (Restrict Violation mode). By default, MAC address learning is disabled on a port.

Examples

```
-> port-security 1/10 max-filtering 6
-> port-security 1/10-13 max-filtering 18
```

Release History

Release 6.1.5; command was introduced.

Related Commands

port-security maximum	Specifies the maximum number of source MAC addresses that an LPS port(s) is allowed to learn.
port-security violation	Selects the method for handling traffic that does not comply with LPS restrictions for the specified port.

MIB Objects

```
learnedPortSecurityTable
   lpsMaxFilteredMacNum
```

port-security convert-to-static

Converts the dynamically learned MAC addresses on the LPS ports to static MAC addresses.

port-security {*slot/port***[***-port2***]** | **chassis} convert-to-static**

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
-port2	The last port number in a range of ports you want to configure on the same slot (for example, 3/1-4 specifies ports 1-4 on slot 3).
chassis	Specifies all the LPS-eligible ports on the chassis.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- You can stop the aging out of dynamic MAC addresses on the LPS ports by converting them to static MAC addresses.
- The conversion of dynamic MAC addresses to static ones does not apply to LPS mobile and authenticated ports.
- The number of converted static MAC addresses cannot exceed the maximum number of MAC addresses allowed on the ports.

Examples

```
-> port-security 4/8 convert-to-static
```

Release History

Release 6.1.5; command was introduced.

Related Commands

port-security	Enables or disables Learned Port Security (LPS) on the switch port(s).
port-security maximum	Specifies the maximum number of source MAC addresses that an LPS port(s) is allowed to learn.

MIB Objects

```
learnedPortSecurityGlobalGroup
   lpsConvertToStatic
```

port-security mac

Configures a single authorized source MAC address for a port that belongs to a specified VLAN.

port-security *slot/port* **mac** *mac_address* **[vlan** *vlan_id***]**

port-security *slot/port* **no mac {all** | *mac_address***} [vlan** *vlan_id***]**

Syntax Definitions

slot/port	Enter the slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
mac_address	The source MAC address (for example, 00:da:39:59:f1:0c) of the port.
all	Flushes all MAC addresses associated with the specified port.
vlan_id	The VLAN or the tagged VLAN to which the LPS port belongs. The range is 1–4094.

Defaults

By default, the default VLAN ID of the port is used.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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.
- LPS must be enabled on the port before configuring a MAC address. If an attempt is made to configure a MAC address on a non-LPS port, an error message is displayed.
- The additional source MAC addresses received on the LPS port which do not match the 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.
You can use the **port-security mac** command to configure the same static MAC on multiple ports. A static LPS MAC is allowed to move between ports belonging to the same VLAN. The system supports a maximum of 64 such entries.

```
Example:
-> vlan 2
-> vlan 2 port default 1/3
```

```
-> vlan 2 port default 1/4
-> port-security 1/3 mac 00:00:00:00:00:01
-> port-security 1/4 mac 00:00:00:00:00:01
```

Examples

```
-> port-security 4/20 mac 00:20:95:00:fa:5c vlan 2
-> port-security 2/11 no mac 00:20:95:00:fa:5c
-> port-security 1/2 no mac all
```

Release History

Release 6.1; command was introduced.
Release 6.1.5; **vlan** parameter was added.

Related Commands

port-security	Enables or disables Learned Port Security (LPS) on the switch port(s).
port-security mac-range	Configures a list of authorized MAC addresses by defining a range of addresses allowed on the port.
port-security shutdown	Configures the amount of time in minutes to allow source learning on all LPS ports. Also, enables or disables the conversion of dynamic MAC addresses to static MAC addresses on LPS ports.
port-security maximum	Specifies the maximum number of source MAC addresses that an LPS port(s) is allowed to learn.
port-security violation	Selects the method for handling traffic that does not comply with LPS restrictions for the specified port.

MIB Objects

```
learnedPortSecurityL2MacAddressTable
   lpsL2MacAddress
   lpsL2VlanId
   lpsL2MacAddressRowStatus
```

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***[**-*port2***] mac-range [low** *mac_address* | **high** *mac_address***]**

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
-*port2*	The last port number in a range of ports you want to configure on the same slot (for example, 3/1-4 specifies ports 1-4 on slot 3).
low *mac_address*	MAC address that defines the low end of a range of MACs (for example, 00:20:95:00:10:2A).
high *mac_address*	MAC address that defines the high end of a range of MACs (for example, 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 6400, 6850E, 6855, 9000E

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 three configured authorized MAC addresses and the maximum number of addresses allowed is set to 10, then only seven additional MAC addresses are allowed on that port.

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 6.1; command was introduced.

Related Commands

port-security	Enables or disables Learned Port Security (LPS) on the switch port(s).
port-security mac	Configures a single authorized source MAC address for a port that belongs to a specified VLAN.
port-security shutdown	Configures the amount of time in minutes to allow source learning on all LPS ports. Also, enables or disables the conversion of dynamic MAC addresses to static MAC addresses on LPS ports.
port-security maximum	Specifies the maximum number of source MAC addresses that an LPS port(s) is allowed to learn.
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
   lpsRowStatus
```

port-security violation

Configures the violation mode in which the LPS port operates when unauthorized traffic is received on that port. This mode determines if the port is shut down, remains up but discards traffic, or allows LPS compliant traffic while filtering unauthorized traffic.

port-security *slot/port***[**-*port2***] violation {shutdown | restrict | discard}**

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
-*port2*	The last port number in a range of ports you want to configure on the same slot (for example, 3/1-4 specifies ports 1-4 on slot 3).
restrict	Filters (blocks) unauthorized traffic but allows traffic that complies with LPS restrictions to forward on the port.
discard	Disables learning on the port but the port remains administratively enabled.
shutdown	Administratively disables the port; 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 6400, 6850E, 6855, 9000E

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 a port is shutdown or goes into discard mode, disable and enable LPS on that port and then use the **port-security release** command to restore the port to normal operation.
- When a port goes into restrict mode, use the **port-security release** command to restore the port to normal operation.

Examples

```
-> port-security 2/14 violation restrict
-> port-security 1/2-10 violation discard
-> port-security 4/10-15 violation shutdown
```

Release History

Release 6.1; command was introduced.
Release 6.4.4; **discard** parameter added.

Related Commands

port-security	Enables or disables Learned Port Security (LPS) on the switch port(s).
port-security release	Releases a port that was shut down due to an LPS violation
port-security maximum	Specifies the maximum number of source MAC addresses that an LPS port(s) is allowed to learn.
port-security mac	Configures a single authorized source MAC address for a port that belongs to a specified VLAN.
port-security mac-range	Configures a list of authorized MAC addresses by defining a range of addresses allowed on the port.
port-security shutdown	Configures the amount of time in minutes to allow source learning on all LPS ports. Also, enables or disables the conversion of dynamic MAC addresses to static MAC addresses on 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 or the entire module.

port-security *slot/port***[**-*port2***] release**

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (for example, 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).
-port2	The last port number in a range of ports you want to configure on the same slot (for example, 3/1-4 specifies ports 1-4 on slot 3).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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.
- When **port-security release** 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 6.1; command was introduced.

Related Commands

port-security	Enables or disables Learned Port Security (LPS) on the switch port(s).
port-security mac	Configures a single authorized source MAC address for a port that belongs to a specified VLAN.
port-security mac-range	Configures a list of authorized MAC addresses by defining a range of addresses allowed on the port.
port-security shutdown	Configures the amount of time in minutes to allow source learning on all LPS ports. Also, enables or disables the conversion of dynamic MAC addresses to static MAC addresses on LPS ports.
port-security maximum	Specifies the maximum number of source MAC addresses that an LPS port(s) is allowed to learn.

MIB Objects

```
learnedPortSecurityTable
   lpsRelease
```

port-security learn-trap-threshold

Configures the number of bridged MAC addresses to learn before sending a trap.

port-security *slot/port***[**-*port2***]** **learn-trap-threshold** *num*

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
-port2	The last port number in a range of ports you want to configure on the same slot (for example, 3/1-4 specifies ports 1-4 on slot 3).
num	The number of bridged MAC addresses to learn before sending a trap. Valid range is 0 to maximum number of MAC addresses configured on LPS port.

Defaults

By default, the number of bridged MAC addresses learned is set to 5.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- When the number of bridged MAC addresses learned on the port matches the specified threshold amount, a trap is sent for every bridged MAC address learned thereafter.
- Sending a trap when this threshold is reached provides notification of newly learned bridged MAC addresses. Trap contents includes identifying information about the MAC, such as the address itself, the corresponding IP address, switch identification, and the slot and port number on which the MAC was learned.

Examples

```
-> port-security 1/10 learn-trap-threshold 6
-> port-security 1/10-13 learn-trap-threshold 18
```

Release History

Release 6.3.1; command was introduced.

Related Commands

show port-security	Displays Learned Port Security (LPS) configuration and table entries.

MIB Objects

```
learnedPortSecurityTable
   lpsLearnTrapThreshold
```

show port-security

Displays Learned Port Security (LPS) configuration and table entries.

show port-security [*slot/port1-port2* | *slot/port***]**

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
-port2	The last port number in a range of ports you want to configure on the same slot (for example, 3/1-4 specifies ports 1-4 on slot 3).
slot	Enter the slot number for a module to specify that the command should include all ports on that module (for example, 6 specifies all ports on the module found in slot 6 of the switch chassis).

Defaults

By default, all ports with an LPS configuration are displayed.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Displays ports that have an LPS configuration, even if LPS is disabled on the port.
- Use the *slot/port1-port2* parameter with this command to display the LPS configuration for a specific port or a range of ports.
- Use the *slot* parameter with this command to display the LPS configuration for all the ports on a specific slot.
- 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
Legend: Mac Address: * = Duplicate Static
        Mac Address: # = Pseudo Static

Port:  7/10
 Operation Mode   :                ENABLED,
 Max MAC bridged  :                      1,
 Trap Threshold   :               DISABLED,
 Max MAC filtered :                      5,
 Low MAC Range    :      00:00:00:00:00:00,
 High MAC Range   :      ff:ff:ff:ff:ff:ff,
 Violation        :              RESTRICT
 Violating MAC    :                  NULL

 MAC Address          VLAN   TYPE
 -------------------+------+-------------------
 00:20:95:00:fa:5c      1    STATIC
```

output definitions

Port	The module slot number and the physical port number on that module.
Operation Mode	The Learned Port Security operation status for the port (**enabled** or **disabled**). Configured through the **port-security** command.
Max MAC bridged	The maximum number of bridged MAC addresses that are allowed on this port. Configured through the **port-security maximum** command.
Trap Threshold	The number of bridged MACs to learn before sending a trap. After this number is reached, a trap is sent out for every MAC learned thereafter. If **disabled** is displayed in this field, the trap threshold is not in force. Configured through the **port-security learn-trap-threshold** command.
Max MAC filtered	The maximum number of filtered MAC addresses that the LPS port can learn. Configured through the **port-security max-filtering** command.
Low MAC Range	MAC address that defines the lower end of a MAC address range. Configured through the **port-security mac-range** command.
High MAC Range	MAC address that defines the higher end of a MAC address range. Configured through the **port-security mac-range** command.
Violation	The security violation mode for the port (**restrict** or **shutdown**). Configured through the **port-security violation** command.
Violating MAC	The MAC Address which caused the violation on this Port.
MAC Address	An individual authorized MAC address. Configured through the **port-security mac** command.
VLAN	The VLAN to which the LPS port belongs.
TYPE	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.

Release History

Release 6.1; command was introduced.
Release 6.1.5; **config-mac-range** parameter was removed.
Release 6.1.5; **Mac Filtered MAC allowed** field was added.
Release 6.3.1; **Trap Threshold** field was added.
Release 6.4.4; **Legend** and **Violating MAC** field added.

Related Commands

show port-security shutdown	Displays the amount of time during which source learning can occur on all LPS ports.

MIB Objects

```
learnedPortSecurityTable
   lpsMaxMacNum
   lpsMaxFilteredMacNum
   lpsLoMacRange
   lpsHiMacRange
   lpsViolationOption
   lpsOperStatus
   lpsRelease
```

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 6400, 6850E, 6855, 9000E

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 0, then a source learning time limit is not active on LPS ports.
- 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 learning window has not expired.

Examples

```
-> show port-security shutdown
LPS Shutdown Config       =  25 min,
Convert-to-static         =  DISABLE,
No Aging                  =  ENABLE,
Boot Up                   =  ENABLE,
Learn As Static           =  DISABLE,
Mac Move                  =  DISABLE,
Remaining Learning Window =  882 sec,
```

output definitions

LPS Shutdown Config	The configured amount of time during which the LPS port can learn new MAC addresses.
Convert-to-static	Indicates whether or not dynamic MACs are converted to static MACs (**enabled** or **disabled**).
No Aging	Indicates whether or not learned MAC addresses can age out or get flushed during the LPS learning window time period (**disabled** or **enabled**).
Boot Up	Indicates whether or not the learning window automatically starts when the switch boots up (**enabled** or **disabled**).
Learn As Static	Indicates whether or not the MAC address is directly learnt as static MAC address during the learning window.

output definitions

Mac Move	Indicates whether or not the movement of pseudo static MAC address is allowed.
Remaining Learning Window	The remaining amount of time during which the LPS port can learn MAC addresses.

Release History

Release 6.1; command was introduced.
Release 6.1.5; **Convert-to-static** and **Remaining Learning Window** fields added.
Release 6.4.4; **No Aging** and **Boot Up** fields added.
Release 6.4.5; **Learn As Static** and **Mac Move** fields added.

Related Commands

port-security learn-trap-threshold	Displays Learned Port Security (LPS) configuration and table entries.

MIB Objects

```
learnedPortSecurityGlobalGroup
   lpsConvertToStatic
   lpsLearningWindowTime
   lpsLearningWindowTimeWithStaticConversion
```

show port-security brief

Displays the per port LPS parameters configured for all the ports.

show port-security brief

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Displays the configured LPS parameters. The parameters are displayed even if the LPS is disabled on the port.

Examples

```
-> show port-security brief
Legend: enable * = Learning Window has expired

Slot/                                Nb Macs    Nb Macs    Nb Macs
Port  Status      Max    Max-Filter Bridged    Filtered   Static
----+-----------+-------+----------+----------+----------+---------
1/1  ENABLED      5       100        5          10         0
1/2  ENABLED      5       100        0          10         5
1/3  RESTRICTED   5       100        5          100        0
1/4  SHUTDOWN     5       100        -          -          -
1/5  DISABLED     5       100        -          -          -
1/6  LOCKED       5       100        -          -          3
```

output definitions

Slot/Port	The slot number for the module and the physical port number on that module (e.g., 1/2 specifies port 2 on slot 1)
Status	Displays the status of the LPS port.
Max	The maximum number of bridged MAC addresses that are allowed on this port. Configured through the **port-security maximum** command.
Max-Filter	The maximum number of filtered MAC addresses that the LPS port can learn. Configured through the **port-security max-filtering** command.
Nb Macs Bridged	Number of bridge MAC address learnt on corresponding port(s).
Nb Macs Filtered	Number of filtered MAC address learnt on corresponding port(s).
Nb Macs Static	Number of static MAC address configured on corresponding port(s).

Release History

Release 6.4.4; command was introduced.

Related Commands

port-security maximum	Configures the maximum number of source MAC addresses that an LPS port(s) is allowed to learn.
port-security max-filtering	Configures the maximum number of MAC addresses that can be filtered on the LPS port(s).

MIB Objects

```
learnedPortSecurityTable
   lpsMaxMacNum
   lpsMaxFilteredMacNum
   lpsMaxStaticMacNum
   lpsOperStatus
   lpsAdminStatus
```

47 Port Mirroring and Monitoring Commands

The Port Mirroring and Port Monitoring features are primarily used 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. Also, enables or diables remote port mirroring.

port mirroring *port_mirror_sessionid* **[no] source** *slot/port***[-***port2***] [***slot/port***[-***port2***]...] destination** *slot/port* **[rpmir-vlan** *vlan_id***] [bidirectional |inport |outport] [unblocked** *vlan_id***] [enable | disable]**

Syntax Definitions

port_mirror_sessionid	Mirroring session identifier.
source	Adds the alphabet “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.
rpmir-vlan *vlan_id*	Reserved VLAN (1–4094) to carry the mirroring traffic.
bidirectional	Specifies bidirectional port mirroring.
inport	Specifies incoming unidirectional port mirroring.
outport	Specifies outgoing unidirectional port mirroring.
vlan_id	VLAN ID is the 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	enable

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The maximum number of mirroring sessions is limited to two on OmniSwitch 6855 Series switches.

- You cannot configure port mirroring and monitoring on the same switching ASIC on OmniSwitch 6855 Series switches. Each switching ASIC controls 24 ports (for example, ports 1–24, 25–48, and so on.). For example, if a port mirroring session is configured for ports 1/12 and 1/22, then configuring a port monitoring session for any of the ports between 1 and 24 is not allowed.
- If a port mirroring session is configured across two switching ASICs, then configuring a monitoring session is not allowed on any of the ports controlled by each of the ASICs involved. For example, if a port mirroring session is configured for ports 1/8 and 1/30 on a 48-port switch, then configuring a port monitoring session involving any of the ports between 1 and 48 is not allowed.
- Port mirroring is not supported on logical link aggregate ports however, it is supported on individual ports that are members of a link aggregate.
- An “N-to-1” port mirroring session is configurable, where “N” can be a number from 1 to 24 (OS6855) or 1 to 128 (OS6850E). In other words, you can configure up to 24 or 128 source ports for a single destination port in a session.
- 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.
- 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.

Usage Guidelines - Remote Port Mirroring

- Remote Port mirroring is supported only on OS6850E switches.
- Use the **rpmir-vlan** parameter with this command to configure remote port mirroring.
- There must not be any physical loop present in the remote port mirroring VLAN.
- Spanning Tree must be disabled for the remote port mirroring VLAN.
- Source learning must be disabled or overridden on the ports belonging to the remote port mirroring VLAN on intermediate and destination switches.
- On OS6850E switch the QoS redirect feature can be used to override source learning.

Examples

```
-> port mirroring 6 destination 6/4
-> port mirroring 6 source 2/3
-> port mirroring 6 destination 6/4
-> port mirroring 6 source 2/3-5 2/7 2/10
-> port mirroring 8 destination 1/12 rpmir-vlan 7
-> port mirroring 8 source 1/7 bidirectional
-> port mirroring 7 destination 6/4 unblocked 750
-> port mirroring 7 source 2/3
-> port mirroring 9 destination 1/24
-> port mirroring 9 source 1/23 inport
-> port mirroring 9 disable
-> port mirroring 8 no source 1/7
-> port mirroring 6 no source 2/10-12 2/14
```

Release History

Release 6.1; command was introduced.
Release 6.3.1; **rpmir-vlan** parameter added.

Related Commands

port mirroring	Enables, disables, or deletes a port mirroring session.
show port mirroring status	Displays the status of mirrored ports. This value may be enabled or disabled.

MIB Objects

```
mirrorTable
   mirrorMirroringIfindex
   mirrorDirection
   mirrorStatus
   mirrorUnblockedVLAN
   mirrorTaggedVLAN
```

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	**disable**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete a port mirroring session.
- 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.

Examples

```
-> port mirroring 6 enable
-> port mirroring 6 disable
-> no port mirroring 6
```

Release History

Release 6.1; 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 the 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 (for example, 3/1 specifies port 1 on slot 3).
filename	Specifies a file name for the monitoring session (for example, **/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 after which the session is 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 6400, 6850E, 6855

Usage Guidelines

- The maximum number of monitoring sessions is limited to one per chassis and/or stack.
- You cannot configure port mirroring and monitoring on the same switching ASIC on OmniSwitch 6855 Series switches. Each switching ASIC controls 24 ports (for example, ports 1–24, 25–48, and so on.). For example, if a port mirroring session is configured for ports 1/12 and 1/22, then configuring a port monitoring session for any of the ports between 1 and 24 is not allowed.
- If a port mirroring session is configured across two switching ASICs, then configuring a monitoring session is not allowed on any of the ports controlled by each of the ASICs involved. For example, if a port mirroring session is configured for ports 1/8 and 1/30 on a 48-port switch, then configuring a port monitoring session involving any of the ports between 1 and 48 is not allowed.
- 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.
- 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 6.1; command was introduced.

Related Commands

port monitoring	Disables, pauses, resumes, or deletes a port monitoring session.
show port monitoring status	Displays the port monitoring status.
show port monitoring file	Displays the port monitoring data.

MIB Objects

```
monitorTable
   monitorSessionNumber
   monitorIfindex
   monitorFileStatus
   monitorFileName
   monitorFileSize
   monitorScreenStatus
   monitorScreenLine
   monitorTrafficType
   monitorStatus
   monitorFileOverWrite
   monitorDirection
   monitorTimeout
```

port monitoring

Disables, pauses, resume, 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 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the **no** form of this 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 6.1; command was introduced.

Related Commands

port monitoring	Configures a port monitoring session.
show port monitoring status	Displays the port monitoring status.

MIB Objects

```
monitorTable
   monitorSessionNumber
   monitorScreenStatus
```

show port mirroring status

Displays the 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 6400, 6850E, 6855, 9000E

Usage Guidelines

If a port mirroring session identifier is not specified with this command, then all port mirroring sessions are displayed.

Examples

```
-> show port mirroring status

 Session    Mirror        Mirror     Unblocked    Config     Oper
          Destination    Direction     Vlan       Status    Status
----------+----------+--------------+----------+----------+---------
   6.        1/41            -         NONE       Enable    Off
----------+----------+--------------+----------+----------+---------
           Mirror
           Source
----------+----------+--------------+----------+----------+---------
   6.        1/20      bidirectional     -        Enable    Off
   6.        1/21      bidirectional     -        Enable    Off
   6.        1/22      bidirectional     -        Enable    Off
   6.        1/23      bidirectional     -        Enable    Off
   6.        1/24      bidirectional     -        Enable    Off
   6.        1/25      bidirectional     -        Enable    Off
   6.        1/26      bidirectional     -        Enable    Off
   6.        1/27      bidirectional     -        Enable    Off
   6.        1/28      bidirectional     -        Enable    Off
   6.        1/29      bidirectional     -        Enable    Off
   6.        1/30      bidirectional     -        Enable    Off
```

output definitions

Session	The port mirroring session identifier.
Mirror Destination	The location of the mirrored port.
Mirror Direction	The direction of the mirroring or mirrored port, which can be **bidirectional** (the default), **inport**, or **outport**.
Unblocked VLAN	The mirroring VLAN ID number.

output definitions (continued)

Config Status	The configuration status of the session.
Oper Status	The current status of the mirroring or mirrored port.
Mirror Source	The location of the mirroring port.

```
-> show port mirroring status

 Session    Mirror        Mirror     Unblocked    Config     Oper
          Destination    Direction     Vlan       Status    Status
----------+----------+--------------+----------+----------+---------
   6.        1/41            -         NONE       Enable    Off
----------+----------+--------------+----------+----------+---------
           Mirror
           Source
----------+----------+--------------+----------+----------+---------
   6.        1/20      bidirectional     -        Enable    Off
   6.        1/21      bidirectional     -        Enable    Off
   6.        1/22      bidirectional     -        Enable    Off
   6.        1/23      bidirectional     -        Enable    Off
   6.        1/24      bidirectional     -        Enable    Off
   6.        1/25      bidirectional     -        Enable    Off
   6.        1/26      bidirectional     -        Enable    Off
   6.        1/27      bidirectional     -        Enable    Off
   6.        1/28      bidirectional     -        Enable    Off
   6.        1/29      bidirectional     -        Enable    Off
   6.        1/30      bidirectional     -        Enable    Off
```

output definitions

Session	The port mirroring session identifier.
Mirror Destination	The location of the mirrored port.
Mirror Direction	The direction of the mirroring or mirrored port, which can be **bidirectional** (the default), **inport**, or **outport**.
Unblocked VLAN	The mirroring VLAN ID number.
Config Status	The configuration status of the session.
Oper Status	The current status of the mirroring or mirrored port.
Mirror Source	The location of the mirroring port.

Release History

Release 6.1; 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 a port that will 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 6400, 6850E, 6855, 9000E

Usage Guidelines

If a port monitoring session identifier is not specified with this command, then all port monitoring sessions are 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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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 the port monitoring status.

MIB Objects

```
monitorTable
   monitorSessionNumber
   monitorIfindex
   monitorTrafficType
```

48 sFlow Commands

sFlow is a network monitoring technology that gives visibility in to the activity of the network, by providing network usage information. It provides the data required to effectively control and manage the network usage. sFlow is a sampling technology that meets the requirements for a network traffic monitoring solution.

sFlow provides a network-wide view of usage and active routes. It is used for measuring network traffic, collecting, storing, and analyzing the traffic data. As it is scalable, that doesn't add significant network load. sFlow is an industry standard with many vendors delivering products with this support. Some of the applications of the sFlow data include:

- Detecting, diagnosing, and fixing network problems
- Real-time congestion management
- Detecting unauthorized network activity
- Usage accounting and billing
- Understanding application mix
- Route profiling and peer optimization
- Capacity planning

sFlow is a sampling technology embedded within switches/routers. It provides the ability to monitor the traffic flows. It requires an sFlow agent software process running as part of the switch software and a sFlow collector which receives and analyses the monitored data. The sFlow collector makes use of SNMP to communicate with an sFlow agent in order to configure sFlow monitoring on the device (switch).

An sFlow agent running on the switch/router combines interface counters and traffic flow (packet) samples, preferably, on all the interfaces into sFlow datagrams that are sent across the network to an sFlow collector.

Packet sampling on the switch/router is typically performed by the switching/routing ASICs, providing wire-speed performance. In this case, an sFlow agent does very little processing, by packaging data into sFlow datagrams that are immediately sent on network. This minimizes the memory and CPU utilization by the sFlow agent.

MIB information for the sFlow commands is as follows:

Filename: AlcatelIND1PortMirMon.MIB
Module: Alcatel-IND1-PORT-MIRRORING-MONITORING-MIB

Filename: SFLOW_RFC3176.MIB
Module: SFLOW-MIB

A summary of the available commands is listed here:

sflow agent
sflow receiver
sflow sampler
sflow poller
show sflow agent
show sflow receiver
show sflow sampler
show sflow poller

sflow agent

Configures a specific sflow agent IP address.

sflow agent ip <*ip_address*>

no sflow agent ip <*ip_address*>

Syntax Definitions

ip_address	The sflow agent IP address.

Defaults

parameter	default
ip-address	0.0.0.0

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete the IP address.
- If no IP address is configured 0.0.0.0 is used.
- If no IP address is configured but the Loopback0 address is configured, the Loopback0 address is used.

Examples

```
-> sflow agent ip 192.168.1.1
-> no sflow agent ip 192.168.1.1
```

Release History

Release 6.3.4; command was introduced
Release 6.4.3; command was deprecated, use **ip managed-interface**.

sflow receiver

Sets the destination hosts where the sFlow datagrams are sent out. If there are multiple destinations, then each destination is associated with the receiver instance. All these destinations are attached to the sFlow manager instance and to an associated sampler/poller.

sflow receiver *num* **name** *string* **timeout {***seconds* | **forever} address {***ip_address* | *ipv6address***} udp-port** *port* **packet-size** *size* **Version** *num*

sflow receiver *receiver_index* **release**

Syntax Definitions

num	Specifies the receiver index.
string	Specifies the name.
seconds | **forever**	Specifies the timeout value.
ip_address| *ipv6address*	Specifies the 32/128-bit ip address.
port	Specifies the UDP (destination) port.
size	Specifies the maximum number of data bytes (size) that can be sent.
num	Specifies the version number.

Defaults

parameter	default
string	empty
seconds	0
ip_address	0.0.0.0(ipv4)
port	6343
size	1400
version num	5

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the **release** form at the end of the command to delete a receiver.

Examples

```
-> sflow receiver 1 name Golden address 198.206.181.3
-> sflow receiver 1 release
```

Release History

Release 6.1.1; command was introduced.

Related Commands

show sflow receiver	Displays the receiver table.

MIB Objects

```
sFlowRcvrTable
   sFlowRcvrIndex
   sFlowRcvrOwner
   sFlowRcvrTimeout
   sFlowRcvrMaximumDatagramSize
   sFlowRcvrAddressType
   sFlowRcvrAddress
   sFlowRcvrPort
   sFlowRcvrDatagramVersion
```

sflow sampler

Gets the hardware sampled from Q-dispatcher and fills up the sampler part of the UDP datagram.

sflow sampler *num portlist* **receiver** *receiver_index* **rate** *value* **sample-hdr-size** *size*

no sflow sampler *num portlist*

Syntax Definitions

num	Specifies the instance id.
portlist	Specifies the interface index range.
receiver_index	Specifies the receiver index.
value	Specifies the rate value for packet sampling.
size	Specifies the maximum number of bytes (size) that can be copied from a sampled packet.

Defaults

parameter	default
receiver_index	0
value	0
size	128

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete a sampler.
- A sampling rate of 1 counts all packets. A sampling rate of 0 disables sampling.

Examples

```
-> sflow sampler 1 2/1-5 receiver 1 rate 1024
-> no sflow sampler 1 2/1-5
```

Release History

Release 6.1.1; command was introduced.

Related Commands

show sflow sampler	Displays the sampler table.

MIB Objects

```
sFlowFsTable
   sFlowFsDataSource
   sFlowFsInstance
   sFlowFsReceiver
   sFlowFsPacketSamplingRate
   sFlowFsMaximumHeaderSize
```

sflow poller

Gets counter samples from ethernet driver and fills up the counter part of the UDP datagram.

sflow poller *num portlist* **receiver** *receiver_index* **interval** *value*

no sflow poller *num portlist*

Syntax Definitions

num	Specifies the instance id.
portlist	Specifies the interface index range.
receiver_index	Specifies the receiver index.
value	Specifies the maximum number of seconds between successive samples (interval value).

Defaults

parameter	default
receiver_index	0
value	0

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the **no** form of this command to delete a poller.

Examples

```
-> sflow poller 1 2/6-10 receiver 1 interval 30
-> no sflow poller 1 2/6-10
```

Release History

Release 6.1.1; command was introduced.

Related Commands

show sflow poller	Displays the poller table.

MIB Objects

```
sFlowCpTable
   sFlowCpDataSource
   sFlowCpInstance
   sFlowCpReceiver
   sFlowCpInterval
```

show sflow agent

Displays the sflow agent table.

show sflow agent

Syntax Definitions

agent	Collects sample datagrams and send it to the collector across the network.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- It is necessary to execute the **ip interface** command to make a Loopback0 IP address as the fixed primary address of the switch, in order to avoid interface changes, which might need the collector software to be restarted for it to communicate using the new agent IP address. Normally, the primary IP address could change depending on the IP interface going up/down. Therefore, the sFlow agent always needs to send a fixed IP address in the datagram.
- The loopback address should be an IP interface configured on the switch.

Examples

```
-> ip interface Loopback0 address 198.206.181.100
-> show sflow agent
Agent Version  = 1.3; Alcatel-Lucent; 6.1.1
Agent IP       = 198.206.181.100
```

output definitions

Agent Version	Identifies the version which includes the MIB version, organization name, and the specific software build of the agent.
Agent address	IP address associated with the agent.

Release History

Release 6.1.1; command was introduced.

Related Commands

show sflow receiver	Displays the receiver table.

MIB Objects

```
sFlowAgent
   sFlowVersion
   sFlowAgentAddressType
   sFlowAgentAddress
```

show sflow receiver

Displays the sflow receiver table.

show sflow receiver [*num***]**

Syntax Definitions

num	Specifies the receiver index.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show sflow receiver
Receiver 1
Name       = Golden
Address    = IP_V4  198.206.181.3
UDP Port   = 6343
Timeout    = 65535
Packet Size= 1400
DatagramVer= 5
```

output definitions

Name	Name of the entry to claim.
Address	IP address of the sFlow collector.
UDP Port	Destination port for sFlow datagrams.
Timeout	Time remaining before the sampler is released and stops sampling.
Packet size	Maximum number of data bytes that can be sent in a single sample datagram.
Datagram ver	Version of sFlow datagrams that should be sent.

Release History

Release 6.1.1; command was introduced.

Related Commands

sflow agent	Sets the destination hosts where the sFlow datagrams are sent out.

MIB Objects

```
sFlowRcvrTable
   sFlowRcvrIndex
```

show sflow sampler

Displays the sflow sampler table.

show sflow sampler[*num***]**

Syntax Definitions

num	Specifies the instance id.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A.

Examples

```
-> show sflow sampler
Instance   Interface    Receiver  Sample-rate   Sample-hdr-size
-----------------------------------------------------------------
   1         2/ 1          1         2048             128
   1         2/ 2          1         2048             128
   1         2/ 3          1         2048             128
   1         2/ 4          1         2048             128
   1         2/ 5          1         2048             128
```

output definitions

Instance	Instance for the flow sampler.
Interface	Interface used for the flow sampler.
Receiver	Receiver associated with the flow sampler.
Sample-rate	Statistical sampling rate for packet sampling from the source.
Sample-hdr-size	Maximum number of bytes that should be copied from a sampled packet.

Release History

Release 6.1.1; command was introduced.

Related Commands

sflow sampler	Gets hardware sampled from Q-dispatcher.

MIB Objects

```
sFlowFsTable
   sFlowFsInstance
```

show sflow poller

Displays the sflow poller table.

show sflow poller [*num***]**

Syntax Definitions

num	Specifies the instance id.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show sflow poller
Instance   Interface    Receiver  Interval
-----------------------------------------
     1        2/ 6         1         30
     1        2/ 7         1         30
     1        2/ 8         1         30
     1        2/ 9         1         30
     1        2/10         1         30
```

output definitions

Instance	Instance for the counter poller.
Interface	Interface used for the counter poller.
Receiver	Receiver associated with the counter poller.
Interval	The maximum number of seconds between successive samples of the counters associated with the data source.

Release History

Release 6.1.1; command was introduced.

Related Commands

sflow poller	Gets counter samples.

MIB Objects

```
sFlowCpTable
   sFlowCpInstance
```

49 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 6400, 6850E, 6855, 9000E

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 6.1; 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 a 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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
```

50 VLAN Stacking Commands

The VLAN Stacking feature provides a method for tunneling multiple customer VLANs (CVLAN) through a service provider network using one or more service provider VLANs by way of 802.1Q double tagging or VLAN Translation. This feature enables service providers to provide their customers with Transparent LAN Services (TLS). This service is multipoint in nature so as to support multiple customer sites or networks distributed over the edges of a service provider network.

MIB information for the VLAN Stacking commands is as follows:

Filename: AlcatelIND1VlanStacking.MIB
Module: Alcatel-IND1-VLAN-STACKING-MIB

Filename: AlcatelIND1VlanManager.MIB
Module: Alcatel-IND1-VLAN-MGR-MIB

A summary of the available commands is listed here:

VLAN Stacking Service Mode	**ethernet-service** **ethernet-service custom-L2-protocol** **ethernet-service source-learning** **ethernet-service service-name** **ethernet-service svlan nni** **ethernet-service nni** **ethernet-service sap** **ethernet-service sap uni** **ethernet-service sap cvlan** **ethernet-service sap-profile** **ethernet-service sap sap-profile** **ethernet-service uni-profile** **ethernet-service uni uni-profile** **ethernet-service uni-profile custom-L2-protocol** **show ethernet-service custom-L2-protocol** **show ethernet-service mode** **show ethernet-service vlan** **show ethernet-service** **show ethernet-service sap** **show ethernet-service port** **show ethernet-service nni** **show ethernet-service nni l2pt-statistics** **clear ethernet-service nni l2pt-statistics** **show ethernet-service uni** **show ethernet-service uni l2pt-statistics** **clear ethernet-service uni l2pt-statistics** **show ethernet-service uni-profile** **show ethernet-service sap-profile**
Ethernet Service Hardware Loopback Test	**loopback-test** **show loopback-test**

ethernet-service

Creates a VLAN Stacking VLAN (SVLAN) for tunneling customer traffic, a management SVLAN for provider traffic, or an SVLAN that the IP Multicast VLAN (IPMV) application will use to distribute multicast traffic.

ethernet-service {svlan | ipmvlan | management-vlan} *svid1***[**-*svid2***] [enable | disable] [[1x1 | flat] stp {enable | disable}] [name** *description***]**

no ethernet-service {svlan | ipmvlan | management-vlan} *svid1***[**-*svid2***]**

Syntax Definitions

svlan	Creates an SVLAN for tunneling customer traffic.
ipmvlan	Creates an SVLAN used by IPMV to distribute multicast traffic.
management-vlan	Creates a management SVLAN for provider traffic.
svid1	The VLAN ID number identifying the SVLAN (2–4094).
-svid2	The last VLAN ID number in a range of SVLANs that you want to configure (e.g. 10-12 specifies VLANs 10, 11, and 12).
enable	Enables the SVLAN administrative status.
disable	Disables the SVLAN administrative status, which blocks all ports bound to that SVLAN.
1x1	Specifies that the Spanning Tree status for the SVLAN applies when the switch is running in the 1x1 Spanning Tree mode.
flat	Specifies that the Spanning Tree status for the SVLAN applies when the switch is running in the flat Spanning Tree mode.
stp enable	Enables the SVLAN Spanning Tree status for the service provider network topology.
stp disable	Disables the SVLAN Spanning Tree status for the service provider network topology.
description	An alphanumeric string of up to 32 characters. Use quotes around the string if the VLAN name contains multiple words with spaces between them (e.g., “Alcatel-Lucent Engineering”).

Defaults

By default, the Spanning Tree status is enabled in both the 1x1 and flat mode when the SVLAN or IPMV is created

parameter	default
enable | disable	**enable**
stp enable | disable	**enable**
description	VLAN ID number

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to delete an SVLAN or a range of SVLANs. Note that SVLAN port associations are also removed when the SVLAN is deleted.
- This command does not work if the *svid* specified already exists as a standard 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 SVLAN 10, then the Spanning Tree status for SVLAN 10 is disabled when the switch is running in the flat mode. However, the current Spanning Tree status for SVLAN 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 SVLAN is changed for both operating modes.
- Note that the Spanning Tree status for an SVLAN only applies to the Spanning Tree topology calculations for the service provider network. This status is not applied to customer VLANs (CVLANs) and does not affect the customer network topology.

Examples

```
-> ethernet-service svlan 1001 name “Customer ABC”
-> ethernet-service ipmvvlan 255
-> ethernet-service management-vlan 355
-> no ethernet-service svlan 1001
-> no ethernet-service ipmvlan 255
-> no ethernet-service management-vlan 355
```

Release History

Release 6.3.1; command was introduced.

Related Commands

show ethernet-service vlan	Displays a list of SVLANs configured fro the switch
ethernet-service custom-L2-protocol	Configures the source learning status for an SVLAN.

MIB Objects

```
vlanTable
   vlanNumber
   vlanDescription
   vlanSvlanTrafficType
   vlanAdmStatus
   vlan1x1StpStatus
   vlanFlatStpStatus
   vlanStpStatus
   vlanStatus
```

ethernet-service custom-L2-protocol

Creates a custom-L2-protocol entry MAC address and optional mask or ether-type with optional subtype.

ethernet-service custom-L2-protocol *name* **mac** *mac-address* **[mask** *mask* **| ethertype** *ether-type* **subtype** *sub-type* **| ssap/dsap** *ssap/dsap* **pid** *pid***]**

no ethernet-service custom-L2-protocol *name*

Syntax Definitions

name	An alphanumeric string of maximum length 32 to identify the custom-L2-protocol entry.
mac-address	MAC address associated to custom-L2-protocol entry in hexadecimal format.
mask	Mask of the MAC address to specify the range of MAC address in the custom-L2-protocol entry in hexadecimal format.
ether-type	An integer ether-type value to specify generic ether-type.
sub-type	An integer sub-type value to specify ether sub-type.
ssap/dsap	Source service access point and destination service access point specific to LLC/SNAP in numerical or hexadecimal format.
pid	Protocol identifier.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to delete the configured custom-L2-protocol entry.
- You cannot delete a custom-L2-protocol entry when the entry is associated to UNI profile on a UNI port.
- You cannot configure ether-type and ether-sub-type when MAC address mask is specified.
- If ether-type is not specified, then ether-sub-type configuration is not allowed.
- The MAC address must be a multicast MAC address. For example, 01:80:c2:00:00:00.
- The mask can be specified to configure a range of MAC address. For example, a mask of ff:ff:ff:ff:ff:00 configures the range of MAC addresses in that range.

- If custom-L2-protocol is configured only with the MAC address and no mask, then:
    - The MAC address cannot be a reserved IPV4/IPV6 multicast MAC address.
    - The MAC address cannot be a MAC-specific control protocol address such as 01-80-C2-00-00-01 or 01-80-C2-00-00-04.
    - The MAC address cannot be a service OAM address such as from 01-80-C2-00-00-30 to 01-80-C2-00-00-3F.
    - The MAC address configured for another custom L2-protocol cannot be used.
- If custom L2-protocol is configured only with a MAC address and a mask, then:
    - The MAC address range cannot overlap with the reserved IPV4 or IPV6 multicast MAC address ranges.
    - The MAC address range must not overlap with the MAC address range configured for another custom L2-protocol. Only nested MAC address ranges are allowed.
- If custom-L2-protocol is configured with an ether-type, and optionally with a sub-type, then:
    - The ether-type/sub-type cannot be configured for another custom-L2-protocol.
    - The ether-type/sub-type cannot be a well known L2 protocol (0x8809/1,0x8809/2, 0x8809/3, 0x888E, 0x88CC, 0x88F5).
- The MAC address, mask, ether-type, sub-type, SSAP/DSAP, and PID cannot be modified once the custom L2-protocol is created. The custom L2-protocol must be deleted and recreated with the new values required.

Examples

```
-> ethernet-service custom-L2-protocol All_IEEE mac 01:80:c2:00:00:00 mask
ff:ff:ff:ff:ff:00

-> ethernet-service custom-L2-protocol ELMI mac 01:80:c2:00:00:07
ethertype 0x88EE

-> ethernet-service custom-L2-protocol p1 mac 01:80:c2:00:11:11

-> ethernet-service custom-L2-protocol p1 mac 01:80:c2:00:11:11 mask
ff:ff:ff:ff:ff:00

-> ethernet-service custom-L2-protocol p1 mac 01:80:c2:00:11:11 ethertype 35555

-> ethernet-service custom-L2-protocol p1 mac 01:80:c2:00:11:11 ethertype 35556
subtype 120

-> ethernet-service custom-L2-protocol p1 mac 01:80:c2:00:11:11 ssap/dsap 43/43
pid 3

-> no ethernet-service custom-L2-protocol p1
```

Release History

Release 6.4.5; command introduced.

Related Commands

show ethernet-service sap	Displays configuration information of the specific custom-L2-protocol entry, if specified, or displays information of all the configured custom-L2-protocol entries in the system.

MIB Objects

```
alaEServiceL2CustomProtocolTable
   AlaEServiceL2CustomProtocolEntry
   alaEServiceL2CustomProtocolID
   alaEServiceL2CustomProtocolMask
   alaEServiceL2CustomProtocolEtherType
   alaEServiceL2CustomProtocolEtherSubType
   alaEServiceL2CustomProtocolSsap
   alaEServiceL2CustomProtocolDsap
   alaEServiceL2CustomProtocolPid
   alaEServiceL2CustomProtocolRowStatus
```

ethernet-service source-learning

Configures the status of source learning on a VLAN Stacking VLAN (SVLAN) used for tunneling customer traffic or on an SVLAN that the IP Multicast VLAN (IPMV) application uses to distribute multicast network traffic.

ethernet-service {svlan | ipmvlan} *svid1***[-***svid2***] source-learning {enable| disable}**

Syntax Definitions

svlan	Specifies an SVLAN for tunneling customer traffic.
ipmvlan	Specifies an SVLAN used by IP Multicast VLAN to distribute multicast traffic.
svid1	The VLAN ID number identifying the SVLAN (2–4094).
-*svid2*	The last VLAN ID number in a range of SVLANs that you want to configure (e.g. 10-12 specifies SVLANs 10, 11, and 12).
enable	Enables source MAC address learning.
disable	Disables source MAC address learning.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- By default, source MAC address learning is enabled on all the SVLANs.
- Disabling source learning on an SVLAN clears all the dynamically learned MAC addresses associated with the VLAN from the MAC address table.
- Static MAC addresses associated with an SVLAN are *not* cleared when source learning is disabled for the SVLAN.
- Configuring the source learning status is not supported on Management SVLANs.

Examples

```
-> ethernet-service svlan 120-150 source-learning disable
-> ethernet-service ipmvlan 320-350 source-learning disable
```

Release History

Release 6.4.2; command introduced.

Related Commands

ethernet-service	Creates a VLAN Stacking VLAN (SVLAN).
show ethernet-service vlan	Displays a list of SVLANs configured for the switch.

MIB Objects

```
vlanTable
   vlanEntry
   vlanNumber
   vlanStatus
   vlanMacLearningControlStatus
```

ethernet-service service-name

Creates a VLAN Stacking service and associates the service with an SVLAN or an IP Multicast VLAN (IPMV). The SVLAN or IPMV specified is the VLAN that will transport traffic for the service.

ethernet-service service-name *service-name* **{svlan | ipmvlan}** *svid*

no ethernet-service service-name *service-name* **{svlan | ipmvlan}** *svid*

Syntax Definitions

service-name	The name of the VLAN Stacking service; an alphanumeric string of up to 32 characters. Use quotes around string if the VLAN name contains multiple words with spaces between them (e.g., “Alcatel-Lucent Engineering”).
svid	The VLAN ID number that identifies an existing SVLAN or IPMV to associate with the VLAN Stacking service (2–4094).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a VLAN Stacking service. Note that when a service is removed, the SVLAN or IPMV association with that service is also removed.
- If the VLAN Stacking service is associated with a Service Access Point (SAP) remove the SAP associations before attempting to remove the service.
- Each VLAN Stacking service is associated with one SVLAN or IPMV. Specifying an additional VLAN ID for an existing service is not allowed.

Examples

```
-> ethernet-service service-name Marketing svlan 10
-> ethernet-service service-name Finance ipmvlan 20
-> no ethernet-service service-name Marketing
```

Release History

Release 6.3.1; command was introduced.

Related Commands

ethernet-service	Creates an SVLAN for customer traffic, a management VLAN for provider traffic, or an IPMV for multicast traffic.

MIB Objects

```
alaEServiceTable
   alaEServiceID
   alaEServiceSVLAN
   alaEServiceVlanType
   alaEServiceRowStatus
```

ethernet-service svlan nni

Configures the switch port as a VLAN Stacking Network Network Interface (NNI) port and associates the port with a customer SVLAN or management SVLAN. A network port connects to another provider bridge and carries both customer and provider traffic.

ethernet-service svlan *svid1***[**-*svid2***] nni {**slot/port1***[*-*port2***]** | **linkagg** *agg_num***} [stp | erp]**

no ethernet-service svlan *svid1***[**-*svid2***] nni {**slot/port1***[*-*port2***]** | **linkagg** *agg_num***}**

Syntax Definitions

svid1	The VLAN ID number identifying the SVLAN (2–4094).
-svid2	The last VLAN ID number in a range of SVLANs that you want to specify (e.g. 10-12 specifies VLANs 10, 11, and 12).
slot/port1	The slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
-port2	The last port number in a range of ports that you want to configure on the same slot (e.g, 3/1-4 specifies ports 1, 2, 3, and 4 on slot 3).
agg_num	The link aggregate ID number (0–31).
stp	Specifies Spanning Tree control for the SVLAN-NNI association.
erp	Specifies Ethernet Ring Protection (ERP) control for the SVLAN-NNI association.

Defaults

parameter	default
stp | erp	**stp**

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to remove an association between an NNI port and an SVLAN. Note that when the last SVLAN association is removed, the NNI port reverts to a conventional switch port.
- This SVLAN ID specified with this command must exist in the switch configuration. Only SVLAN IDs are accepted; IPMVLAN IDs are not supported with this command.
- When this command is used, the default VLAN for the NNI port is changed to a VLAN reserved by the switch.for applications such as VLAN Stacking. The reserved VLAN is not configurable using standard VLAN management commands.
- Associating a network port to an SVLAN is required.

Examples

```
-> ethernet-service svlan 10 nni 1/3
-> ethernet-service svlan 255 nni 2/10-15
-> ethernet-service svlan 500 nni linkagg 31
-> no ethernet-service svlan 10 nni 1/3
-> no ethernet-service svlan 255 nni 2/12
```

Release History

Release 6.3.1; command was introduced.
Release 6.3.4; **stp** and **erp** parameters added.

Related Commands

ethernet-service	Creates an SVLAN for customer traffic, a management VLAN for provider traffic, or an IPMV for multicast traffic.
ethernet-service nni	Configures the vendor TPID value, the legacy BPDU processing status, and the transparent bridging status for a VLAN Stacking Network Network Interface (NNI).

MIB Objects

```
alaEServiceNniSvlanTable
   alaEServiceNniSvlanNni
   alaEServiceNniSvlanSvlan
   alaEServiceNniSvlanRowStatus
```

ethernet-service nni

Configures the vendor TPID value, the legacy BPDU processing status, and the transparent bridging status for a VLAN Stacking Network Network Interface (NNI).

ethernet-service nni {*slot/port1***[-***port2***]** | *agg_num***} [tpid** *value***] [{stp | gvrp | mvrp} legacy-bpdu {enable | disable}] [transparent-bridging {enable | disable}]**

Syntax Definitions

slot/port1	The slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
-port2	The last port number in a range of ports that you want to configure on the same slot (e.g, 3/1-4 specifies ports 1, 2, 3, and 4 on slot 3).
agg_num	The link aggregate ID number (0–31).
value	Specifies the TPID value of the port.
stp	Specifies Spanning Tree legacy BPDU support.
gvrp	Specifies GVRP legacy BPDU support.
mvrp	Specifies MVRP legacy BPDU support.
legacy-bpdu enable	Enables the specified legacy BPDU support.
legacy-bpdu disable	Disables the specified legacy BPDU support.
transparent-bridging enable	Enables transparent bridging.
transparent-bridging disable	Disables transparent bridging.

Defaults

parameter	default
value	**0x8100**
stp legacy-bpdu enable | disable	**disable**
gvrp legacy-bpdu enable | disable	**disable**
mvrp legacy-bpdu enable | disable	**disable**
transparent-bridging enable | disable	**disable**

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- This command only applies to ports configured as VLAN Stacking NNI ports.

- Enable legacy BPDU support only on VLAN Stacking network ports that are connected to legacy BPDU switches. Enabling legacy BPDU between AOS switches may cause flooding or an unstable network.
- If legacy BPDU is enabled on a network port while at same time BPDU flooding is enabled on user ports, make sure that tagged customer BPDUs are not interpreted by intermediate switches in the provider network.
- Note that if the peer switch connected to the VLAN Stacking network port supports the Provider MAC address (i.e., STP, 802.1ad/D6.0 MAC), then enabling legacy BPDU support is not required on the network port. Refer to the following table to determine the type of STP, GVRP, or MVRP MAC used:

STP	
Customer MAC address	{0x01, 0x80, 0xc2, 0x00, 0x00, 0x00}
Provider MAC address (802.1ad/D6.0)	{0x01, 0x80, 0xc2, 0x00, 0x00, 0x08}
Provider MAC address (Legacy MAC)	{0x01, 0x80, 0xc2, 0x00, 0x00, 0x00}
GVRP	
Customer MAC address	{0x01, 0x80, 0xc2, 0x00, 0x00, 0x21}
Provider MAC address	{0x01, 0x80, 0xc2, 0x00, 0x00, 0x0D}
MVRP	
Customer MAC address	(0x01, 0x80, 0xc2, 0x00, 0x00, 0x21)
Provider MAC address	(0x01, 0x80, 0xc2, 0x00, 0x00, 0x0D)

- GVRP legacy BPDU are supported only on network ports that already have GVRP enabled for the port.
- STP legacy BPDU and transparent bridging are supported only when the flat Spanning Tree mode is active on the switch.
- When transparent bridging is enabled, the NNI forwards SVLAN traffic without processing packet contents. As a result, the NNI port can also forward traffic for SVLANs that are not configured on the local switch, thus allowing for a greater number of NNI port associations with SVLANs.
- Note that enabling transparent bridging is recommended only on NNI ports that are known to and controlled by the network administrator.
- If the Spanning Tree operating mode for the switch is changed from flat mode to 1x1 mode, transparent bridging is automatically disabled on all NNI ports.

Examples

```
-> ethernet-service nni 2/10-15 tpid 88a8
-> ethernet-service nni 31 stp legacy-bpdu enable
-> ethernet-service nni 10 gvrp legacy-bpdu enable
-> ethernet-service nni 7/1 mvrp legacy-bpdu enable
-> ethernet-service nni 1/10 transparent bridging enable
```

Release History

Release 6.3.1; command was introduced.
Release 6.3.4; **transparent-bridging** parameter added.
Release 6.4.3; **mvrp** parameter added.

Related Commands

ethernet-service svlan nni	Configures the switch port as a VLAN Stacking NNI port and associates the port with a customer SVLAN, management SVLAN, or an IP Multicast VLAN (IPMV).
show ethernet-service nni	Displays configuration information for NNI ports.

MIB Objects

```
alaEServicePortTable
   alaEServicePortID
   alaEServicePortType
   alaEServicePortVendorTpid
   alaEServicePortLegacyStpBpdu
   alaEServicePortLegacyGvrpBpdu
   alaEServicePortLegacyMvrpBpdu
   alaEServicePortRowStatus
```

ethernet-service sap

Creates a VLAN Stacking Service Access Point (SAP) and associates the SAP with a VLAN Stacking service.

ethernet-service sap *sapid* **service-name** *service-name*

no ethernet-service sap *sapid*

Syntax Definitions

sapid	The SAP ID number identifying the service instance (1-1024).
service-name	The name of the service to associate with this SAP.

Defaults

The “default-sap-profile” profile is automatically associated with the SAP ID when the SAP is created.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to delete a VLAN Stacking SAP. When a SAP is deleted, all port and CVLAN associations with the SAP are also deleted.
- The service name specified with this command must exist in the switch configuration. Use the **ethernet-service service-name** command to create a service to associate with the SAP.
- Each SAP ID is associated with only one service. However, it is possible to associate one service with multiple SAP IDs.

Examples

```
-> ethernet-service sap 10 service-name CustomerA
-> no ethernet-service sap 11
```

Release History

Release 6.3.1; command was introduced.

Related Commands

ethernet-service service-name	Creates a VLAN Stacking service and associates the service with an SVLAN or an IP Multicast VLAN (IPMV).
ethernet-service sap-profile	Creates a VLAN Stacking SAP profile.
ethernet-service sap sap-profile	Associates a SAP profile with a SAP ID.

MIB Objects

```
alaEServiceSapTable
   alaEServiceSapID
   alaEServiceSapService
   alaEServiceSapRowStatus
```

ethernet-service sap uni

Configures the switch port as a VLAN Stacking User Network Interface (UNI) and associates the port with a VLAN Stacking Service Access Point (SAP). A UNI port is a customer facing port on which traffic enters the SAP.

ethernet-service sap *sapid* **uni {***slot/port1***[**-*port2***]** | **linkagg** *agg_num***}**

ethernet-service sap *sapid* **no uni {***slot/port1***[**-*port2***]** | **linkagg** *agg_num***}**

Syntax Definitions

sapid	The SAP ID number identifying the service instance (1–1024).
slot/port1	The slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
-port2	The last port number in a range of ports that you want to configure on the same slot (e.g, 3/1-4 specifies ports 1, 2, 3, and 4 on slot 3).
agg_num	The link aggregate ID number (0–31).

Defaults

A switch port or a link aggregate becomes a VLAN Stacking UNI port by default when the port or link aggregate is associated with a VLAN Stacking SAP.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to remove an association between a UNI port and a SAP. Note that when the last SAP association is removed, the UNI port converts back to a conventional switch port.
- The SAP ID specified with this command must exist. Use the **ethernet-service sap** command to create a SAP.
- Note that if the SAP ID specified with this command is associated with an IPMVLAN, the SAP profile must specify CVLAN translation. In addition, multicast traffic is not associated with the IPMVLAN until the UNI port is associated with the IPMVLAN as a receiver port. For more information, see the “IP Multicast VLAN Commands” chapter in this guide.
- When this command is used, the default VLAN for the UNI port is changed to a reserved VLAN and all customer traffic received is dropped until the type of traffic for the port is configured using the **ethernet-service sap cvlan** command.

Examples

```
-> ethernet-service sap 10 uni 1/3
-> ethernet-service sap 10 uni 2/10-15
-> ethernet-service sap 10 uni linkagg 31
-> ethernet-service sap 10 no uni 1/3
-> ethernet-service sap 10 no uni linkagg 31
```

Release History

Release 6.3.1; command was introduced.

Related Commands

ethernet-service sap	Creates a VLAN Stacking SAP and associates the SAP with a VLAN Stacking SAP profile and service.
ethernet-service sap sap-profile	Creates a UNI profile that is used to specify how to process control packets ingressing on UNI ports.
ethernet-service uni uni-profile	Associates a VLAN Stacking UNI profile with a UNI port.

MIB Objects

```
alaEServiceSapUniTable
   alaEServiceSapUniSap
   alaEServiceSapUniUni
   alaEServiceSapUniRowStatus
```

ethernet-service sap cvlan

Associates customer VLAN (CVLAN) traffic with a VLAN Stacking Service Access Point (SAP). The parameter values configured with this command are applied to frames received on all SAP UNI ports and determines the type of customer traffic that is accepted on the UNI ports and processed by the service.

ethernet-service sap *sapid* **cvlan {all** | *cvid* **|** *cvid1-cvid2* | **untagged}**

ethernet-service sap *sapid* **no cvlan {all** | *cvid* **|** *cvid1-cvid2* | **untagged}**

Syntax Definitions

sapid	The SAP ID number (1–1024).
all	Applies the SAP profile to tagged and untagged frames.
cvid1	Applies the SAP profile to frames tagged with this CVLAN ID.
cvid1-cvid2	Applies the SAP profile to frames tagged with a CVLAN ID that falls within this range of CVLAN IDs (for example, 10-12 specifies frames tagged with CVLAN 10, 11, or 12).
untagged	Applies the SAP profile only to untagged frames.

Defaults

By default, no CVLAN traffic is associated with the SAP ID when the SAP is created.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to remove a CVLAN ID or the designation for **all** or **untagged** frames from the SAP. Note that when the last CVLAN parameter is deleted from an SAP configuration, the SAP itself is not automatically deleted.
- The **all** and **untagged** parameters are configurable in combination with a CVLAN ID. For example, if **untagged** and a CVLAN ID are associated with the same SAP ID, then the SAP profile is applied to only untagged traffic *and* traffic tagged with the specified CVLAN ID. All other traffic is dropped.
- The SAP ID specified with this command must exist. Use the **ethernet-service sap** command to create a SAP.
- Note that this command is not supported with SAP IDs that are associated with an IPMVLAN.
- Configuring both the **all** and **untagged** parameter for the same SAP is not allowed. Specify only one of these two parameters per SAP.
- When either the **all** or **untagged** parameter is configured for the SAP, the default VLAN for the UNI ports associated with the SAP is changed to the VLAN assigned to the service that is associated with the SAP.

- Only one SAP with the **all** or **untagged** option per UNI is allowed. For example, if UNI port 1/17 is part of SAP 10 and SAP 20 and SAP 10 is configured for **all** traffic, then only **untagged** or a CVLAN ID is allowed for SAP 20.

Examples

```
-> ethernet-service sap 10 cvlan 200
-> ethernet-service sap 10 cvlan all
-> ethernet-service sap 11 cvlan 100-150
-> ethernet-service sap 11 cvlan untagged
-> ethernet-service sap 10 no cvlan 200
-> ethernet-service sap 10 no cvlan 100-150
```

Release History

Release 6.3.1; command was introduced.

Related Commands

ethernet-service sap	Creates a VLAN Stacking Service Access Point (SAP) and associates the SAP with a VLAN Stacking service.

MIB Objects

```
alaEServiceSapCvlanTable
   alaEServiceSapUniSap
   alaEServiceSapUniUni
   alaEServiceSapUniRowStatus
```

ethernet-service sap-profile

Creates a profile for a VLAN Stacking Service Access Point (SAP). Profile attributes are used to define traffic engineering policies that are applied to traffic serviced by the SAP.

ethernet-service sap-profile *sap-profile-name*
[bandwidth not-assigned]
[egress-bandwidth *mbps***]**
[{shared | not-shared} ingress-bandwidth *mbps***]**
[cvlan-tag {preserve | translate}]
[priority [not-assigned | map-inner-to-outer-p | map-dscp-to-outer-p | fixed *value***]]**

no ethernet-service sap-profile *sap-profile-name*

Syntax Definitions

sap-profile-name	Alphanumeric string of up to 32 characters. Use quotes around string if the profile name contains multiple words with spaces between them (e.g., “Alcatel-Lucent Engineering”).
bandwidth not-assigned	Specifies that the profile will not allocate switch resources to enforce bandwidth requirements. Applies only when the profile specifies the default ingress bandwidth value (zero).
egress-bandwidth *mbps*	The maximum amount of egress bandwidth, in megabits per second, to be allowed for SAP ports (0-9999).
shared	Shares the ingress bandwidth limit across all SAP ports and CVLANs.
not shared	Applies the ingress bandwidth limit to individual SAP ports and CVLANs; bandwidth is not shared.
ingress-bandwidth *mbps*	The maximum amount of ingress bandwidth, in megabits per second, to be allowed for SAP ports.
cvlan-tag preserve	Retains the customer VLAN ID (inner tag) and double tags the frame with the SVLAN ID (outer tag).
cvlan-tag translate	Replaces the customer VLAN ID with the SVLAN ID.
priority not-assigned	Specifies that the SAP profile will not allocate switch resources to enforce the priority mapping. Applies only when the profile specifies the default priority value (fixed).
priority map-inner-to-outer-p	Maps the customer VLAN (inner tag) priority bit value to the SVLAN (outer tag) priority bit value.
priority map-dscp-to-outer-p	Maps the customer VLAN (inner tag) DSCP value to the SVLAN (outer tag) priority bit value.
priority fixed *value*	Sets the SVLAN (outer tag) priority bit to the specified value. Values range from 0 (lowest priority) to 7 (highest priority).

Defaults

parameter	default
shared | not shared	**shared**
mbps	0
preserve | translate	preserve
not-assigned | map-inner-to-outer-p | map-dscp-to-outer-p | fixed *value*	**fixed** 0

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to delete a SAP profile.
- If a profile is not specified when a SAP is created, a default profile (default-sap-profile) is automatically associated with the SAP.
- Use the **ethernet-service sap sap-profile** command to associate a profile to a VLAN Stacking SAP.
- Only one SAP profile name is associated with each SAP ID; however, it is possible to associate the same SAP profile name to multiple SAP IDs.
- By default, the **bandwidth not-assigned** and **priority not-assigned** parameters are not specified when a profile is created. This means that even if no bandwidth value is specified or the priority is set to fixed (the default), QoS still allocates switch resources to enforce bandwidth and priority settings for the profile. In addition, QoS policy rules cannot override the profile bandwidth or priority settings.
- Use the **bandwidth not-assigned** and **priority not-assigned** parameters to prevent the profile from triggering QoS allocation of switch resources. When a profile is created using these parameters, QoS policy rules/ACLs are then available to define more custom bandwidth and priority settings for profile traffic. For example, mapping several inner DSCP/ToS values to the same outer 802.1p value.
- Egress bandwidth can be configured only for SVLANs and not for IPMVLANs.
- A CVLAN-UNI combination associated with a SAP having egress bandwidth configuration is unique and it cannot be configured on any other SAP with egress bandwidth configuration.

Examples

```
-> ethernet-service sap-profile video1 egress-bandwidth 1000
-> ethernet-service sap-profile video1 ingress-bandwidth 10 cvlan translate
map-inner-to-outer-p
-> ethernet-service sap-profile voice1 not-shared ingress-bandwidth 10 cvlan
preserve fixed 1
-> ethernet-service sap-profile "QoS Mapping" bandwidth not-assigned priority
not-assigned
-> no ethernet-service sap-profile video1
```

Release History

Release 6.3.1; command was introduced.
Release 6.3.4; **bandwidth not-assigned** parameter added.
Release 6.4.2; **egress-bandwidth** parameter added.
Release 6.4.3; **priority not-assigned** parameter added.

Related Commands

ethernet-service sap	Creates a VLAN Stacking SAP and associates the SAP with a service.
ethernet-service sap sap-profile	Associates a SAP profile with a SAP ID.

MIB Objects

```
alaEServiceSapProfileTable
   alaEServiceSapProfileID
   alaEServiceSapProfileCVLANTreatment
   alaEServiceSapProfilePriorityMapMode
   alaEServiceSapProfileFixedPriority
   alaEServiceSapProfileIngressBW
   alaEServiceSapProfileEgressBW
   alaEServiceSapProfileBandwidthShare
   alaEServiceSapRowStatus
```

ethernet-service sap sap-profile

Associates a VLAN Stacking Service Access Point (SAP) with a SAP profile. This command is also used to change an existing SAP profile association.

ethernet-service sap *sapid* **sap-profile** *sap-profile-name*

Syntax Definitions

sapid	The SAP ID number (1–1024).
sap-profile-name	The name of the SAP profile to associate with this SAP ID.

Defaults

The “default-sap-profile” profile is automatically associated with the SAP ID when the SAP is created.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- If a profile association exists for the specified SAP ID, the current profile is replaced with the profile specified with this command.
- The SAP ID specified with this command must exist. Use the **ethernet-service sap** command to create a SAP.
- The SAP profile specified with this command must exist. Use the **ethernet-service sap-profile** command to create a SAP profile.
- To change the profile associated with the SAP back to the default profile, enter “default-sap-profile” with this command.
- Note that if the SAP ID specified with this command is associated with an IPMVLAN, the profile associated with the SAP ID must specify CVLAN tag translation. Double tagging is not supported with IPMVLAN SAPs that are also associated with a UNI port.
- Do not specify a service name; doing so will return an error message. This command is only for associating an existing profile to a VLAN Stacking SAP.

Examples

```
-> ethernet-service sap 10 sap-profile CustomerC
-> ethernet-service sap 11 sap-profile CustomerD
```

Release History

Release 6.3.1; command was introduced.

Related Commands

ethernet-service sap	Creates a VLAN Stacking SAP and associates the SAP with a VLAN Stacking SAP profile and service.
ethernet-service sap-profile	Creates a VLAN Stacking SAP profile.

MIB Objects

```
alaEServiceSapTable
   alaEServiceSapID
   alaEServiceSapProfile
   alaEServiceSapRowStatus
```

ethernet-service uni-profile

Creates a User Network Interface (UNI) profile that is used to specify how to process control packets ingressing on UNI ports.

ethernet-service uni-profile *uni-profile-name* **[tunnel-mac** *mac-address***] [l2-protocol {vtp | vlan | uplink | udld | stp | pvst | pagp | oam | mvrp | lacpmarker | gvrp | dtp | cdp | amap | 802.3ad | 802.1x | 802.1ab {peer | discard | tunnel | mac-tunnel}}**

no ethernet-service uni-profile *uni-profile-name*

Syntax Definitions

uni-profile-name	Alphanumeric string of up to 32 characters. Use quotes around string if the profile name contains multiple words with spaces between them (e.g., “Alcatel-Lucent Engineering”).
mac-address	The mac address to be used when configuring a protocol for tunnel-mac.
vtp	Cisco’s VTP Protocol.
vlan	Cisco’s VLAN Protocol.
uplink	Cisco’s Uplink Fast Protocol
udld	Cisco’s UDLD Protocol.
stp	Spanning Tree BPDU.
pvst	Cisco’s PVST Protocol.
pagp	Cisco’s PAGP Protocol.
oam	OAM Protocol.
mvrp	MVRP Protocol.
lacpmarker	LACP Marker Protocol.
gvrp	Specifies how GARP VLAN Registration Protocol packets will be processed on the UNI port.
dtp	Cisco’s DTP Protocol**.**
cdp	Cisco’s DTP Protocol**.**
amap	Specifies how Alcatel Management Adjacency Protocol packets will be processed on the UNI port.
802.3ad	Specifies how 802.3ad and 802.3ah control frames will be processed on the UNI port.
802.1x	Specifies how 802.1x control frames will be processed on the UNI port.
802.1ab	Specifies how 802.1ab control frames will be processed on the UNI port.
peer	Allows the UNI port to participate in the specified protocol.

discard	Discards the specified PDU.
tunnel	Tunnels the specified PDU across the provider network without modifying the MAC address.
mac-tunnel	Changes the destination MAC address to either the configured or default tunnel MAC address before forwarding.

Defaults

parameter	default	Protocol DA MAC Address	Default Tunnel MAC	Other	Other
stp	**tunnel**	0180c2000000	01000ccdcdd0	-	
gvrp	**tunnel**	0180c2000021	01000ccdcdd0	-	
802.3ad	**peer**	0180c2000002	01000ccdcdd0	-	
802.1x	**discard**	-	-	-	
802.1ab	**discard**	0180c200000e	01000ccdcdd0	-	
amap	**discard**	0020da007004	01000ccdcdd0	-	
vtp	**discard**	01000ccccccc	01000ccdcdd0	-	-
vlan	**discard**	01000ccdcdce	01000ccdcdd0	-	-
uplink	**discard**	01000ccdcdcd	01000ccdcdd0	-	-
udld	**discard**	01000ccccccc	01000ccdcdd0	-	-
pvst	**discard**	01000ccccccd	01000ccdcdd0	-	-
pagp	**discard**	01000ccccccc	01000ccdcdd0	-	
oam	**peer**	0180c2000002	01000ccdcdd0	-	
mvrp	**tunnel**	-	01000ccdcdd0	-	
lacpmarker	**peer**	0180c2000002	01000ccdcdd0	-	
dtp	**discard**	01000ccccccc	01000ccdcdd0	-	-
cdp	**discard**	01000ccccccc	01000ccdcdd0	-	

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to delete a UNI profile.
- Remove any UNI profile associations with UNI ports before attempting to modify or delete the profile.
- If a protocol is configured with the **mac-tunnel** parameter and no mac address has been configured, the default Tunnel MAC address from the table above is used.

- Not all of the protocol parameters are currently supported with the **peer**, **tunnel**, and **discard** parameters. Use the following table to determine the parameter combinations that are supported:

	peer	discard	tunnel
stp	no	yes	yes
802.1x	no	yes	yes
802.1ab	yes	yes	yes
802.3ad	yes	yes	yes
gvrp	no	yes	yes
amap	yes	yes	yes
vtp	no	yes	yes
vlan	no	yes	yes
uplink	no	yes	yes
udld	yes	yes	yes
pvst	no	yes	yes
pagp	no	yes	yes
oam	yes	yes	yes
mvrp	no	yes	yes
lacpmarker	yes	yes	yes
dtp	no	yes	yes
cdp	no	yes	yes

- Note that 802.3ad and 802.3ah control frames are processed the same. The **802.3ad** parameter specifies how both 802.3ad and 802.3ah control frames are to be processed on the UNI port.
- Note that the VLAN Stacking provider edge (PE) switch will not tunnel GVRP frames unless the GVRP feature and/or GVRP transparent switching functionality is enabled on the PE switch. This is true even if GVRP processing is enabled for the VLAN Stacking port.
- If a user-configured UNI profile is *not* associated with a UNI port, then the default profile (default-uni-profile) is used to process control packets ingressing on the port.

Examples

```
-> ethernet-service uni-profile uni_1 l2-protocol stp gvrp discard
-> ethernet-service uni-profile uni_1 l2-protocol vrp mac-tunnel
-> ethernet-service uni-profile uni_config_tunnel_mac tunnel-mac 00:00:00:00:00:99
-> ethernet-service uni-profile uni_config_tunnel_mac l2-protocol gvrp mac-tunnel
-> no ethernet-service uni-profile uni_1
```

Release History

Release 6.3.1; command was introduced.
Release 6.4.3; **tunnel-mac** and **mac-tunnel** parameters were added.

Related Commands

ethernet-service uni uni-profile	Associates a VLAN Stacking UNI profile with a UNI port.
ethernet-service sap uni	Configures the switch port as a VLAN Stacking UNI and associates the port with a VLAN Stacking Service Access Point (SAP).
show ethernet-service nni l2pt-statistics	Displays the profile associations for VLAN Stacking UNI ports.
show ethernet-service uni l2pt-statistics	Displays the profile attribute configuration for VLAN Stacking UNI profiles.

MIB Objects

```
alaEServiceUNIProfileTable
   alaEServiceUNIProfileID
   alaEServiceUNIProfileStpBpduTreatment
   alaEServiceUNIProfile8021xTreatment
   alaEServiceUNIProfile8021ABTreatment
   alaEServiceUNIProfile8023adTreatment
   alaEServiceUNIProfileGvrpTreatment
   alaEServiceUNIProfileAmapTreatment
   alaEServiceUNIProfileLacpTreatment
   alaEServiceUNIProfileLacpMarkerTreatment
   alaEServiceUNIProfileOamTreatment
   alaEServiceUNIProfileCiscoPagpTreatment
   alaEServiceUNIProfileCiscoUdldTreatment
   alaEServiceUNIProfileCiscoCdpTreatment
   alaEServiceUNIProfileCiscoVtpTreatment
   alaEServiceUNIProfileCiscoDtpTreatment
   alaEServiceUNIProfileCiscoPvstTreatment
   alaEServiceUNIProfileCiscoVlanTreatment
   alaEServiceUNIProfileCiscoUplinkTreatment
alaEServiceUNIProfileProtocolTreatment
   alaEServiceUNIProfileTunnelMac
   alaEServiceUNIProfileRowStatus
```

ethernet-service uni uni-profile

Associates a VLAN Stacking User Network Interface (UNI) profile with a UNI port.

ethernet-service uni {*slot/port1***[-***port2***]** | *agg_num***} uni-profile** *uni-profile-name*

Syntax Definitions

slot/port1	The slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
-port2	The last port number in a range of ports that you want to configure on the same slot (e.g, 3/1-4 specifies ports 1, 2, 3, and 4 on slot 3).
agg_num	The link aggregate ID number (0–31).
uni-profile-name	Alphanumeric string of up to 32 characters. Use quotes around string if the profile name contains multiple words with spaces between them (e.g., “Alcatel-Lucent Engineering”).

Defaults

The default profile (default-uni-profile) is used to process control packets ingressing on a UNI port. This profile is assigned at the time a port is configured as a VLAN Stacking UNI.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- This UNI specified with this command must exist in the switch configuration.
- To change the profile associated with a UNI port, use this command and specify a different profile name than the one currently associated with the port. The last profile associated with the port, is the profile that is applied to UNI port traffic.
- To change the profile associated with a UNI port back to the default profile, enter “default-uni-profile” with this command.

Examples

```
-> ethernet-service uni 1/3 uni-profile uni_1
-> ethernet-service uni 2/10-15 uni-profile default-uni-profile
-> no ethernet-service uni 1/3 uni-profile uni_1
```

Release History

Release 6.3.1; command was introduced.

Related Commands

ethernet-service sap sap-profile	Creates a UNI profile that is used to specify how to process control packets ingressing on UNI ports.
ethernet-service sap uni	Configures the switch port as a VLAN Stacking UNI and associates the port with a VLAN Stacking Service Access Point (SAP).

MIB Objects

```
alaEServicePortTable
   alaEServicePortID
   alaEServicePortType
   alaEServicePortUniProfile
   alaEServiceSapUniRowStatus
```

ethernet-service uni-profile custom-L2-protocol

Associates a custom-L2-protocol entry to a UNI profile.

ethernet-service uni-profile *uni-profile-name* **custom-L2-protocol** *custom-L2-protocol name* **{tunnel | discard | mac-tunnel}**

no ethernet-service uni-profile *uni-profile-name* **custom-L2-protocol** *custom-L2-protocol name*

Syntax Definitions

uni-profile-name	Name of the configured UNI profile.
custom-L2-protocol name	Name of the configured custom L2-protocol entry name to be associated to the UNI profile.
tunnel	Tunnels the specified PDU across the provider network without modifying the MAC address.a packet with destination MAC configured in the custom-L2-protocol entry is transparently forwarded.
discard	Discards the specified PDU.
mac-tunnel	Changes the destination MAC address to the configured tunnel MAC address of the UNI profile before forwarding.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to delete association of custom-L2-protocol entry from a UNI profile.
- Use the **mac-tunnel** action only when the custom-L2-protocol is set with an ether-type and optionally a sub-type.
- More than one custom-L2-protocol entry can be configured at a time.
- A custom-L2-protocol entry cannot be specified more than once in the command line.
- A custom-L2-protocol entry cannot be associated to a UNI profile if the UNI profile is associated to UNI port.
- UNI port recognizes L2 frames with TPID 0x8100, 0x9100 and 0x88a8. Frames with other TPIDs considered as untagged CVLAN frames.

Examples

```
-> ethernet-service uni-profile profile1 custom-L2-protocol
tunnel-mac-ethertype mac-tunnel

-> ethernet-service uni-profile profile2 custom-L2-protocol
tunnel-mac-range tunnel discard-mac discard

-> no ethernet-service uni-profile xxxxx custom-L2-protocol
tunnel-mac-ethertype  tunnel-mac-range

-> ethernet-service uni-profile profile1 custom-L2-protocol CP1 tunnel

-> ethernet-service uni-profile profile2 custom-L2-protocol CP2 mac-tunnel

-> ethernet-service uni-profile profile3 custom-L2-protocol CP3 discard

-> no ethernet-service uni-profile profile1 custom-L2-protocol CP1
```

Release History

Release 6.4.5; command introduced.

Related Commands

show ethernet-service custom-L2-protocol	Displays configuration information of the specific custom-L2-protocol entry if specified or displays information of all the configured custom-L2-protocol entries in the system.

MIB Objects

```
alaEServiceUNIProfileL2CustomProtocolTable
   AlaEServiceUNIProfileL2CustomProtocolEntry
   alaEServiceUNIProfileID
   alaEServiceUNIProfileL2CustomProtocolID
   alaEServiceUNIProfileL2CustomProtocolTreatment
   alaEServiceUNIProfileL2CustomProtocolRowStatus
```

show ethernet-service custom-L2-protocol

Displays configuration information of the specific custom-L2-protocol entry if specified or displays information of all the configured custom-L2-protocol entries in the system.

show ethernet-service custom-L2-protocol *custom-L2-protocol*

Syntax Definitions

custom-L2-protocol	Name of the configured custom-L2-protocol entry for which the information must be displayed.

Defaults

By default, the configuration information of all the configured custom-L2-protocol entries are displayed if a custom-L2-protocol entry name is not specified with this command.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

Enter the name of a custom-L2-protocol entry for which the configuration information must be displayed.

Examples

```
-> show ethernet-service custom-l2-protocol

Custom
L2 Protocol    Mac               Mask              Ether-Type   Sub-Type
                                                   (or)          (or)
                                                   Ssap/Dsap     Pid
--------------+------------------+----------------+------------+-----------
prof1          01:80:c2:01:02:03     -                 0xaa/aa      0x0003
prof2          01:80:c2:01:02:03     -                 0x0601       0xff
prof3          01:80:c2:01:02:03     -                 0x0601        -
prof4          01:80:c2:01:02:03     -                 -             -
prof5          01:80:c2:01:02:03   ff:ff:ff:ff:ff:00   -             -
```

output definitions

Custom L2 Protocol	The name of the configured custom L2-protocol entry.
MAC	Displays the MAC address associated to custom L2-protocol entry.
Mask	Displays the mask for the specified MAC address.
Ether-Type	Displays the ether-type value for generic ether-type.
Sub-Type	Displays the subtype value.

Release History

Release 6.4.5; command introduced.

Related Commands

ethernet-service custom-L2-protocol	Creates a custom L2-protocol entry MAC address and optional mask or ether-type with optional subtype.

MIB Objects

```
alaEServiceL2CustomProtocolTable
   AlaEServiceL2CustomProtocolEntry
   alaEServiceL2CustomProtocolID
   alaEServiceL2CustomProtocolMac
   alaEServiceL2CustomProtocolMask
   alaEServiceL2CustomProtocolEtherType
   alaEServiceL2CustomProtocolEtherSubType
   alaEServiceL2CustomProtocolSsap
   alaEServiceL2CustomProtocolDsap
   alaEServiceL2CustomProtocolPid
```

show ethernet-service mode

Displays the active VLAN Stacking mode for the switch.

show ethernet-service mode

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

This command is available in both modes: Legacy or EServices.

Examples

```
-> show ethernet-service mode
Vlan Stacking Mode: Legacy Mode

-> show ethernet-service mode
Vlan Stacking Mode: EServices Mode
```

output definitions

Vlan Stacking Mode	Displays the current VLAN Stacking mode (**Legacy Mode** or **EServices Mode**).

Release History

Release 6.3.1; command was introduced.

Related Commands

show ethernet-service	Displays configuration information for VLAN Stacking Ethernet services.

MIB Objects

```
alaEServiceInfo
   alaEServiceMode
```

show ethernet-service vlan

Displays a list of SVLANs configured fro the switch.

show ethernet-services vlan [*svid1***-[***svid2***]]**

Syntax Definitions

svid1	The VLAN ID number identifying the SVLAN (2–4094).
-svid2	The last VLAN ID number in a range of SVLANs that you want to specify (e.g. 10-12 specifies VLANs 10, 11, and 12).

Defaults

By default, all SVLANs are displayed if an SVLAN or range of SVLANs is not specified with this command.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

Specify a single SVLAN ID or a range of SVLAN IDs to display configuration information for a specific SVLAN or range of SVLANs.

Examples

```
-> show ethernet-services vlan
  vlan           Type                    name
+--------+------------+-------------------------+
  4010     svlan          Customer ABC
  4011     ipmvlan        Video-Service
  4020     mgmt           Provider Management
  4021     svlan          Customer XYZ
  4030     ipmvlan        HBO

-> show ethernet-service vlan 4010
Name                : Customer ABC
Traffic Type        : svlan
```

output definitions

vlan	The SVLAN ID number identifying the instance.
Traffic Type	The type of SVLAN (**svlan** = customer traffic, **mgmt** = management traffic, or **ipmvlan** = IP Multicast VLAN traffic).
name	The user-defined text description for the SVLAN. By default, the SVLAN ID is specified for the description.

Release History

Release 6.3.1; command was introduced.

Related Commands

ethernet-service	Creates a VLAN Stacking VLAN (SVLAN) for tunneling customer traffic, a management SVLAN for provider traffic, or an SVLAN that the IP Multicast VLAN (IPMV) application will use to distribute multicast traffic.
show ethernet-service	Displays configuration information for VLAN Stacking Ethernet services.

MIB Objects

```
vlanTable
   vlanNumber
   vlanDescription
   vlanSvlanTrafficType
```

show ethernet-service

Displays configuration information for VLAN Stacking Ethernet services.

show ethernet-service [service-name *service-name* | **svlan** *svid***]**

Syntax Definitions

service-name	The name of an existing VLAN Stacking service; an alphanumeric string of up to 32 characters. Use quotes around string if the VLAN name contains multiple words with spaces between them (e.g., “Alcatel-Lucent Engineering”).
svid	The VLAN ID number that identifies an existing SVLAN (2–4094).

Defaults

By default, all services are displayed if a service name or SVLAN ID is not specified with this command.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Enter the name of a service to display configuration information for a specific service.
- Enter an SVLAN ID to display configuration information for all services that are associated with a specific SVLAN.

Examples

```
-> show ethernet-service

Service Name : VideoOne
    SVLAN   : 300
    NNI(s)  : 2/1, 3/2
    SAP Id  : 20
        UNIs        : 1/1, 1/2
        CVLAN(s)    : 10, 20
        sap-profile : sap-video1
    SAP Id  : 30
        UNIs        : 1/3
        CVLAN(s)    : untagged, 40
        sap-profile : sap-video2

Service Name : CustomerABC
    SVLAN   : 255
    NNI(s)  : 1/22
    SAP Id  : 10
        UNIs        : 2/10, 2/11
        CVLAN(s)    : 500, 600
        sap-profile : default-sap-profile
```

```
Service Name : ipmv_service
    IPMVLAN : 40
    NNI(s)  : No NNIs configured
    SAP Id  : 2
        UNIs        : 1/22
        CVLAN(s)    : 100
        sap-profile : translate_profile

-> show ethernet-service service-name CustomerABC

Service Name : CustomerABC
    SVLAN   : 255
    NNI(s)  : 1/22
    SAP Id  : 10
        UNIs        : 2/10, 2/11
        CVLAN(s)    : 500, 600
        sap-profile : default-sap-profile

-> show ethernet-service svlan 300

Service Name : VideoOne
    SVLAN   : 300
    NNI(s)  : 2/1, 3/2
    SAP Id  : 20
        UNIs        : 1/1, 1/2
        CVLAN(s)    : 10, 20
        sap-profile : sap-video1
    SAP Id  : 30
        UNIs        : 1/3
        CVLAN(s)    : 30, 40
        sap-profile : sap-video2
```

output definitions

Service Name	The name of the VLAN Stacking service.
SVLAN or IPMVLAN	Displays the SVLAN ID associated with the service. Note that SVLAN appears as the field name if the VLAN ID is an SVLAN; IPMVLAN appears as the field name if the VLAN ID is an IP Multicast SVLAN.
NNI(s)	VLAN Stacking Network Network Interface ports associated with the service to tunnel SVLAN customer traffic.
SAP Id	The ID number for the VLAN Stacking Service Access Point that is applied to the service (1-1024).
UNIs	VLAN Stacking User Network Interface ports that receive customer traffic.
CVLAN(s)	Customer VLAN IDs ingressing on UNI ports.
sap-profile	The name of the SAP profile associated with the SAP.

Release History

Release 6.3.1; command was introduced.

Related Commands

ethernet-service service-name	Creates a VLAN Stacking service and associates the service with an SVLAN or an IPMVLAN.
show ethernet-service vlan	Displays a list of all or a range of configured SVLANs or the parameters of a specified SVLAN.

MIB Objects

```
alaEServiceTable
   alaEServiceID
   alaEServiceSVLAN
alaEServiceNniSvlanTable
   alaEServiceNniSvlanNni
alaEServiceSapTable
   alaEServiceSapID
alaEServiceSapUniTable
   alaEServiceSapUniUni
alaEServiceSapCvlanTable
   alaEServiceSapCvlanCvlan
   alaEServiceSapCvlanMapType
alaEServiceSapProfileTable
   alaEServiceProfileID
```

show ethernet-service sap

Displays configuration information for VLAN Stacking Service Access Points (SAP).

show ethernet-services sap [*sapid***]**

Syntax Definitions

sapid	The SAP ID number identifying the service instance (1-1024).

Defaults

By default, all SAPs are displayed if a SAP ID is not specified with this command.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

Specify a single SAP ID (1-1024) to display configuration information for a specific SAP.

Examples

```
-> show ethernet-services sap

   SAP Id  : 10
        UNIs        : 2/10, 2/11
        CVLAN(s)    : 500, 600
        sap-profile : default-sap-profile

    SAP Id  : 20
        UNIs        : 1/1, 1/2
        CVLAN(s)    : 10, 20
        sap-profile : sap-video1

    SAP Id  : 30
        UNIs        : 1/3
        CVLAN(s)    : 30, 40
        sap-profile : sap-video2

-> show ethernet-service sap 10

 SAP Id  : 10
        UNIs        : 2/10, 2/11
        CVLAN(s)    : 500, 600
        sap-profile : default-sap-profile
```

output definitions

SAP Id	The ID number for the VLAN Stacking Service Access Point that is applied to the service.
UNIs	VLAN Stacking User Network Interface ports that receive customer traffic.
CVLAN(s)	Customer VLAN IDs ingressing on UNI ports.
sap-profile	The name of the SAP profile associated with the SAP.

Release History

Release 6.3.1; command was introduced.

Related Commands

ethernet-service sap	Creates a VLAN Stacking Service Access Point (SAP) and associates the SAP with a VLAN Stacking SAP profile and service.
show ethernet-service	Displays configuration information for VLAN Stacking Ethernet services.

MIB Objects

```
alaEServiceSapTable
   alaEServiceSapID
alaEServiceSapUniTable
   alaEServiceSapUniUni
alaEServiceSapCvlanTable
   alaEServiceSapCvlanCvlan
   alaEServiceSapCvlanMapType
alaEServiceSapProfileTable
   alaEServiceProfileID
```

show ethernet-service port

Displays configuration information for a VLAN Stacking service port.

show ethernet-services port {*slot/port* | **linkagg** *agg_num***}**

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).
agg_num	The link aggregate ID number (0–31).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

Specifying a slot/port or link aggregate ID number is required with this command.

Examples

```
-> show ethernet-service port 1/10

Interface : 1/10
Port Type   : UNI
    UNI Profile   : default-uni-profile
    Default SVLAN : 4095

Service Name : ipmv_service
    IPMVLAN : 40
    NNI(s)  : No NNIs configured
    SAP Id  : 2
        UNIs        : 1/10
        CVLAN(s)    : 100
        sap-profile : translate_profile

Service Name : svlan_service
    SVLAN   : 20
    NNI(s)  : No NNIs configured
    SAP Id  : 1
        UNIs        : 1/10
        CVLAN(s)    : 200
        sap-profile : translate_profile
```

```
-> show ethernet-service port 1/22

Interface : 1/22
Port Type : NNI

Service Name : CustomerABC
    SVLAN   : 255
    NNI(s)  : 1/22
    SAP Id  : 10
        UNIs        : 2/10, 2/11
        CVLAN(s)    : 500, 600
        sap-profile : default-sap-profile

Service Name : Video-Service
    SVLAN   : 300
    NNI(s)  : 1/22, 3/2
    SAP Id  : 20
        UNIs        : 1/1, 1/2
        CVLAN(s)    : 10, 20
        sap-profile : sap-video1
    SAP Id  : 30
        UNIs        : 1/3
        CVLAN(s)    : 30, 40
        sap-profile : sap-video2
```

output definitions

Interface	The slot and port number or link aggregate ID for the specified interface.
Port Type	The type of VLAN Stacking port (**UNI** or **NNI**).
Service Name	The name of the VLAN Stacking service.
SVLAN or IPMVLAN	Displays the SVLAN ID associated with the service. Note that SVLAN appears as the field name if the VLAN ID is an SVLAN; IPMVLAN appears as the field name if the VLAN ID is an IP Multicast SVLAN.
NNI(s)	VLAN Stacking Network Network Interface ports associated with the service to tunnel SVLAN customer traffic.
SAP Id	The ID number for the VLAN Stacking Service Access Point that is applied to the service (1-1024).
UNIs	VLAN Stacking User Network Interface ports that receive customer traffic.
CVLAN(s)	Customer VLAN IDs ingressing on UNI ports.
sap-profile	The name of the SAP profile associated with the SAP.

Release History

Release 6.3.1; command was introduced.

Related Commands

ethernet-service svlan nni	Configures the switch port as a VLAN Stacking NNI port and associates the port with a customer SVLAN, management SVLAN, or an IP Multicast VLAN (IPMV).
ethernet-service sap uni	Configures the switch port as a VLAN Stacking UNI and associates the port with a VLAN Stacking SAP.
show ethernet-service	Displays configuration information for VLAN Stacking Ethernet services.

MIB Objects

```
alaEServiceTable
   alaEServiceID
   alaEServiceSVLAN
alaEServiceNniSvlanTable
   alaEServiceNniSvlanNni
alaEServiceSapTable
   alaEServiceSapID
alaEServiceSapUniTable
   alaEServiceSapUniUni
alaEServiceSapCvlanTable
   alaEServiceSapCvlanCvlan
   alaEServiceSapCvlanMapType
alaEServiceSapProfileTable
   alaEServiceProfileID
```

show ethernet-service nni

Displays configuration information for VLAN Stacking Network Network Interface (NNI) ports.

show ethernet-services nni [*slot/port* | **linkagg** *agg_num***]**

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).
agg_num	The link aggregate ID number (0–31).

Defaults

By default, all NNI ports are displayed if a slot/port or link aggregate ID number is not specified.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

Use the *slot/port* or **linkagg** *agg_num* parameter to display information for a specific switch port or link aggregate ID.

Examples

```
-> show ethernet-service nni

Port  TPID   Legacy STP BPDU Legacy GVRP BPDU Legacy MVRP BPDU Transparent Bridging
-----+------+---------------+----------------+----------------+--------------------
1/22  0x8100     Disable         Disable          Disable            Disable
1/23  0x8100     Disable         Disable          Disable            Disable

- show ethernet-service nni 1/23

Port  TPID   Legacy STP BPDU Legacy GVRP BPDU Legacy MVRP BPDU Transparent Bridging
-----+------+---------------+----------------+----------------+--------------------
1/23  0x8100     Disable         Disable          Disable            Disable
```

output definitions

Port	The slot/port number or link aggregate ID for the NNI port.
TPID	The vendor TPID value configured for the NNI port.
Legacy STP BPDU	Whether or not the NNI port will process STP legacy BPDU.
Legacy GVRP BPDU	Whether or not the NNI port will process GVRP legacy BPDU.
Legacy MVRP BPDU	Whether or not the NNI port will process MVRP legacy BPDU.
Transparent Bridging	Whether or not transparent bridging is enabled for the NNI port.

Release History

Release 6.3.1; command was introduced.
Release 6.3.4; **Transparent Bridging** field added.
Release 6.4.3: **Legacy MVRP BPDU** field added.

Related Commands

ethernet-service svlan nni	Configures the switch port as a VLAN Stacking NNI port and associates the port with a customer SVLAN, management SVLAN, or an IP Multicast VLAN (IPMV).
ethernet-service nni	Configures the vendor TPID value, the legacy BPDU processing status, and the transparent bridging status for a VLAN Stacking NNI port.
show ethernet-service	Displays configuration information for VLAN Stacking Ethernet services.

MIB Objects

```
alaEServicePortTable
   alaEServicePortID
   alaEServicePortVendorTpid
   alaEServicePortLegacyStpBpdu
   alaEServicePortLegacyGvrpBpdu
   alaEServicePortLegacyMvrpBpdu
```

show ethernet-service nni l2pt-statistics

Displays the statistics information of Network Network Interface (NNI) ports.

show ethernet-services nni [*slot/port* | **linkagg** *agg_num***] l2pt-statistics**

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).
agg_num	The link aggregate ID number (0–31).

Defaults

By default, all NNI ports are displayed if a slot/port or link aggregate ID number is not specified.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

Use the *slot/port* or **linkagg** *agg_num* parameter to display statistics information for a specific switch port or link aggregate ID.

Examples

```
-> show ethernet-service nni L2PT-statistics

Slot/Port   Rx Mac-Tunnel     Mac-tunnel discard
---------+-----------------+-----------------------
1/23        1234                 2
1/24        256                  0
```

output definitions

Slot/Port	The slot/port number or link aggregate ID for the NNI port.
Rx Mac-Tunnel	The total number of frames trapped to CPU with tunnel MAC.
Mac-tunnel discard	The total number of discarded frames that are trapped to CPU with tunnel MAC.

Release History

Release 6.4.5; command was introduced.

Related Commands

ethernet-service svlan nni	Configures the switch port as a VLAN Stacking NNI port and associates the port with a customer SVLAN, management SVLAN, or an IP Multicast VLAN (IPMV).
ethernet-service nni	Configures the vendor TPID value, the legacy BPDU processing status, and the transparent bridging status for a VLAN Stacking NNI port.
show ethernet-service	Displays configuration information for VLAN Stacking Ethernet services.
clear ethernet-service nni l2pt-statistics	Clears all Network Network Interface (NNI) ports statistics.

MIB Objects

```
AlaEServiceUNIPortL2StatisticsEntry
   alaEServiceNNIPortID
   alaEServiceNNIPortL2RxMACTunneledFrames
   alaEServiceNNIPortL2MACTunneledDiscardFrames
```

clear ethernet-service nni l2pt-statistics

Clears all Network Network Interface (NNI) ports statistics.

clear ethernet-services nni [linkagg *agg_num* | *slot/port* | *port range***] l2pt-statistics**

Syntax Definitions

agg_num	The link aggregate ID number (0–31) for which the statistics is to be cleared.
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) for which the statistics is to be cleared.
port range	Range of port for which the statistics is to be cleared.

Defaults

By default, statistics of all NNI ports are cleared if a slot/port or port range or link aggregate ID number is not specified.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

Use the *slot/port* or port range or **linkagg** *agg_num* parameter to clear statistics information for a specific switch port or range of ports or link aggregate ID.

Examples

```
-> clear ethernet-service nni L2PT-statistics
```

Release History

Release 6.4.5; command was introduced.

Related Commands

ethernet-service svlan nni	Configures the switch port as a VLAN Stacking NNI port and associates the port with a customer SVLAN, management SVLAN, or an IP Multicast VLAN (IPMV).
ethernet-service nni	Configures the vendor TPID value, the legacy BPDU processing status, and the transparent bridging status for a VLAN Stacking NNI port.
show ethernet-service	Displays configuration information for VLAN Stacking Ethernet services.
show ethernet-service nni l2pt-statistics	Displays the statistics information of Network Network Interface (NNI) ports.

MIB Objects

```
AlaEServiceNNIPortL2ProtocolStatisticsEntry
   alaEServiceNNIPortID
   alaEServiceNNIPortL2ClearStats
   alaEServiceNNIPortL2GlobalClearStatistics
```

show ethernet-service uni

Displays a list of UNI ports configured for the switch and the profile association for each port.

show ethernet-service uni [*slot/port* | **linkagg** *agg_num***]**

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).
agg_num	The link aggregate ID number (0–31).

Defaults

By default, profile information for all UNI ports is displayed if a slot/port or link aggregate ID number is not specified.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

Specify a slot/port or link aggregate ID number to display information for a single slot/port or link aggregate ID.

Examples

```
-> show ethernet-service uni

    Port    UNI Profile
+--------+--------------------+
     1/1   uni-profile-default
     1/2   multi-site
     1/3   multi-site

- show ethernet-service uni 1/3

    Port    UNI Profile
+--------+--------------------+
     1/3   multi-site
```

output definitions

Port	The slot/port number or link aggregate ID for the UNI port.
UNI Profile	The UNI profile associated with the port.

Release History

Release 6.3.1; command was introduced.

Related Commands

ethernet-service sap sap-profile	Creates a UNI profile that is used to specify how to process control packets ingressing on UNI ports.
ethernet-service uni uni-profile	Associates a VLAN Stacking UNI profile with a UNI port.
show ethernet-service uni l2pt-statistics	Displays the profile attribute configuration for VLAN Stacking User Network Interface (UNI) profiles.

MIB Objects

```
alaEServiceUniProfileTable
   alaEServicePortID
   alaEServicePortProfileID
```

show ethernet-service uni l2pt-statistics

Displays the statistics of all protocols configured per UNI port.

show ethernet-service uni [*slot/port* | **linkagg** *agg_num***] l2pt-statistics**

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).
agg_num	The link aggregate ID number (0–31).

Defaults

By default, statistics information for all UNI ports and associated l2 protocols is displayed if a slot/port or link aggregate ID number is not specified.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

Specify a slot/port or link aggregate ID number to display information for a single slot/port or link aggregate ID.

Examples

```
-> show ethernet-service uni L2PT-statistics

Rx, Tunnel and Drop are counted only in software
                                                Mac     Mac         Source
Slot/Port L2 Protocol   Rx  Tunnel Drop Peer Tunnel  De-tunnel     MAC
---------+-----------+-----+------+----+----+------+----------+-------------
1/1       STP           10   0       0    0    10      10      000000:000001
1/1       802.1x        10   0       0    0    10      10      000000:000001
1/1       802.3ad       10   0       0    10   0       0       000000:000001
1/1       802.1ab       0    0       0    0    0       0       -
1/1       GVRP          0    0       0    0    0       0       -
1/1       AMAP          0    0       0    0    0       0       -
1/1       OAM           0    0       0    0    0       0       -
1/1       LACPMARKER    0    0       0    0    0       0       -
1/1       UDLD          0    0       0    0    0       0       -
1/1       PAPG          10   10      0    0    0       0       000000:000001
1/1       CDP           10   0       10   0    0       0       000000:000001
1/1       VTP           10   0       0    0    10      0       000000:000001
1/1       DTP           10   10      0    0    0       10      000000:000001
1/1       PVST          0    0       0    0    0       0       -
1/1       VLAN          0    0       0    0    0       0       -
1/1       UPLINK        0    0       0    0    0       0       -
1/1       MVRP          0    0       0    0    0       0       -
1/1       STP           10   0       0    0    10      10      000000:000001
1/2       802.1x1       0    0       0    0    10      10      000000:000001
1/2       802.3ad       10   0       0    10   0       0       000000:000001
```

```
1/2       802.1ab       0    0       0    0    0       0       -
1/2       GVRP          0    0       0    0    0       0       -
1/2       AMAP          0    0       0    0    0       0       -
1/2       OAM           0    0       0    0    0       0       -
1/2       LACPMARKER    0    0       0    0    0       0       -
1/2       UDLD          0    0       0    0    0       0       -
1/2       PAPG          10   10      0    0    0       0       000000:000001
1/2       CDP           10   0       10   0    0       0       000000:000001
1/2       VTP           10   0       0    0    10      0       000000:000001
1/2       DTP           10   10      0    0    0       10      000000:000001
1/2       PVST          0    0       0    0    0       0       -
1/2       VLAN          0    0       0    0    0       0       -
1/2       UPLINK        0    0       0    0    0       0       -
1/2       MVRP          0    0       0    0    0       0       -
1/2       Custom 1      1    1       0    0    0       0       000000:000002
```

output definitions

Slot/Port	Service UNI port associated with an L2 protocol and L2 protocol statistics.
L2 Protocol	The l2 protocol associated with the service UNI port.
Rx	The total number of frames received by the protocol on the port and trapped in CPU.
Tunnel	The total number of tunneled frames received by the protocol on the port and trapped in CPU.
Drop	The total number of tunneled frames received by the protocol on the port and trapped in CPU and dropped.
Peer	The total number of tunneled frames received by the protocol on the port and trapped in CPU and peered.
Mac Tunnel	The total number of tunneled frames received by the protocol on the port and trapped in CPU and MAC tunneled.
Mac De-tunnel	The total number of tunneled frames received by the protocol on the port and trapped in CPU and MAC de-tunneled.
Source MAC	Specifies the source MAC address of the last frame of the protocol on the port trapped in CPU.

Release History

Release 6.4.5; command was introduced.

Related Commands

ethernet-service sap sap-profile	Creates a UNI profile that is used to specify how to process control packets ingressing on UNI ports.
ethernet-service uni uni-profile	Associates a VLAN Stacking UNI profile with a UNI port.
show ethernet-service uni l2pt-statistics	Displays the profile attribute configuration for VLAN Stacking User Network Interface (UNI) profiles.
clear ethernet-service uni l2pt-statistics	Clears the statistics of all protocols configured per UNI port.

MIB Objects

```
alaEServiceUNIPortL2ProtocolStatisticsTable
   AlaEServiceUNIPortL2StatisticsEntry
   alaEServiceUNIPortID
   alaEServiceUNIPortL2ProtocolID
   alaEServiceUNIPortL2RxFrames
   alaEServiceUNIPortL2TunneledFrames
   alaEServiceUNIPortL2DroppedFrames
   alaEServiceUNIPortL2PeeredFrames
   alaEServiceUNIPortL2MACTunneledFrames
   alaEServiceUNIPortL2MACDeTunneledFrames
   alaEServiceUNIPortL2LastSourceMAC
```

clear ethernet-service uni l2pt-statistics

Clears the statistics of all protocols configured per UNI port.

clear ethernet-service uni [linkagg *agg_num* | *slot/port* | *port range***] l2pt-statistics**

Syntax Definitions

agg_num	The link aggregate ID number (0–31) for which the statistics is to be cleared.
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) for which the statistics is to be cleared.
port range	Range of port for which the statistics is to be cleared.

Defaults

By default, statistics information for all UNI ports and associated l2 protocols is displayed if a slot/port or link aggregate ID number is not specified.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

Specify a slot/port or port range or link aggregate ID number to clear statistics for a single slot/port or the range of port or link aggregate ID.

Examples

```
-> clear ethernet-service uni 1/1 L2PT-statistics
```

Release History

Release 6.4.5; command was introduced.

Related Commands

ethernet-service sap sap-profile	Creates a UNI profile that is used to specify how to process control packets ingressing on UNI ports.
ethernet-service uni uni-profile	Associates a VLAN Stacking UNI profile with a UNI port.
show ethernet-service uni l2pt-statistics	Displays the profile attribute configuration for VLAN Stacking User Network Interface (UNI) profiles.
show ethernet-service uni l2pt-statistics	Displays the statistics of all protocols configured per UNI port.

MIB Objects

```
AlaEServiceUNIPortL2ProtocolStatisticsClearEntry
   alaEServiceUNIPortClearID
   alaEServiceUNIPortL2ClearStats
   alaEServiceUNIPortL2GlobalClearStatistics
```

show ethernet-service uni-profile

Displays the profile attribute configuration for VLAN Stacking User Network Interface (UNI) profiles.

show ethernet-service uni-profile [*uni-profile-name***]**

Syntax Definitions

uni-profile-name	Alphanumeric string of up to 32 characters. Use quotes around string if the profile name contains multiple words with spaces between them (e.g., “Alcatel-Lucent Engineering”).

Defaults

By default, all UNI profiles are displayed if a UNI profile name is not specified with this command.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

Specify a UNI profile name to display attributes for a single UNI profile.

Examples

```
-> show ethernet-service uni-profile
Profile Name: default-uni-profile
  Tunnel MAC : 01:00:0c:cd:cd:d0,
  STP : tunnel,     802.1x : drop,       802.3ad : peer,       802.1ab    : drop,
  GVRP: tunnel,     AMAP   : drop,       OAM     : peer,       LACPMARKER : peer,
  UDLD: drop,       PAGP   : drop,       CDP     : drop,       VTP        : drop,
  DTP : drop,       PVST   : drop,       VLAN    : drop,       UPLINK     : drop,
  MVRP: tunnel
```

output definitions

Profile Name	The name of the UNI profile.
Tunnel MAC	The MAC address to be used for mac tunneling.
PROTOCOL: mode	The protocol and configured mode: **peer -** The UNI port is participating in the specified protocol. **drop -** Discards the specified PDU **tunnel -** The PDU is being tunneled across the provider network without modifying the MAC address. **mac-tunnel -** The PDU is being tunneled across the provider network after changing the destination MAC address.

Release History

Release 6.3.1; command was introduced.
Release 6.4.3; **Tunnel MAC** field and **mac-tunnel** mode were added.

Related Commands

ethernet-service uni-profile	Creates a UNI profile that is used to specify how to process control packets ingressing on UNI ports.
ethernet-service uni uni-profile	Associates a VLAN Stacking UNI profile with a UNI port.
show ethernet-service nni l2pt-statistics	Displays the profile associations for VLAN Stacking User Network Interface (UNI) ports.

MIB Objects

```
alaEServiceUNIProfileTable
   alaEServiceUNIProfileID
   alaEServiceUNIProfileStpBpduTreatment
   alaEServiceUNIProfile8021xTreatment
   alaEServiceUNIProfile8021ABTreatment
   alaEServiceUNIProfile8023adTreatment
   alaEServiceUNIProfileGvrpTreatment
   alaEServiceUNIProfileAmapTreatment
   alaEServiceUNIProfileLacpTreatment
   alaEServiceUNIProfileLacpMarkerTreatment
   alaEServiceUNIProfileOamTreatment
   alaEServiceUNIProfileCiscoPagpTreatment
   alaEServiceUNIProfileCiscoUdldTreatment
   alaEServiceUNIProfileCiscoCdpTreatment
   alaEServiceUNIProfileCiscoVtpTreatment
   alaEServiceUNIProfileCiscoDtpTreatment
   alaEServiceUNIProfileCiscoPvstTreatment
   alaEServiceUNIProfileCiscoVlanTreatment
   alaEServiceUNIProfileCiscoUplinkTreatment
alaEServiceUNIProfileProtocolTreatment
   alaEServiceUNIProfileTunnelMac
   alaEServiceUNIProfileRowStatus
```

show ethernet-service sap-profile

Displays the profile attribute configuration for VLAN Stacking Service Access Point (SAP) profiles.

show ethernet-service sap-profile *sap-profile-name*

Syntax Definitions

sap-profile-name	Alphanumeric string of up to 32 characters. Use quotes around string if the profile name contains multiple words with spaces between them (e.g., “Alcatel-Lucent Engineering”).

Defaults

By default, all SAP profiles are displayed if a SAP profile name is not specified with this command.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Specify a SAP profile name to display attributes for a single SAP profile.
- Egress bandwidth can be configured only for SVLANs and not for IPMVLANs.

Examples

```
-> show ethernet-service sap-profile

   Profile Name      Ingr/Egr    Ingr Bw     Inner Tag   Priority  Priority
                         Bw      Sharing      Option     Mapping     Value
-------------------+-----------+-----------+-----------+----------+-------+
audiosap               0/10      Disable     Preserve     fixed      0
default-sap-profile    0/0       Enable      Preserve     fixed      0
sap-video1             0/0       NA          Preserve     in-out     P
sap-conf-video2        10/20     Enable      Preserve     NA         NA

-> show ethernet-service sap-profile sap-video1

   Profile Name      Ingr/Egr    Ingr Bw     Inner Tag   Priority  Priority
                         Bw      Sharing      Option     Mapping     Value
-------------------+-----------+-----------+-----------+----------+-------+
sap-video1             0/0       NA           Preserve     in-out     P
```

output definitions

Profile Name	The name of the SAP profile.
Ingr/Egr Bw	The maximum amount of ingress-bandwidth (1=1,000,000 mbps) and egress-bandwidth (0-9999) allowed for SAP ports.

output definitions

Ingr Bw Sharing	The status of bandwidth sharing (**enable**, **disable**, or **NA**). If enabled, the ingress bandwidth value is shared across all SAP ports and CVLANs. If disabled, the bandwidth value is not shared and applied to individual SAP ports and CVLANs. If **NA** displays in this field, the bandwidth value for the profile is not assigned.
Inner Tag Option	Indicates how the CVLAN tag is processed (**translate** or **preserve**). If set to **preserve**, the CVLAN tag is retained and the SVLAN is added to the frame. If set to **translate**, the CVLAN tag is changed to the SVLAN tag.
Priority Mapping	Indicates how the priority value is configured for the SVLAN (**in-ou, fixed**, or **NA**). If set to **in-out**, the CVLAN priority value is mapped to the SVLAN. If set to fixed, a user-specified priority value is used for the SVLAN priority. If set to **NA**, the priority for the profile is not assigned.
Priority Value	Indicates the priority value mapped to the SVLAN (a number, **P**, **DSCP**, or **NA**). A number indicates a fixed, user-specified value is used; **P** indicates the CVLAN 802.1p bit value is used; **DSCP** indicates the CVLAN DSCP value is used; **NA** indicates the priority value for the profile is not assigned.

Release History

Release 6.3.1; command was introduced.
Release 6.4.2; **Egr** (egress bandwidth) field added along with **Ingr** (ingress bandwidth) field.
Release 6.4.3; **NA** used to indicate bandwidth/priority values for the profile are not assigned.

Related Commands

ethernet-service sap-profile	Creates a profile for a VLAN Stacking Service Access Point (SAP).
ethernet-service sap	Creates a VLAN Stacking SAP and associates the SAP with a service and SAP profile.
ethernet-service sap sap-profile	Specifies a different SAP profile for the SAP.
show ethernet-service sap	Displays configuration information for VLAN Stacking SAPs.

MIB Objects

```
alaEServiceSapProfileTable
   alaEServiceSapProfileID
   alaEServiceSapProfileCVLANTreatment
   alaEServiceSapProfilePriorityMapMode
   alaEServiceSapProfileFixedPriority
   alaEServiceSapProfileIngressBW
   alaEServiceSapProfileEgressBW
   alaEServiceSapProfileBandwidthShare
```

loopback-test

Configures a wire-speed Ethernet loopback test profile and enables or disables the activation of the profile. The loopback test profile specifies the switch attributes that are required to conduct an ingress or egress loopback operation on a switch port.

loopback-test *profile_name* **source-mac** *src_address* **destination-mac** *dest_address* **vlan** *vlan_id* **loopback-port** *slot/port* **type {inward | outward}**

loopback-test *profile_name* **{enable | disable}**

no loopback-test *profile_name*

Syntax Definitions

profile_name	Alphanumeric string of up to 31 characters. Use quotes around string if the profile name contains multiple words with spaces between them (e.g., “Alcatel-Lucent Engineering”).
src_address	A unique source MAC address for the test frame.
dest_address	A unique destination MAC address for the test frame.
vlan_id	The VLAN ID of the test frame. Always use the outer VLAN ID.
slot/port	The switch port number to use for the loopback test.
inward	Sets the type of loopback test to ingress.
outward	Sets the type of loopback test to egress.
enable	Enables the loopback test profile.
disable	Disables the loopback test profile.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to delete a loopback profile.
- Use the **loopback-test enable** command to enable the loopback test profile on the specified port. When the profile is enabled, the loopback operation is enabled for the port.
- Use the **loopback-test disable** command to disable the loopback operation for the specified port.
- Once a UNI or NNI port is designated as a loopback port, the port is no longer eligible to participate in other switch functions. In addition, an outward loopback port goes “out-of-service” and will no longer carry customer traffic but remains active for test frame traffic. However, an inward loopback port remains “in-service” and will continue to carry customer traffic as well as test frame traffic.

- Only Layer 2 loopback tests are supported, so test frames are not routed. As a result, the loopback test operation will only swap the source and destination MAC address of bridged test frames.
- In a typical ingress loopback scenario, specifying the switch base MAC addess as the destination address is recommended. In a typical egress loopback scenario, a customer premises equipment (CPE) MAC address can be used, but configuring and using a static MAC address on the egress loopback port is recommended.
- The port specified for an inward loopback test is the port on which test frames are received and looped back. The port specified for an outward test is the egress destination port on which test frames are looped back. The loopback operation performed on the specified port swaps the source and destination MAC address of the test frame and then forwards the frame back to the test head.
- The switch creates a static MAC address entry for the egress port when the outward loopback profile is applied on that port.. The static address created is the destination MAC address specified in the profile. If the switch receives a non-test frame that contains the same MAC address, both the test and non-test frames are filtered even if they were received on different ports.
- If the MAC addresses specified in the loopback test profile are actual network address (for example, 02:da:95:e1:22:10, not aa:aa:aa:aa:aa:aa), flush the MAC address table for the switch when the loop-back test is finished.

Examples

The following command examples create an ingress UNI and NNI test profile:

```
-> loopback-test PE1-inward-UNI source-mac 00:00:00:dd:aa:01 destination-mac
00:00:00:cc:aa:bb vlan 1001 loopback-port 1/1 type inward

-> loopback-test PE2-inward-NNI source-mac 00:00:00:dd:aa:02 destination-mac
00:00:00:cc:aa:bc vlan 1001 loopback-port 2/1 type inward
```

The following command examples create an egress UNI and NNI test profile:

```
-> loopback-test PE2-outward-UNI source-mac 00:00:00:dd:ab:01 destination-mac
00:00:00:cc:ab:bb vlan 1001 loopback-port 1/1 type outward

-> loopback-test PE1-outward-NNI source-mac 00:00:00:cc:ab:bb destination-mac
00:00:00:dd:ab:01b vlan 1001 loopback-port 2/1 type outward
```

The following command examples enable and disable a loopback test profile:

```
-> loopback-test PE1-outward-UNI enable
-> loopback-test PE1-outward-UNI disable
```

Release History

Release 6.4.3; command was introduced.

Related Commands

ethernet-service sap-profile	Creates a profile for a VLAN Stacking Service Access Point (SAP).
show loopback-test	Displays the profile configuration for a loopback test profile.

MIB Objects

```
alaQoSHwLoopbackProfileTable
   alaQoSHwLoopbackProfileName
   alaQoSHwLoopbackSourceMac
   alaQoSHwLoopbackDestinationMac
   alaQoSHwLoopbackVlan
   alaQoSHwLoopbackPort
   alaQoSHwLoopbackType
   alaQoSHwLoopbackProfileStatus
   alaQoSHwLoopbackProfileRowStatus
```

show loopback-test

Displays the profile configuration for a hardware loopback test profile.

show loopback-test [*profile_name***]**

Syntax Definitions

profile_name	The name of an existing hardware loopback test profile.

Defaults

By default, all profiles are displayed if a profile name is not specified with this command.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

Use the *profile_name* parameter to display the loopback test configuration for a specific profile.

Examples

```
-> show loopback-test
Profile-Name     Src-Mac              Dest-Mac           Vlan   Port  Type   Status
-----------------|------------------|------------------|------|-----|------+------
pro1             00:d0:95:f3:63:58   00:00:00:00:00:0a   100    6/1   Inward Start
Total Entries = 1
```

output definitions

Profile Name	The name of the loopback test profile.
Src-Mac	The source MAC address of the test packet.
Dest-Mac	The destination MAC address of the test packet.
Vlan	The VLAN ID of the loopback port.
Port	The UNI or NNI loopback port.
Type	The type of loopback test; **Inward** (ingress) or **Outward** (egress).
Status	The status of the loopback test (**Enable**, **Disable**, or **Config**).

Release History

Release 6.4.3; command was introduced.

51 Ethernet OAM Commands

Service provider networks are large and complex with a wide user base, and they often involve different operators that must work together in order to provide end-to-end services to enterprise customers. Operations, Administration, and Maintenance (OAM) provides service assurance over a converged network that service providers are looking for in an Ethernet network. Ethernet OAM addresses areas such as availability, mean time to repair and more. Ethernet OAM focuses on two main areas that are most in need by service providers and are rapidly evolving in the standards bodies, Service OAM and Link OAM. These two OAM protocols have unique objectives but are complementary to each other. Service OAM provides monitoring and troubleshooting of end-to-end Ethernet service instances, while Link OAM allows a provider to monitor and troubleshoot an individual Ethernet link.

MIB information for the Ethernet OAM commands is as follows:

Filename: AlcatelIND1Eoam.MIB
Module: Alcatel-IND1-ETHERNET-OAM-MIB

Filename: IETF_802_1ag.MI
Module: IEEE8021-CFM-MIB

A summary of the available commands is listed here:

EthOAM vlan Configuration Commands	**ethoam vlan**
EthOAM Domain Configuration Commands	**ethoam domain** **ethoam domain mhf** **ethoam domain id-permission**
EthOAM Management Association Configuration Commands	**ethoam association** **ethoam association mhf** **ethoam association id-permission** **ethoam association ccm-interval** **ethoam association endpoint-list** **clear ethoam statistics**
EthOAM Default-Domain Configuration Commands	**ethoam default-domain level** **ethoam default-domain mhf** **ethoam default-domain id-permission** **ethoam default-domain primary-vlan**
EthOAM Management Point Configuration Commands	**ethoam endpoint** **ethoam endpoint admin-state** **ethoam endpoint rfp** **ethoam endpoint ccm** **ethoam endpoint priority** **ethoam endpoint lowest-priority-defect**
EthOAM Loopback and Linktrace Commands	**ethoam linktrace** **ethoam loopback**

EthOAM Timer Configuration Commands	**ethoam fault-alarm-time** **ethoam fault-reset-time**
EthOAM Performance Monitoring Configuration Commands	**ethoam one-way-delay** **ethoam two-way-delay** **clear ethoam**
EthOAM Show Commands	**show ethoam** **show ethoam domain** **show ethoam domain association** **show ethoam domain association end-point** **show ethoam default-domain configuration** **show ethoam default-domain** **show ethoam remote-endpoint domain** **show ethoam cfmstack** **show ethoam linktrace-reply** **show ethoam linktrace-tran-id** **show ethoam vlan** **show ethoam statistics** **show ethoam config-error** **show ethoam one-way-delay** **show ethoam two-way-delay**

ethoam vlan

Creates an association between Primary VID and Non-Primary VID(s).

ethoam vlan {*vlanid-list***} primary-vlan {***vlan-id***}**

no ethoam vlan {*vlanid-list***}**

Syntax Definitions

vlanid-list	VLAN Identifier List, for example: ’10 30-40’ or ‘10’
vlan-id	VLAN Identifier,for example: ‘20’

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Each VLAN ID specified must be created before creating any association.
- Each VLAN ID specified must be between 1 and 4094.
- Each VLAN ID specified must be static.
- A Non-Primary VID can only be associated with single Primary VID only.
- Once Primary VID is associated with Non-Primary VID, then it can not be configured as Non-Primary VID. Its association must be removed before it is configured as Non-Primary VID.
- This CLI shall trigger Automip for this VLAN, if either ‘mhf’ is enabled for MA or default-MD with primary VLAN same as the primary VLAN of this VLAN.
- If the VLAN is deleted using VLAN CLI (no vlan <vid>) and VLAN is non-primary, then the entry for this VLAN in the VLAN table will be deleted. This shall in turn delete all MEPs and MIPs associated with it. If the deleted VLAN is primary VLAN, then all its associated VLAN entries in the VLAN table shall be deleted. This shall in turn delete all MAs on this deleted VLAN.
- Use the **no** form of this command to dissociate Primary VID from the Non-Primary VID(s).

Examples

```
-> ethoam vlan 10 primary-vlan 20
-> ethoam vlan 11-15 primary-vlan 20
-> ethoam vlan 30 40-50 primary-vlan 20
-> no ethoam vlan 10
```

Release History

Release 6.4.3; command was introduced

Related Commands

show ethoam vlan	Displays the Ethernet OAM statistics of all the Management Domains configured on the bridge.

MIB Objects

dot1agCfmVlanTable
- dot1agCfmVlanComponentId
- dot1agCfmVlanVid
- dot1agCfmVlanPrimaryVid
- dot1agCfmVlanRowStatus

ethoam domain

Creates an Ethernet domain with a specific name.

ethoam domain *name* **format {none | dnsname | mac-address-uint | string}**
level *num*

no ethoam domain *name*

Syntax Definitions

name	Specifies the domain name used while creating the management domain for which this management association is created.
none	This format is supported for the inter-op with ITU-T Y.1731.
string	Character String.
mac-address-unit	MAC address + 2-octet (unsigned) integer.
dnsname	Domain Name like string, globally unique text string derived from a DNS name.
num	MD Level and it ranges from 0 to 7

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Maximum domain length is 43.
- Use format as ‘none’ for inter-op with ITU-T Y.1731.
- Domain name is unique in a system.
- Deletion of MD shall result in the deletion of all MAs, MEPs and MIPs configured in it.

Examples

```
-> ethoam domain MD format none level 3
-> ethoam domain MD1 format string level 4
```

Release History

Release 6.2.1; command was introduced.
Release 6.3.1; **carriercode**, **countrycode**, **vpnId** parameters deleted; **mac-address** parameter replaced with **mac-address-uint** parameter; **level** and *mac_address* parameters added.

Release 6.4.3 *domain_name* | *mac_address*, *level_num* parameters replaced with *name,num* parameters; **none** parameter added.

Related Commands

show ethoam	Displays the information of all the Management Domains (MD) configured on the bridge.
show ethoam domain	Displays the information of a specific Management Domain configured on the bridge.

MIB Objects

```
dot1agCfmMdTable
   dot1agCfmMdName
   dot1agCfmMdFromat
   dot1agCfmMdLevel
```

ethoam domain mhf

Configure the Message Handling Function (MHF) value for MD entry.

ethoam domain *name* **mhf {none** | **explicit** | **default}**

Syntax Definitions

name	Specifies the domain name used while creating the management domain for which this management association is created.
none	No MHFs can be created.
default	MHFs can be created.
explicit	MHFs can be created only if a MEP is created at some lower MD Level.

Defaults

parameter	default
none | explicit | default	**none**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Domain must be created before it is modified.

Examples

```
-> ethoam domain MD mhf default
```

Release History

Release 6.3.1; command was introduced.
Release 6.4.3 *domain_name* | *mac_address* parameters replaced with *name* parameters; **none** parameter added.

Related Commands

show ethoam	Displays the information of all the Management Domains (MD) configured on the bridge.

MIB Objects

```
dot1agCfmMdTable
   dot1agCfmMdName
   dot1agCfmMdMhfCreation
```

ethoam domain id-permission

Configures the ID-permission value for MD entry.

ethoam domain *name* **id-permission {none | chassisid}**

Syntax Definitions

name	Specifies the domain name used while creating the management domain for which this management association is created.
none	Sender ID TLV is not to be sent.
chassisid	Chassis ID Length, Chassis ID Subtype and Chassis ID TLV are to be present.System name shall be filled as Chassis ID.

Defaults

parameter	default
none | chassisid	**none**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Domain must be created before it is modified.

Examples

```
-> ethoam domain MD id-permission chassisid
```

Release History

Release 6.4.3; command was introduced.

Related Commands

show ethoam default-domain configuration	Displays the values of scalar Default-MD objects.
show ethoam domain	Displays the information of a specific Management Domain configured on the bridge.

MIB Objects

```
dot1agCfmMdTable
   dot1agCfmMdName
   dot1agCfmMdIdPermission
```

ethoam association

Creates Maintenance Association (MA) entry.

ethoam association *ma_name* **format {vpnid | unsignedint | string | primaryvid | icc-based} domain** *md_name* **primary-vlan** *vlan-id*

no ethoam association *ma_name* **domain** *md_name*

Syntax Definitions

ma_name	Association name for the created Ethernet OAM Association.
vpnid	As specified in RFC 2685 VPN ID.
unsignedint	2-octet unsigned integer.
string	Character String.
primaryvid	Primary VLAN ID (12 bits represented in a 2-octet integer).
icc-based	This format is supported for inter-op with ITU-T.
md_name	Specifies the domain name used while creating the management domain for which this management association is created.
vlan-id	Primary VLAN Identifier.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Maximum association name is name 44 minus the length of its domain name.
- Use format as ‘icc-based’ to inter-op with ITU-T Y.1731.
- Domain must be created before the creation of MA.
- VLAN must be created before the creation of MA.
- VLAN specified must be a primary VID.
- VLAN ID specified must be between 1 and 4094.
- Deletion of MA shall result in the deletion of MIPs and MEPs (on primary and non-primary VLAN) configured in it.

Examples

```
-> ethoam association MA format string domain MD primary-vlan 100
```

Release History

Release 6.2.1; command was introduced.
Release 6.3.1; **primaryVid** and *mac_address* parameters added;
Release 6.4.3; **icc-based** parameter added.

Related Commands

show ethoam domain association	Displays the information of a specified MA in a Management Domain configured on the bridge.

MIB Objects

```
dot1agCfmMaNetTable
   dot1agCfmMaNetFormat
   dot1agCfmMaNetName
   dot1agCfmMaNetRowStatus
dot1agCfmMaCompTable
   dot1agCfmMaComponentId
   dot1agCfmMaCompPrimaryVid
   dot1agCfmMaCompRowStatus
```

ethoam association mhf

Configures the MIP Half Function (MHF) value for MA Entry.

ethoam association *ma_name* **domain** *md_name* **mhf {none | default | explicit | defer}**

Syntax Definitions

ma_name	Association name for the created Ethernet OAM Association.
md_name	Specifies the domain name used while creating the management domain for which this management association is created.
none	No MHFs can be created.
default	MHFs can be created.
explicit	MHFs can be created only if a MEP is created at some lower MD Level.
defer	The creation of MHFs is determined by the corresponding MD object 'dot1agCfmMdMhfCreation'.

Defaults

parameter	default
none | explicit | default | defer	**defer**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- MA must be created before it is modified.
- On modification of 'mhf' for any MA, Automip shall also be invoked for all VLANS associated with this primary VID.

Examples

```
-> ethoam association MA domain MD mhf-creation defer
```

Release History

Release 6.2.1; command was introduced.
Release 6.3.1; *mac_address* parameter added.
Release 6.4.3; command was introduced.

Related Commands

show ethoam domain association	Displays the information of a specified MA in a Management Domain configured on the bridge.
show ethoam default-domain	Displays the information of the default MA.

MIB Objects

```
dot1agCfmMaNetTable
   dot1agCfmMaNetName
dot1agCfmMaCompTable
   dot1agCfmMaCompMhfCreation
```

ethoam association id-permission

Configure id-permission value for MA Entry.

ethoam association *ma_name* **domain** *md_namemd_name* **id-permission {none | chassisid | defer}**

Syntax Definitions

ma_namema_name	Association name for the created Ethernet OAM Association.
md_name	Specifies the domain name used while creating the management domain for which this management association is created.
none	Sender ID TLV is not to be sent.
chassisid	Chassis ID Length, Chassis ID Subtype and Chassis ID TLV are to be present.
defer	The contents of the Sender ID TLV are determined by the corresponding MD object ‘dot1agCfmMdIdPermission’.

Defaults

parameter	default
none |chassisid | defer	**defer**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

MA must be created before it is modified.

Examples

```
-> ethoam association MA domain MD id-permission defer
```

Release History

Release 6.4.3; command was introduced.

Related Commands

show ethoam domain association	Displays the information of a specified MA in a Management Domain configured on the bridge.
show ethoam domain	Displays the information of a specific Management Domain configured on the bridge.

MIB Objects

```
dot1agCfmMaNetTable
   dot1agCfmMaNetName
dot1agCfmMaCompTable
   dot1agCfmMaCompMIdPermission
```

ethoam association ccm-interval

Modifies the Continuity Check Message (CCM) transmission interval of an Ethernet OAM Maintenance Association.

ethoam association *association_name* **domain {***domain_name* | *mac_address***}**
ccm-interval {interval-invalid | interval100ms | interval1s | **interval10s** | **interval1m** | **interval10m}**

Syntax Definitions

ma_name	Name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.
md_name	Specifies the domain name. For more information on the different formats of the domain name, refer to **ethoam domain** command on page 51-5.
interval-invalid	Specifies that no CCMs are sent by a MEP
interval100ms	Specifies the CCMs are sent every 100 milli seconds.
interval1s	Specifies that CCMs are sent every 1 second.
interval10s	Specifies that CCMs are sent every 10 seconds.
interval1m	Specifies that CCMs are sent every minute.
interval10m	Specifies that CCMs are sent every 10 minutes.

Defaults

parameter	default
interval-invalid | **interval100ms** | **interval1s** | **interval10s** | **interval1m** | **interval10m**	**interval10s**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

The *ma_name* should be unique amid all those used by or available to the service provider within a domain.

Examples

```
-> ethoam association MA domain MD ccm-interval interval10s
```

Release History

Release 6.2.1; command was introduced.
Release 6.3.1; **intervalnone** parameter replaced with **interval-invalid** parameter; **interval1m**, **interval10m**, and *mac_address* parameters added; **interval60s** parameter deleted.
Release 6.4.4; **interval100ms** parameter added.

Related Commands

show ethoam domain	Displays the information of a specific Management Domain configured on the bridge.

MIB Objects

```
dot1agCfmMaNetTable
   dot1agCfmMaNetName
dot1agCfmMaCompTable
   dot1agCfmMaCompMIdPermission
```

ethoam association endpoint-list

Modifies the MEP list of an Ethernet OAM Maintenance Association.

ethoam association *ma_name* **domain {***md_name* | *mac_add***}**
endpoint-list *mep_id***[-***mep_id2***]**

no ethoam association *association_name* **domain {***domain_name* | *mac_add***}**
endpoint-list *mep_id***[-***mep_id2***]**

Syntax Definitions

ma_name	Name of the Ethernet OAM Association. Up to 48 (minus domain name length) characters may be used.
md_name	Specifies the domain name. For more information on the different formats of the domain name, refer to **ethoam domain** command on page 51-5
mac_add	Specifies the CFM system MAC address.
mep_id	Specifies the MEP number.
mep_id2	Last MEP number in a range of MEPs you want to configure.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove the MEP list.
- Note that only the MEP that is associated with the MEP list of the MA can be configured locally on the bridge or monitored remotely.
- The *ma_name* should be unique within a domain.

Examples

```
-> ethoam association MA domain MD endpoint-list 100-200
-> no ethoam association MA domain MD endpoint-list 100-200
```

Release History

Release 6.3.1; command was introduced.

Related Commands

show ethoam domain association	Displays the information of a specified MA in a Management Domain configured on the bridge.

MIB Objects

```
dot1agCfmMdTable
    dot1agCfmMdName
dot1agCfmMaNetTable
    dot1agCfmMaNetName
Dot1agCfmMaMepList
    dot1agCfmMaMepListIdentifier
    dot1agCfmMaMepListRowStatus
```

clear ethoam statistics

Clear statistics for all MEPs or for a particular MEP.

clear ethoam statistics [domain *domain* **association** *association* **endpoint** *mep-id***]**

Syntax Definitions

domain	Specifies the domain name used while creating the management domain for which this management association is created.
association	Association name for the created Ethernet OAM Association.
mep-id	MEP Identifier. Valid Range is 1-8191.

Defaults

None

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

None

Examples

```
-> clear ethoam statistics
-> clear ethoam statistics domain MD association MA endpoint 10
```

Release History

Release 6.4.3; command was introduced.

Related Commands

show ethoam statistics	Displays the Ethernet OAM of all the Management Domains configured on the bridge. Also, displays the statistics of all the MAs and matching MEPs for all the MDs.

MIB Objects

```
dot1agCfmMdTable
      dot1agCfmMdName
  dot1agCfmMaNetTable
      dot1agCfmMaNetName
  dot1agCfmMepTable
      dot1agCfmMepIdentifier
      alaCfmMepClearStats
  alaCfmGlobalClearStats
```

ethoam default-domain level

Configure the effective level of all default domain entries with the level value set to **no level**.

ethoam default-domain level {*num***}**

no ethoam default-domain

Syntax Definitions

num	The MD level whose value range from 0-7.

Defaults

Default value is 0.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- MD Level shall range from 0 to 7.

Examples

```
-> ethoam default-domain level 1
```

Release History

Release 6.4.3; command was introduced.

Related Commands

show ethoam default-domain configuration	Displays the values of scalar Default-MD objects.

MIB Objects

```
Dot1agCfmDefaultMdLevel
```

ethoam default-domain mhf

Configure the effective MHF value for all default domain entries with MHF value set to **defer**.

ethoam default-domain mhf {none | default | explicit}

no ethoam default-domain

Syntax Definitions

none	No MHFs can be created.
default	MHFs can be created.
explicit	MHFs can be created only if a MEP is created at some lower MD Level. Defaults

Defaults

Default value is none.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> ethoam default-domain mhf default
```

Release History

Release 6.4.3; command was introduced.

Related Commands

show ethoam default-domain configuration	Displays the values of scalar Default-MD objects.

MIB Objects

```
dot1agCfmDefaultMdDefMhfCreation
```

ethoam default-domain id-permission

Configures the effective ID permission value for all default domain entries with the ID permission value set to **defer**.

ethoam default-domain id-permission {none | chassisid}

no ethoam default-domain

Syntax Definitions

none	Sender ID TLV is not to be sent.
chassisid	Chassis ID Length, Chassis ID Subtype and Chassis ID TLV are to be present.

Defaults

Default value is none.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> ethoam default-domain id-permission chassisid
```

Release History

Release 6.4.3; command was introduced.

Related Commands

show ethoam default-domain configuration	Displays the default domain configuration.

MIB Objects

```
dot1agCfmDefaultMdDefIdPermission
```

ethoam default-domain primary-vlan

Configures the default domain settings for the specified primary VLAN.

ethoam default-domain primary-vlan {*vlan-id***} [level {no-level | *num*}] [mhf {none | default | explicit | defer}] [id-permission {none | chassisid | defer}]**

no ethoam default-domain

Syntax Definitions

vlan-id	VLAN Identifier.
no-level	MD level is inherited from the default domain level.
num	MD Level. Valid range is 0 to 7.
none	No MHFs can be created.
default	MHFs can be created.
explicit	MHFs can be created only if a MEP is created at some lower MD Level.
defer	MHF defers to the default domain MHF value.
none	Sender ID TLV is not to be sent.
chassisid	Chassis ID Length, Chassis ID Subtype and Chassis ID TLV are to be present.
defer	ID permission defers to the default domain ID permission value.

Defaults

parameter	default
no-level | *num*	**no-level**
none | **explicit** | **default** | **defer**	**defer**
none | **chassisid** | **defer**	**defer**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

On modification of MHF for any primary VID, Automip is invoked for all VLANS associated with this primary VID.

Examples

```
-> ethoam default-domain primary-vlan 10 id-permission chassid level 3 mhf default.
-> ethoam default-domain primary-vlan 10 id-permission chassid
-> ethoam default-domain primary-vlan 10 level 3
-> ethoam default-domain primary-vlan 10 mhf default
-> ethoam default-domain primary-vlan 10 level 3 mhf default
```

Release History

Release 6.4.3; command was introduced.

Related Commands

show ethoam default-domain	Displays the information of all the default MD.

MIB Objects

```
dot1agCfmDefaultMdTable
   dot1agCfmDefaultMdComponentId
   dot1agCfmDefaultMdPrimaryVid
   dot1agCfmDefaultMdLevel
```

ethoam endpoint

Creates a Maintenance End Point (MEP) and virtual MEP.

ethoam endpoint *mep-id* **domain** *md_name* **association** *ma_name* **direction { up | down } {port {***slot/port* **| virtual | linkagg** *agg_id***} [primary-vlan** *vlan_id***]**

no ethoam endpoint *mep-id* domain *md_name* association *ma_name*

Syntax Definitions

mep_id	Specifies the Maintenance Association End Point. The valid range is 1–8191.
md_name	Specifies the domain name used while creating the management domain for which this management association is created.
ma_name	Association name for the created Ethernet OAM Association.
up	For UP MEP.
down	For DOWN MEP.
slot/port	Physical slot and port number on which MEP needs to be created.
virtual	Keyword for creating virtual MEP.
agg_id	Linkagg Identifier on which MEP needs to be created.
vlan_id	VLAN identifier.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete a maintenance endpoint.
- The *mep_id* must be unique amid all those used by or available to the service provider in the specified MA.
- The direction for virtual MEP must always be up.
- For creating a virtual MEP the value of port must be given the keyword “virtual”.

Examples

```
-> ethoam endpoint 10 domain MD association MA direction up port 1/1
-> ethoam endpoint 10 domain MD association MA direction down linkagg 1
-> ethoam endpoint 10 domain MD association MA direction down linkagg 1 vlan 10
-> ethoam endpoint 1 domain md1 association ma1 direction up port virtual primary-
vlan 100
-> no ethoam endpoint 10 domain MD association MA
```

Release History

Release 6.4.3; command was introduced.
Release 6.4.4; **virtual** parameter added.

Related Commands

show ethoam domain association end-point	Displays the information of a specific MEP in a Management Domain configured on the bridge.

MIB Objects

```
dot1agCfmMdTable
   dot1agCfmMdName
dot1agCfmMaNetTable
   dot1agCfmMaNetName
dot1a gCfmMepTable
   dot1agCfmMepIdentifier
   dot1agCfmMepDirection
   dot1agCfmMepIfIndex
   dot1agCfmMepPrimaryVid
```

ethoam endpoint admin-state

Configures the administrative state of MEP.

ethoam endpoint *mep_id* **domain {***md_name* | *mac_address***} association** *ma_name* **admin-state {enable | disable}**

Syntax Definitions

mep_id	Specifies the Maintenance Association End Point. The valid range is 1–8191.
md_name	Specifies the domain name used while creating the management domain for which this management association is created.
mac_address	Specifies the CFM system MAC address.
association_name	Association name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.
enable	Administratively enables MEP.
disable	Administratively disables MEP.

Defaults

The default value is disable.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

The *mep_id* specified must already exist in the switch configuration.

Examples

```
-> ethoam endpoint 100 domain MD association MA admin-state enable
```

Release History

Release 6.2.1; command was introduced.
Release 6.3.1; *mac_address* parameter added.

Related Commands

show ethoam domain association end-point	Displays the information of a specific MEP in a Management Domain configured on the bridge.

MIB Objects

```
Dot1agCfmMep
   dot1agCfmMepIndex
   dot1agCfmMepIdentifier
   dot1agCfmMepDirection
   dot1agCfmMepPortNumber
   dot1agCfmMepMacAddress
   dot1agCfmMepAdminStatus
   dot1agCfmMepFngState
   dot1agCfmMepCcmEnabled
   dot1agCfmMepCcmTransmitting
   dot1agCfmMepCcmLtmPriority
   dot1agCfmMepCcmNotReceived
   dot1agCfmMepCcmStreamError
   dot1agCfmMepCcmStreamOther
   dot1agCfmMepRdiReceived
   dot1agCfmMepLastCcmMaFault
   dot1agCfmMepLastCcmCrossConnFault
   dot1agCfmMepCcmOut
   dot1agCfmMepLbmNextSeqNumber
   dot1agCfmMepLbrIn
   dot1agCfmMepLbrInOutOfOrder
   dot1agCfmMepLbrOut
   dot1agCfmMepLtmNextSeqNumber
   dot1agCfmMepLtmIn
   dot1agCfmMepLtrOut
   dot1agCfmMepDefectsPresent
   dot1agCfmMepDefectsAbsent
   dot1agCfmMepRowStatus
```

ethoam endpoint rfp

Enables or disables the Remote Fault Propagation (RFP) on MEP.

ethoam endpoint *mep_id* **domain {***md_name* | *mac_address***} association** *ma_name* **rfp {enable | disable}**

Syntax Definitions

mep_id	Specifies the Maintenance Association End Point. The valid range is 1–8191.
md_name	Specifies the domain name used while creating the management domain for which this management association is created.
mac_address	Specifies the CFM system MAC address.
ma_name	Association name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.
enable	Administratively enables RFP on MEP.
disable	Administratively disables RFP on MEP.

Defaults

The default value of RFP is disable.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The *mep_id* specified must already exist in the switch configuration.
- The domain and association must be created before RFP can be enabled.
- The MEP must be an UP MEP. If down MEP is specified, CLI returns with an error.
- The admin state of the MEP must be enabled in order to report faults.
- RFP cannot be enabled on virtual UP MEP since it is not associated with a physical interface.
- It is recommended that if RFP is enabled on a port, then any other violation feature (Link Monitoring or Link Fault Propagation) should not be configured.
- It is recommended that if RFP is enabled on a port, then automatic recovery is disabled for that port.
- If Link Monitoring is configured on a RFP enabled port, then the wait-to-restore timer must be less than the CCM interval.

Examples

```
-> ethoam endpoint 1 domain md1 association ma1 rfp enable
```

Release History

Release 6.4.4; command was introduced.

Related Commands

show ethoam domain association end-point	Displays the information of a specific MEP in a Management Domain configured on the bridge.

MIB Objects

```
Dot1agCfmMDTable
   dot1agCfmMdName
dot1agCfmMaNetTable
   dot1agCfmMaNetName
dot1agCfmMepTable
   dot1agCfmMepIdentifier
   dot1agCfmRfpEnabled
```

ethoam endpoint ccm

Configures the MEP to generate Continuity Check Messages (CCM).

ethoam endpoint *mep_id* **domain {***md_name* | *mac_address***} association** *ma_name*
ccm {enable | disable}

Syntax Definitions

mep_id	Specifies the Maintenance Association End Point. The valid range is 1–8191.
md_name	Specifies the domain name. For more information on the different formats of the domain name, refer to **ethoam domain**.
mac_address	Specifies the CFM system MAC address.
ma_name	Name of the Ethernet OAM association. Up to 48 (minus the domain name length) characters may be used.
enable	Enables MEP to generate CCMs.
disable	Disables MEP to generate CCMs.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

The *mep_id* should be unique amid all those used by or available to the service provider in the specified MA.

Examples

```
-> ethoam endpoint 100 domain MD association MA ccm enable
```

Release History

Release 6.2.1; command was introduced.
Release 6.3.1; *mac_address* parameter added.

Related Commands

show ethoam domain association end-point	Displays the information of a specific MEP in a Management Domain configured on the bridge.

MIB Objects

```
Dot1agCfmMep
   dot1agCfmMepIndex
   dot1agCfmMepIdentifier
   dot1agCfmMepDirection
   dot1agCfmMepPortNumber
   dot1agCfmMepMacAddress
   dot1agCfmMepAdminStatus
   dot1agCfmMepFngState
   dot1agCfmMepCcmEnabled
   dot1agCfmMepCcmTransmitting
   dot1agCfmMepCcmLtmPriority
   dot1agCfmMepCcmNotReceived
   dot1agCfmMepCcmStreamError
   dot1agCfmMepCcmStreamOther
   dot1agCfmMepRdiReceived
   dot1agCfmMepLastCcmMaFault
   dot1agCfmMepLastCcmCrossConnFault
   dot1agCfmMepCcmOut
   dot1agCfmMepLbmNextSeqNumber
   dot1agCfmMepLbrIn
   dot1agCfmMepLbrInOutOfOrder
   dot1agCfmMepLbrOut
   dot1agCfmMepLtmNextSeqNumber
   dot1agCfmMepLtmIn
   dot1agCfmMepLtrOut
   dot1agCfmMepDefectsPresent
   dot1agCfmMepDefectsAbsent
   dot1agCfmMepRowStatus
```

ethoam endpoint priority

Configures the priority values for CCMs and Linktrace Messages (LTMs) transmitted by a MEP.

ethoam endpoint *mep_id* **domain {***md_name* | *mac_address***} association** *ma_name* **priority** *ccm_ltm_priority*

Syntax Definitions

mep_id	Specifies the Maintenance Association End Point. The valid range is 1–8191.
md_name	Specifies the domain name. For more information on the different formats of the domain name, refer to **ethoam domain** command on page 51-5.
mac_address	Specifies the CFM system MAC address.
ma_name	Name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.
ccm_ltm_priority	Priority value for CCMs and LTMs transmitted by the MEP. The valid range is 0–7.

Defaults

parameter	default
ccm_ltm_priority	7

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

The *mep_id* should be unique amid all those used by or available to the service provider in the specified MA.

Examples

```
-> ethoam endpoint 100 domain MD association MA priority 6
```

Release History

Release 6.2.1; command was introduced.
Release 6.3.1; *mac_address* parameter added.

Related Commands

show ethoam domain association end-point	Displays the information of a specific MEP in a Management Domain configured on the bridge.

MIB Objects

```
Dot1agCfmMep
   dot1agCfmMepIndex
   dot1agCfmMepIdentifier
   dot1agCfmMepDirection
   dot1agCfmMepPortNumber
   dot1agCfmMepMacAddress
   dot1agCfmMepAdminStatus
   dot1agCfmMepFngState
   dot1agCfmMepCcmEnabled
   dot1agCfmMepCcmTransmitting
   dot1agCfmMepCcmLtmPriority
   dot1agCfmMepCcmNotReceived
   dot1agCfmMepCcmStreamError
   dot1agCfmMepCcmStreamOther
   dot1agCfmMepRdiReceived
   dot1agCfmMepLastCcmMaFault
   dot1agCfmMepLastCcmCrossConnFault
   dot1agCfmMepCcmOut
   dot1agCfmMepLbmNextSeqNumber
   dot1agCfmMepLbrIn
   dot1agCfmMepLbrInOutOfOrder
   dot1agCfmMepLbrOut
   dot1agCfmMepLtmNextSeqNumber
   dot1agCfmMepLtmIn
   dot1agCfmMepLtrOut
   dot1agCfmMepDefectsPresent
   dot1agCfmMepDefectsAbsent
   dot1agCfmMepRowStatus
```

ethoam endpoint lowest-priority-defect

Configures the lowest priority fault alarm for the lowest priority defect for a MEP.

ethoam endpoint *mep_id* **domain {***md_name* | *mac_address***} association** *ma_name* **lowest-priority-defect** *lowest_priority_defect*

Syntax Definitions

mep_id	Specifies the Maintenance Association End Point. The valid range is 1–8191.
md_name	Specifies the domain name. For more information on the different formats of the domain name, refer to **ethoam domain** command on page 51-5.
mac_address	Specifies the CFM system MAC address.
ma_name	Name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.
lowest_priority_defect	The lowest priority defect that can generate a Fault alarm. Possible values are **xcon**, **rem-err-xcon**, **no-defect**, **mac-rem-err-xcon**, **err-xcon**, and **all-defect**.

Defaults

parameter	default
lowest_priority_defect	mac-rem-err-xcon

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

The *mep_id* should be unique amid all those used by or available to the service provider in the specified MA.

Examples

```
-> ethoam endpoint 100 domain esd.alcatel-lucent.com association alcatel-sales
lowest-priority-defect all-defect
```

Release History

Release 6.3.1; command was introduced.

Related Commands

show ethoam domain association end-point	Displays the information of a specific MEP in a Management Domain configured on the bridge.

MIB Objects

```
Dot1agCfmMep
   dot1agCfmMepIndex
   dot1agCfmMepIdentifier
   dot1agCfmMepDirection
   dot1agCfmMepPortNumber
   dot1agCfmMepMacAddress
   dot1agCfmMepAdminStatus
   dot1agCfmMepFngState
   dot1agCfmMepCcmEnabled
   dot1agCfmMepCcmTransmitting
   dot1agCfmMepCcmLtmPriority
   dot1agCfmMepCcmNotReceived
   dot1agCfmMepCcmStreamError
   dot1agCfmMepCcmStreamOther
   dot1agCfmMepRdiReceived
   dot1agCfmMepLastCcmMaFault
   dot1agCfmMepLastCcmCrossConnFault
   dot1agCfmMepCcmOut
   dot1agCfmMepLbmNextSeqNumber
   dot1agCfmMepLbrIn
   dot1agCfmMepLbrInOutOfOrder
   dot1agCfmMepLbrOut
   dot1agCfmMepLtmNextSeqNumber
   dot1agCfmMepLtmIn
   dot1agCfmMepLtrOut
   dot1agCfmMepDefectsPresent
   dot1agCfmMepDefectsAbsent
   dot1agCfmMepRowStatus
```

ethoam linktrace

Enables the maintenance entity to initiate transmitting Link Trace Messages (LTM).

ethoam linktrace {target-macaddress *mac_address* **| target-endpoint** *t-mepid***} source-endpoint** *s-mepid* **domain {***d-name* | *mac_add***} association** *a-name* **[flag [fdb-mpdb | fdbonly]] [hop-count** *hop_count***]**

Syntax Definitions

mac_add	Target MAC address to be transmitted.
t-mepid	Specifies the MEP for which the Loopback message is targeted.
s-mepid	Specifies the MEP that transmits the Loopback message. The valid range is 1–8191.
d-name	Specifies the domain name. For more information on the different formats of the domain name, refer to **ethoam domain**.
domain *mac_address*	Specifies the CFM system MAC address.
a-name	Name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.
fdbonly	Specifies that only the MAC addresses learned in a bridge's active data forwarding table will be used to decide the egress port.
hop_count	Indicates the number of hops remaining in this LTM. Each bridge that handles the LTM decreases the value by 1. This decreased value is returned to the LTM. The valid range is 1–2^32.

Defaults

parameter	default
flag	**fdbonly**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- This command allows an operator to generate a LTM for the specified MEP.
- This command signals the MEP that it should transmit a Linktrace message and detect the presence or lack of the corresponding Linktrace messages.

Examples

```
-> ethoam linktrace target-macaddress 10:aa:ac:12:12:ad source 4 domain MD
association flag fdbonly hop-count 32
Transaction Id: 6943

-> ethoam linktrace target-endpoint 15 source 4 domain MD association
Transaction Id: 6934
```

Release History

Release 6.2.1; command was introduced.
Release 6.3.1; **target-macaddress**, **target-endpoint**, **source-endpoint,** and **domain** *mac_address* parameters added; **end-point** parameter deleted.

Related Commands

show ethoam domain	Displays the information of a specified Management Domain configured on the bridge.

MIB Objects

```
Dot1agCfmMep
   dot1agCfmMepIdentifier
   dot1agCfmMepTransmitLtmFlags
   dot1agCfmMepTransmitLtmTargetMacAddress
   dot1agCfmMepTransmitLtmTargetMepId
   dot1agCfmMepTransmitLtmTargetlsMepId
   dot1agCfmMepTransmitLtmTtl
   dot1agCfmMepTransmitLtmResult
   dot1agCfmMepTransmitEgressIdentifier
```

ethoam loopback

Initiates the transmission of loopback messages from the specified source MEP to the specified target MEP or MAC address. Also triggers the source MEP to detect the presence or lack of a corresponding loopback reply from the target.

ethoam loopback {target-endpoint *t-mepid* **| target-macaddress** *mac_add***} source-endpoint** *s-mepid* **domain** *d-name* **association** *a-name* **[number** *num***] [data** *string***] [vlan-priority** *vlan-priority***] [drop-eligible { true | false }]**

Syntax Definitions

t-mepid	Specifies the MEP for which the Loopback message is targeted. The valid range is 1-8191.
mac_add	Target MAC address to be transmitted.
s-mepid	Specifies the MEP that transmits the Loopback message. The valid range is 1–8191.
d-name	Specifies the domain name. For more information on the different formats of the domain name, refer to **ethoam domain**.
a-name	Name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.
num	Number of loopback messages. Valid range is 1-10.
string	Specifies the amount of data to be included in the Data Type Length Value (TLV), if the Data TLV is selected to be sent. The valid range is 1–255.
vlan-priority	VLAN Priority. Valid Range is 0-7.
true	Sets the drop eligibility bit in the VLAN tag to true.
false	Sets the drop eligibility bit in the VLAN tag to false.

Defaults

parameter	default
num	1
vlan-priority	CCM priority
drop-eligible {true | false}	**true**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Source and target MEP-ID, MD and MA must already exist before loopback is initiated.
- If data TLV is not set, then it is not sent in the loopback message.

Examples

```
-> ethoam loopback target-endpoint 10 source-endpoint 20 domain MD association MA
number 3
Reply from 00:0E:B1:6B:43:89: bytes=64 seq=0 time=100ms
Reply form 00:0E:B1:6B:43:89: bytes=64 seq=0 time=112ms
Request timed out.
----00:E0:B1:6B:43:89 ETH-LB Statistics----
3 packets transmitted, 2 packets received, 33% packet loss
round-trip (ms)  min/avg/max = 100/106/112
```

Release History

Release 6.2.1; command was introduced.
Release 6.3.1; **target-macaddress**, **target-endpoint**, **source-endpoint**, and **domain** *mac_address* parameters added; **end-point** parameter deleted.

Related Commands

show ethoam domain	Displays the information of a specified Management Domain configured on the bridge.

MIB Objects

```
dot1agCfmMdTable
   dot1agCfmMdName
dot1agCfmMaNetTable
   dot1agCfmMaNetName
dot1agCfmMepTable
   dot1agCfmMepIdentifier
   dot1agCfmMepTransmitLbmDestMacAddress
   dot1agCfmMepTransmitLbmDestMepId
   dot1agCfmMepTransmitLbmDestIsMepId
   dot1agCfmMepTransmitLbmMessages
   dot1agCfmMepTransmitLbmDataTlv
   dot1agCfmMepTransmitLbmVlanPriority
   dot1agCfmMepTransmitLbmVlanDropEnable
   dot1agCfmMepTransmitLbmStatus
```

ethoam fault-alarm-time

Configures the timeout value for the Fault Notification Generation Alarm time that specifies the time interval during which one or more defects should be detected before the fault alarm is issued.

ethoam fault-alarm-time *centiseconds* **endpoint** *endpoint_id* **domain {***md_name* | *mac_address***} association** *ma_name*

no ethoam fault-alarm-time endpoint *endpoint_id* **domain {***md_name* | *mac_address***} association** *ma_name*

Syntax Definitions

centiseconds	The Fault Notification Generation Alarm timeout value, in centi seconds. The valid range is 250–1000.
endpoint_id	Specifies the MEP of a specific MA. The valid range is 1–8191.
md_name	Specifies the domain name. For more information on the different formats of the domain name, refer to **ethoam domain** command on page 51-5.
ma_name	Name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.

Defaults

parameter	default
centiseconds	250

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to restore the Fault Notification Generation Alarm timeout value to the default value.
- The Fault Notification Generation Alarm timeout value is configurable per MEP.

Examples

```
-> ethoam fault-alarm-time 500 endpoint 100 domain esd.alcatel-lucent.com associa-
tion alcatel_sales
-> no ethoam fault-alarm-time endpoint 100 domain esd.alcatel-lucent.com associa-
tion alcatel_sales
```

Release History

Release 6.3.1; command was introduced.

Related Commands

show ethoam domain association end-point	Displays the information of a specific MEP in a Management Domain configured on the bridge.

MIB Objects

```
Dot1agCfmMep
   dot1agCfmMepFngAlarmTime
```

ethoam fault-reset-time

Configures the timer value for the Fault Notification Generation Reset time that specifies the time interval during which the fault alarm is re-enabled to process faults. The fault alarm will only be re-enabled if no new faults are received during this time interval.

ethoam fault-reset-time *centiseconds* **endpoint** *endpoint_id* **domain {***mac_add* | *d-name***} association** *a-name*

no ethoam fault-reset-time endpoint *endpoint_id* **domain {***mac_add* | *d-name***} association** *a-name*

Syntax Definitions

centiseconds	The Fault Notification Generation Reset timer value, in centi seconds. The valid range is 250–1000.
mep-id	Specifies the MEP of a specific MA. The valid range is 1–8191.
d-name	Specifies the domain name. For more information on the different formats of the domain name, refer to **ethoam vlan** command on page 51-3.
a-name	Name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.

Defaults

parameter	default
centiseconds	1000

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to restore the Fault Notification Generation Reset timeout value to the default value.
- The Fault Notification Generation Reset timer value is configurable per MEP.

Examples

```
-> ethoam fault-reset-time 250 end-point 100 domain esd.alcatel-lucent.com associa-
tion alcatel_sales
-> no ethoam fault-reset-time end-point 100 domain esd.alcatel-lucent.com associa-
tion alcatel_sales
```

Release History

Release 6.3.1; command was introduced.

Related Commands

ethoam fault-alarm-time	Configures the timeout value for the Fault Notification Generation Alarm time.
show ethoam domain association end-point	Displays the information of a specific MEP in a Management Domain configured on the bridge.

MIB Objects

```
Dot1agCfmMep
   dot1agCfmMepFngResetTime
```

ethoam one-way-delay

Initiates a one-way-delay measurement (1DM) to determine the one-way frame delay (latency) and delay variation (jitter) between two MEPs.

ethoam one-way-delay {target-endpoint *t-mepid* **| target-macaddress** *mac_add***} source-endpoint** *s-mepid* **domain** *domain* **association** *association* **[vlan- priority** *vlan-priority***]**

Syntax Definitions

t-mepid	Target MEP-ID. Valid Range 1-8191.
mac_add	Target MAC-Address.
s-mepid	Source MEP-ID. Vaild Range 1-8191.
domain	The maintenance domain name.
association	The maintenance association name.
vlan-priority	VLAN Priority. Valid Range is 0-7.

Defaults

parameter	default
vlan-priority	7

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Source MEP-ID, MD and MA must be created before initiating 1DM.
- When **target-endpoint** is specified then entry must be present in the RMEP table, no matter if its status is RMEP_OK or RMEP_FAILED, before initiating 1DM. So target-macaddress can be used to bypass such a restriction.
- Although the OmniSwitch implementation of Ethernet frame delay measurement (ETH-DM) is compliant with ITU-T Y.1731, delay measurement can be performed for both ITU-T Y.1731 and IEEE 802.1ag MEPs.
- If the 1DM is initiated with a **target-macaddress** and an egress port is found for this MAC address, then the 1DM frames are transmitted from that port. Otherwise, 1DM frames are flooded in the MEP's VLAN.
- One-way delay measurement requires NTP clock synchronization between the sending and receiving MEPs.

Examples

```
-> ethoam one-way-delay target-endpoint 10 source-endpoint 12 domain MD
association MA vlan-priority 4

-> ethoam one-way-dealy target-macaddress 00:e0:b1:6a:52:4c source-endpoint 12
domain MD association MA vlan-priority 4
```

Release History

Release 6.4.3; command was introduced

Related Commands

show ethoam one-way-delay	Displays the one-way-delay and jitter parameters for all entries or for the MAC address of a specific MEP.

MIB Objects

```
dot1agCfmMdTable
    dot1agCfmMdName
dot1agCfmMaNetTable
    dot1agCfmMaNetName
dot1agCfmMepTable
    dot1agCfmMepIdentifier
alaCfmMepTable
    alaCfmMepOWDTMacAddress
    alaCfmMepOWDTMepIdentifier
    alaCfmMepOWDTPriority
```

ethoam two-way-delay

Initiate a two-way-delay measurement to determine the round-trip latency and jitter between two MEPs. The initiating MEP sends delay measurement message (DMM) frames to the receiving MEP. The receiving MEP responds with delay measurement reply (DMR) frames.

ethoam two-way-delay {target-endpoint *t-mepid* **| target-macaddress** *mac_add***} source-endpoint** *s-mepid* **domain** *domain* **association** *association* **[vlan- priority** *vlan-priority***]**

Syntax Definitions

t-mepid	Target MEP-ID. Valid Range 1-8191.
mac_add	Target MAC-Address.
s-mepid	Source MEP-ID. Vaild Range 1-8191.
domain	The maintenance domain name.
association	The maintenance association name.
vlan-priority	VLAN Priority. Valid Range is 0-7.

Defaults

parameter	default
vlan-priority	7

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Source MEP-ID, MD and MA must be created before initiating a two-way delay measurement.
- When **target-endpoint** is specified then entry must be present in the RMEP table, no matter if the status is RMEP_OK or RMEP_FAILED, before initiating two-way-delay. So **target-macaddress** can be used to bypass such a restriction.
- The CLI console will pause until all DMRs are received or maximum of 3 seconds to ensure that all the DMRs have been returned. If the operation fails, then the appropriate message is displayed. If the operation is successful, no message is displayed.
- If the DMM is initiated by UP MEP with a **target-macaddress** and the egress port is found for this MAC address, then DMM frames are transmitted from that port. Otherwise, DMM frames are flooded in the MEP's VLAN.
- Two-way delay measurement does *not* require NTP clock synchronization on the sending and receiving MEPs.

- Although the OmniSwitch implementation of Ethernet frame delay measurement (ETH-DM) is compliant with ITU-T Y.1731, delay measurement can be performed for both ITU-T Y.1731 and IEEE 802.1ag MEPs.
- This command initiates an on-demand OAM performance measurement. To set up continuous two-way delay measurement, see the “Service Assurance Agent Commands” chapter for information about how to configure a SAA for continuous two-way frame delay measurement.

Examples

```
-> ethoam two-way-delay target-endpoint 10 source-endpoint 12 domain MD
association MA vlan-priority 4
Reply from 00:0E:B1:6B:43:89 delay=2584us jitter=282us
-> ethoam two-way-delay target-macaddress 00:e0:b1:6a:52:4c source-endpoint 12
domain MD association MA vlan-priority 4
Reply form 00:E0:B1:6A:52:4C: delay=2584us jitter=282us
```

Release History

Release 6.4.3; command was introduced

Related Commands

show ethoam two-way-delay	Displays the two-way-delay delay and jitter parameters for all entries or for the MAC address of a specific MEP.

MIB Objects

```
dot1agCfmMdTable
    dot1agCfmMdName
dot1agCfmMaNetTable
    dot1agCfmMaNetName
dot1agCfmMepTable
    dot1agCfmMepIdentifier
alaCfmMepTable
    alaCfmMepTWDTMacAddress
    alaCfmMepTWDTMepIdentifier
    alaCfmMepTWDTPriority
```

clear ethoam

Delete all the one-way-delay or two-way-delay entries

clear ethoam {one-way-delay-table | two-way-delay-table}

Syntax Definitions

None

Defaults

None

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

None

Examples

```
-> clear ethoam one-way-delay-table
-> clear ethoam two-way-delay-table
```

Release History

Release 6.4.3; command was introduced

Related Commands

ethoam one-way-delay	Initiates the two one-way-delay messages from a particular MEP to an RMEP.

MIB Objects

```
alaCfmGlobalOWDClear
   alaCfmGlobalTWDClear
```

show ethoam

Displays the information of all the Management Domains (MD) configured on the bridge.

show ethoam

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

This command displays all the MAs for all the MDs.

Examples

```
-> show ethoam
System Configuration
  Ethernet OAM system mac address: 00:D0:95:EC:84:B0,
  Number of Maintenance Domains: 1
    Maintenance Domain: esd.alcatel-lucent.com
        Maintenance Association: alcatel-sales
```

output definitions

Ethernet OAM system mac address	The MAC address of the Ethernet OAM system.
Number of Maintenance Domains	The number of maintenance domains configured on the bridge.
Maintenance Domain	The name of the maintenance domain.
Maintenance Association	The name of the maintenance association.

Release History

Release 6.2.1; command was introduced.

Related Commands

ethoam domain	Creates an Ethernet domain with a specific name.

MIB Objects

```
Dot1agCfmMd
   dot1agCfmMdName
Dot1agCfmMa
   dot1agCfmMaName
```

show ethoam domain

Displays the information of a specific Management Domain configured on the bridge.

show ethoam domain *md_name*

Syntax Definitions

md_name	Specifies the domain name used while creating the management domain for which this management association is created.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show ethoam domain MD
Total number of MAs configured in this MD = 1
MD Attributes
  MD-Format : string,
  MD-Level : level-3,
  MD-MHFstatus : mhfNone,
  MD-IdPermission : sendIdNone
    Maintenance Association : MA
      MA-Format : string,
      Primary Vlan : 199,
      Associated Vlan-list : none,
      Total Number of Vlans : 1,
      MA-MHFstatus : mhfNone,
      MA-IdPermission : sendIdNone,
      CCM-interval : interval10s,
      MEP-List(MEP-Id) : 10
```

output definitions

MD-level	The level at which the MD was created.
MD-MHFstatus	Indicates whether the maintenance entity can create MHFs for this MD. Options include **none, explicit,** or **default**.
Maintenance Association	The name of the maintenance association.
Vlan	The VLAN ID monitored by this MA. If the MA is not attached to any VLAN, 0 will be displayed.

output definitions (continued)

MA-MHFstatus	Indicates whether the maintenance entity can create MHFs for this MA. Options include **none, explicit,** or **default**.
CCM-interval	The interval between the CCM transmissions.
MEP-Id	Indicates the Maintenance End Point.

Release History

Release 6.2.1; command was introduced.
Release 6.4.3; *mac_address* parameter deleted.

Related Commands

show ethoam	Displays the information of all the Management Domains (MD) configured on the bridge.
ethoam domain	Creates an Ethernet domain with a specific name.

MIB Objects

```
Dot1agCfmMd
   dot1agCfmMdLevel
   dot1agCfmMdMhfCreation
Dot1agCfmMa
   dot1agCfmMaName
   dot1agCfmMaVid
   dot1agCfmMaMhfCreation
   dot1agCfmMaCcmInterval
Dot1agCfmMep
   dot1agCfmMepIdentifier
```

show ethoam domain association

Displays the information of a specific MA in a Management Domain configured on the bridge.

show ethoam domain *md_name* **association** *ma_name*

Syntax Definitions

md_name	Specifies the domain name.
ma_name	Name of the Ethernet OAM Association.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show ethoam domain MD association MA
Total number of MEPs configured in this MA = 1
MA-Format : string,
Primary Vlan : 100,
Associated Vlan-list : none,
Total Number of Vlans : 1,
MA-MHFstatus : mhfDefer,
MA-IdPermission : sendIdDefer,
CCM-interval : interval10s,
MEP-List(MEP-Id) : 1-5,

Legend: MEP-Id: * = Inactive Endpoint


MEP-ID   Admin State Direction   Mac-Address         Port      Primary Vlan
--------+-----------+----------+-------------------+----------+----------------
      1      disable      up    00:E0:B1:A0:78:A3     virtual    100
```

output definitions

Primary Vlan	The VLAN ID monitored by this MA. If the MA is not attached to any VLAN, 0 will be displayed.
MA-MHFstatus	Indicates whether the maintenance entity can create MHFs for this MA. Options include **none, explicit,** or **default**.
CCM-interval	The interval between the CCM transmissions.
MEP-ID	Indicates the Maintenance End Point.

output definitions (continued)

Admin State	Indicates the administrative state (**up** or **down)** of the MEP.
Direction	The direction of the MEP.
MAC Address	The MAC address of the MEP.
Port	The slot/port number of the Bridge port to which the MEP is attached.

Release History

Release 6.2.1; command was introduced.
Release 6.3.4; *mac_address* parameter deleted.

Related Commands

ethoam association	Creates an Ethernet OAM Maintenance Association in the specified domain.

MIB Objects

```
Dot1agCfmMa
   dot1agCfmMaVid
   dot1agCfmMaMhfCreation
   dot1agCfmMaCcmInterval
Dot1agCfmMep
   dot1agCfmMepIdentifier
   dot1agCfmMepActive
   dot1agCfmMepDirection
   dot1agCfmMepIfIndex
   dot1agCfmMepMacAddress
```

show ethoam domain association end-point

Displays the information of a specific MEP in a Management Domain configured on the bridge.

show ethoam domain *md_name* **association** *ma_name* **end-point** *mep-id*

Syntax Definitions

md_name	Specifies the domain name.
ma_name	Name of the Ethernet OAM Association.
mep-id	Specifies the MEP of a specific MA. The valid range is 1–8191.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show ethoam domain MD association MA endpoint 10
Admin State : disable,
Direction : up,
Slot/Port: virtual,
MacAddress: 00:E0:B1:A0:78:A3,
Fault Notification : FNG_RESET,
CCM Enabled : disabled,
RFP Status : enabled,
CCM Linktrace Priority : 7,
CCM Not Received : false,
CCM Error defect : false,
CCM Xcon defect : false,
MEP RDI defect : false,
MEP Last CCM Fault : not specified,
MEP Xcon Last CCM Fault : not specified,
MEP Error Mac Status : false,
MEP Lbm NextSeqNumber : 0,
MEP Ltm NextSeqNumber : 32157,
Fault Alarm Time : 250,
Fault Reset Time : 1000,
Lowest PrDefect Allowed : DEF_MAC_REM_ERR_XCON,
Highest PrDefect Present : DEF_NONE
```

output definitions

Admin State	Indicates the administrative state **(up** or **down**) of the MEP.
Direction	The direction of the MEP.
Slot/Port	The slot/port number of the Bridge port to which the MEP is attached.If the value is virtual, it indicates a virtual port.
MAC Address	The MAC address of the MEP.
Fault Notification	Indicates the current state of the MEP Fault Notification Generator State Machine, which can be **FNG_RESET**, **FNG_DEFECT**, **FNG_REPORT_DEFECT**, **FNG_DEFECT_REPORTED**, or **FNG_DEFECT_CLEARING**.
RFP Status	Indicates the status of the RFP.
CCM Enabled	Indicates whether the MEP generates CCMs (**enabled**) or not (**disabled**).
CCM Linktrace Priority	Indicates the priority value for CCMs and LTMs transmitted by the MEP.
CCM Not Received	Indicates if CCMs are not being received (**true**) or received (**false**) from at least one of the configured remote MEPs.
CCM Error defect	Indicates if a stream of erroneous CCMs is being received (**true**) or not (**false**) from a MEP in this MA.
CCM Xcon defect	Indicates if a stream of CCMs is being received (**true**) or not (**false**) from a MEP that belongs to another MA.
MEP RDI Received	Indicates that any other MEP in this MA is transmitting the RDI bit. Options include **true** or **false**.
MEP Last CCM Fault	The last-received CCM that triggered a MA fault.
MEP Xcon Last CCM Fault	The last-received CCM that triggered a cross-connect fault.
MEP Error Mac Status	Indicates a port status TLV. Options include **true** or **false**.
MEP Lbm NextSeqNumber	The next Transaction Identifier or Sequence Number to be sent in an LBM.
MEP Ltm NextSeqNumber	The next Transaction Identifier or Sequence Number to be sent in an LTM.
Fault Alarm Time	The time interval during which one or more defects should be detected before the fault alarm is issued
Fault Reset Time	The time interval during which the fault alarm is re-enabled to process faults
Lowest PrDefect Allowed	The lowest priority defect that allowed to generate fault alarm.
Highest PrDefect Present	The highest priority defect since the MEPs Fault Notification Generator in reset state.

Release History

Release 6.2.1; command was introduced.
Release 6.3.4; *mac_address* parameter deleted.
Release 6.4.4; **RFP Status** added.

Related Commands

ethoam endpoint	Creates an Ethernet OAM Maintenance End Point in the specified MA.
ethoam endpoint admin-state	Configures the administrative state of MEP.

MIB Objects

```
Dot1agCfmMep
   dot1agCfmMepActive
   dot1agCfmMepDirection
   dot1agCfmMepPortNumber
   dot1agCfmMepMacAddress
   dot1agCfmMepFngState
   dot1agCfmMepCcmEnabled
   dot1agCfmMepCcmLtmPriority
   dot1agCfmMepSomeRMepCcmDefect
   dot1agCfmMepErrorCcmDefect
   dot1agCfmMepXconCcmDefect
   dot1agCfmMepSomeRdiDefect
   dot1agCfmMepErrorCcmLastFailure
   dot1agCfmMepXconCcmLastFailure
   dot1agCfmMepErrMacStatus
   dot1agCfmMepLtmNextSeqNumber
   dot1agCfmMepFngAlarmTime
   dot1agCfmMepFngAlarmTime
   dot1agCfmMepLowPrDef
   dot1agCfmMepHighestPrDefect
```

show ethoam default-domain configuration

Displays the level, MHF, and ID permission values for the default domain.

show ethoam default-domain configuration

Syntax Definitions

N/A

Defaults

N/A.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show ethoam default-domain configuration
Level : 3,
MHF-Creation : mhfdefault,
ID-Permission : sendIdnone
```

output definitions

Level	The level assigned to the default domain. Configured through the **ethoam default-domain level** command.
MHF-creation	Indicates the MHF value for a VLAN that is part of the default MD Options include **none**, **explicit**, or **default**. Configured through the **ethoam default-domain mhf** command.
ID-Permission	The ID permision of the default domain. Configured through the **ethoam default-domain id-permission** command.

Release History

Release 6.4.3; command was introduced.

Related Commands

show ethoam default-domain	Displays the primary VLAN configuration for the default domain.

MIB Objects

```
dot1agCfmMaDefualtMdDefLevel
   dot1agCfmMaDefualtMdDefMhfCreation
   dot1agCfmMaDefualtMdDefIdPermission
```

show ethoam default-domain

Displays all the default MD information for all the primary VLANs or for a specific primary VLAN.

show ethoam default-domain [primary-vlan *vlan_id***]**

Syntax Definitions

vlan_id	The primary VLAN ID.

Defaults

By default, the default MD information for all primary VLANs is displayed.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the *vlan_id* parameter with this command to view information about the default MD for a specific primary VLAN.

Examples

```
-> show ethoam default-domain

Primary-Vlan   Mhf-creation    Level      Id-Permission Status
--------------+-------------+-----------+--------------+--------
      1        mhfDefer       no-level    sendIdDefer    true
      10       mhfDefault         3       sendIdNone     true

-> show ethoam default-domain primary-vlan 10
Primary-Vlan   Mhf-creation    Level      Id-Permission  Status
--------------+-------------+-----------+--------------+--------
      10        mhfDefault        3       sendIdNone     true
```

output definitions

Primary Vlan	The primary VLAN ID of the default MD.
Mhf-creation	The primary VLAN ID MHF value (**none**, **explicit**, or **default**).
Level	The primary VLAN level (**no-level**, **0–7**).
Id-Permission	The primary VLAN ID permission (**none**, **chassid**, or **defer**).

Release History

Release 6.3.1; command was introduced.

Related Commands

ethoam default-domain primary-vlan	Modifies the default domain for the specified primary VLAN.

MIB Objects

```
Dot1agCfmDefaultMdLevel
   dot1agCfmDefaultMdLevelVid
   dot1agCfmDefaultMdLevelMhfCreation
   dot1agCfmDefaultMdLevelLevel
```

show ethoam remote-endpoint domain

Displays the information of all remote MEPs learned as a part of the CCM message exchange.

show ethoam remote-endpoint domain *d_name* **association** *a_name* **end-point** *s-mepid* **[remote-mep** *r-mepid***]**

Syntax Definitions

d_name	Specifies the domain name.
a_name	Specifies the name of the Ethernet OAM Association.
s-mepid	Specifies the MEP of a specific MA. The valid range is 1–8191.
r-mepid	The remote MEP. The valid range is 1–8191.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show ethoam remote-endpoint domain MD association MA endpoint 10
Legends: PortStatusTlv: 1 = psBlocked, 2 = psUp, 0 = psNoTlv
         InterfaceStatusTlv: 1 = ifUp, 2 = ifDown, 4 = ifUnknown, 0=ifNoTlv


RMEP-ID RMEP     OkFailed  Mac Address    port I/f   RDI   Ch-id  Ch-id
        Status    Time                   Tlv  Tlv  value Subtype
------+---------+------+-----------------+---+----+-----+--------+------
  20   RMEP_OK   634600 00:E0:B1:6E:41:65  2   1   false LCL-ASND DUT-1
  30   RMEP_OK   334600 00:E0:B1:6E:41:64  2   1   false LCL-ASND DUT-2
```

output definitions

MEP-ID	Indicates the Maintenance End Point.
RMEP Status	The operational state of the remote MEP Remote State machines for this MEP, which can be **RMEP_IDLE**, **RMEP_START**, **RMEP_FAILED**, or **RMEP_OK**.
OkFailed Time	The time (SysUpTime) when the Remote MEP state machine last entered either the **RMEP_FAILED** or **RMEP_OK**.
MacAddress	The MAC address of the remote MEP.

output definitions (continued)

Port Status Tlv	The MAC status TLV last received.
I/f Status Tlv	The interface status TLV last received.

```
Note: - Output shown above is not accurate as it is adjusted to display it in the
single row. Following are modified:
P/S Tlv - Port Status Tlv
I/F Tlv - I/F Status Tlv
Ch-id Subtype - Chassis ID Subtype
Ch-id - Chassis ID
LCL-ASND - LOCALLY_ASSIGNED
```

Release History

Release 6.3.4; command was introduced.

Related Commands

show ethoam domain association end-point	Displays the information of a specific MEP in a Management Domain configured on the bridge.

MIB Objects

```
dot1agCfmMepDbTable
   dot1agCfmMepDbRMepIdentifier
   dot1agCfmMepDbRMepState
   dot1agCfmMepDbRMepFailedOkTime
   dot1agCfmMepDbRdi
   dot1agCfmMepDbPortStatusTlv
   dot1agCfmMepDbInterfaceStatusTlv
   dot1agCfmMepDbChassisIdSubtype
   dot1agCfmMepDbChassisId
```

show ethoam cfmstack

Displays the contents of CFM Stack Managed Object, which determines the relationships among MEPs and MIPs on a specific bridge port.

show ethoam cfmstack {port *slot/port* **| virtual | linkagg** *agg_num***}**

Syntax Definitions

slot/port	Slot and port number for which the contents of the configured MEP or MIP will be displayed.
agg_num	The aggregate ID for which the contents of the configured MEP or MIP will be displayed.
virtual	Virtual port.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show ethoam cfmstack port 1/3
Up MHF Configured:
  Vlan-id: 100,
  Direction:  up,
  MAC-Address: 00:D0:95:EC:84:B0,
  Maintenance Association: alcatel-sales,
  Maintenance Domain: esd.alcatel-lucent.com,
  MD-level: 3

Down MHF Configured:
  Vlan-id: 100,
  Direction: down,
  MAC-Address: 00:D0:95:F6:33:DA,
  Maintenance Association: alcatel-sales,
  Maintenance Domain: esd.alcatel-lucent.com,
  MD-level: 3

-> show ethoam cfmstack port virtual
MEP-Id 32 - Vlan 30:
  Direction: up,
  MAC-Address: 00:E0:B1:A5:F2:34,
  Maintenance Association: MA4,
  Maintenance Domain: MD4,
  MD-level: 4
```

output definitions

Vlan-id	The VLAN ID to which the MEP is attached.
Direction	Indicates the direction (**Inward** or **Outward)** of the Maintenance Point (MP) on the Bridge port.
MAC-Address	The MEP ID configured on this port.
Maintenance Domain	The name of the maintenance domain.
Maintenance Association	The name of the maintenance association.
MD-level	The MD level at which the MD was created.

Release History

Release 6.2.1; command was introduced.

Related Commands

ethoam endpoint admin-state	Creates an Ethernet OAM Maintenance End Point in the specified MA.

MIB Objects

```
Dot1agCfmMd
   dot1agCfmMdName
Dot1agCfmMa
   dot1agCfmMaName
Dot1agCfmStack
   dot1agCfmStackVlanIdOrNone
   dot1agCfmStackDirection
   dot1agCfmStackMacAddress
   dot1agCfmStackMdLevel
```

show ethoam linktrace-reply

Displays the content of the Linktrace reply (LTR) returned by a previously transmitted LTM. This command displays the LTR based on the transaction identifier or sequence number of the LTM for which the LTR is to be displayed.

show ethoam linktrace-reply domain *d-name* **association** *a-name* **endpoint** *s-mepid* **tran-id** *num*

Syntax Definitions

d-name	Specifies the domain name.
a-name	Name of the Ethernet OAM Association.
s-mepid	Specifies the MEP for which LTR is to be displayed. The valid range is 1-8191.
num	Specifies the Transaction ID or sequence number returned from a previously transmitted LTM.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- "LTM operation successful. Target is reachable." – This message suggests that LTM has reached the target and all the expected LTRs have been received.
- "LTM operation unsuccessful. Target not reachable." – This message suggests that LTM is successfully initiated but the target is not reachable.
- "LTM operation unsuccessful. Target is reachable." – This message suggest that Target is reachable but at least one of the LTR from intermediate hop is not received.
- "LTM operation in progress." – This message suggests that LTM operation is in progress. This message will appear if show CLI is fired before LTM Time-out time.
- "LTM Timed out."- This message suggests that either LTM is not initiated properly or when none of the expected LTRs is received in LTM Time-out duration which is 5 seconds.

Examples

```
-> show ethoam linktrace-reply domain MD association MA endpoint 10 tran-id 1256
LTM operation successful. Target is reachable.
Ttl : 63,
  LTM Forwarded : yes,
  Terminal MEP : no,
  Last Egress Identifier : 00-00:00:D0:95:EA:79:62,
  Next Egress Identifier : 00-00:00:D0:95:EA:9E:BA,
  Relay Action : RLY_FDB,
```

```
  Chassis ID Subtype : LOCALLY_ASSIGNED,
  Chassis ID : DUT-2,
  Ingress Action : ING_OK,
  Ingress Mac : 00:D0:95:EA:9E:D4,
  Ingress Port ID Subtype : LOCALLY_ASSIGNED,
  Ingress Port ID : 1/1,
  Egress Action : EGR_OK,
  Egress Mac : 00:D0:95:EA:9E:D5,
  Egress Port ID Subtype : LOCALLY_ASSIGNED,
  Egress Port ID : 1/2

Ttl : 62,
  LTM Forwarded : no,
  Terminal MEP : yes,
  Last Egress Identifier : 00-00:00:D0:95:EA:9E:BA,
  Next Egress Identifier : 00-00:00:00:00:00:00:00:00,
  Relay Action : RLY_HIT,
  Chassis ID Subtype : LOCALLY_ASSIGNED,
  Chassis ID : DUT-3,
  Ingress Action : ING_OK,
  Ingress Mac : 00:D0:95:EA:AB:D2,
  Ingress Port ID Subtype : LOCALLY_ASSIGNED,
  Ingress Port ID : 1/1,
  Egress Action : EGR_NONE,
  Egress Mac : 00:00:00:00:00:00,
  Egress Port ID Subtype : NONE,
  Egress Port ID : none
```

output definitions

Ttl	Time to live field for the returned LTR.
LTM Forwarded	Indicates whether the LTM was forwarded or not.
Terminal MEP	Indicates whether the MP reported in the reply Ingress/Egress TLV is a MEP.
Last Egress Identifier	Identifies the MEP linktrace initiator that originated, or the responder that forwarded, the LTM to which this LTR is the response.
Next Egress Identifier	Identifies the linktrace responder that transmitted this LTR, and can forward the LTM to the next hop.
Relay Action	Indicates how the dataframe targeted by the LTM would be passed to Egress bridge port. Options include **RLY_HIT**, **RLY_FDB**, or **RLY_MPDB**.
Ingress Action	Indicates how the dataframe targeted by the LTM would be received on the receiving MP. Options include **ING_NONE**, **ING_OK**, **ING_DOWN**, **ING_BLOCKED**, or **ING_VID**.
Ingress Mac	The MAC address returned in the ingress MAC address field.
Egress Action	Indicates how the dataframe targeted by the LTM would be passed through Egress bridge port. Options include **ING_NONE**, **ING_OK**, **ING_DOWN**, **ING_BLOCKED**, or **ING_VID**.
Egress Mac	The MAC address returned in the egress MAC address field.

Release History

Release 6.2.1; command was introduced.
Release 6.3.4; *mac_address* parameter deleted.

Related Commands

ethoam linktrace	Enables the maintenance entity to initiate transmitting of Link Trace Messages (LTM).

MIB Objects

```
Dot1agCfmLtr
   dot1agCfmLtrTtl
   dot1agCfmLtrForwarded
   dot1agCfmLtrTerminalMep
   dot1agCfmLtrLastEgressIdentifier
   dot1agCfmLtrNextEgressIdentifier
   dot1agCfmLtrRelay
   dot1agCfmLtrIngress
   dot1agCfmLtrIngressMac
   dot1agCfmLtrEgress
   dot1agCfmLtrEgressMac
```

show ethoam linktrace-tran-id

Displays the transaction identifiers returned by previously generated LTMs from a specified MEP.

show ethoam linktrace-tran-id domain {*domain_name* | *mac_address***} association** *association_name* **endpoint** *mep_id*

Syntax Definitions

domain_name	Specifies the domain name.
mac_address	Specifies the CFM system MAC address.
association_name	Name of the Ethernet OAM Association.
mep_id	Specifies the MEP for which LTR is to be displayed. The valid range is 1-8191.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show ethoam linktrace-tran-id domain esd.alcatel-lucent.com association
alcatel-sales endpoint 3
S.No   Transaction Id
-------+----------------------
      1    13357,
      2    13358,
      3    13359,
```

output definitions

S.No	Indicates the sequence number.
Transaction Id	Indicates the Transaction Identifier returned from a previously transmitted LTM.

Release History

Release 6.3.1; command was introduced.

Related Commands

ethoam linktrace	Enables the maintenance entity to initiate transmitting of Link Trace Messages (LTM).

MIB Objects

```
Dot1agCfmLtr
   dot1agCfmLtrSeqNumber
```

show ethoam vlan

Displays the Ethernet OAM statistics of all the Management Domains configured on the bridge. Also, displays the statistics of all the MAs and matching MEPs for all the MDs.

show ethoam vlan *vlan-id*

Syntax Definitions

vlan-id	VLAN ID, primary or non-primary VID (for example, ‘10’)

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show ethoam vlan 10
Primary Vlan : 10,
Associated Vlan-list : 15-20 25 50-80

-> show ethoam vlan 15
Primary Vlan : 10,
Associated Vlan-list : 15-20 25 50-80
```

Release History

Release 6.3.4; command was introduced.

Related Commands

ethoam endpoint	Enables the maintenance entity to initiate transmitting loopback messages (LBMs) and obtaining loopback replies.

MIB Objects

```
dot1agCfmMaVlanTable
    dot1agCfmVlanVid
    dot1agCfmVlanPrimaryVid
```

show ethoam statistics

Displays the Ethernet OAM of all the Management Domains configured on the bridge. Also, displays the statistics of all the MAs and matching MEPs for all the MDs.

show ethoam statistics domain {*domain_name* | *mac_address***} [association** *association_name***] [end-point** *endpoint_id***]**

Syntax Definitions

domain_name	Specifies the domain name.
mac_address	Specifies the CFM system MAC address.
association_name	Specifies the name of Ethernet OAM Association.
endpoint_id	Specifies a MEP for a specific MA.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show ethoam statistics domain MD
MEP-ID  CCM   CCM Seq   LBR   LBR Out  LBR   LBR Bad  Unexpected   MA
        Out    Error    In   of order  Out     MSDU    LTR In
------+------+-------+------+--------+------+--------+----------+---------
     3    105       0      0        0      0        0          0  MA

-> show ethoam statistics domain MD association MA
MEP-ID  CCM   CCM Seq   LBR   LBR Out  LBR   LBR Bad  Unexpected
        Out    Error    In   of order  Out     MSDU    LTR In
------+------+-------+------+--------+------+--------+----------
     3    105       0      0        0      0        0          0

-> show ethoam statistics domain MD association MA endpoint 3
MEP-ID  CCM   CCM Seq   LBR   LBR Out  LBR   LBR Bad  Unexpected
        Out    Error    In   of order  Out     MSDU    LTR In
------+------+-------+------+--------+------+--------+----------
     3    105       0      0        0      0        0          0
```

output definitions

MEP-Id	The MEP ID configured in the specified MA.
CCM Out	The total number of CCMs transmitted.

output definitions

CCM Seq Error	The total number of out-of-sequence CCMs received from all remote MEPs.
LBR In	The total number of valid, in-order LBRs received.
LBR Out of order	The total number of valid, out-of-order LBRs received.
LBR Out	The total number of LBRs transmitted.
LBR Bad MSDU	The total number of LBRs received whose mac_service_data_unit did not match.
Unexpected LTR In	The total number of unexpected LTRs received.

Release History

Release 6.2.1; command was introduced.
Release 6.3.1; *mac_address* parameter added.

Related Commands

ethoam endpoint	Enables the maintenance entity to initiate transmitting loopback messages (LBMs) and obtaining loopback replies.

MIB Objects

```
Dot1agCfmMep
   dot1agCfmMepIdentifier
   dot1agCfmMepCcmOut
   dot1agCfmMepRCcmSequenceErrors
   dot1agCfmMepLbrIn
   dot1agCfmMepLbrInOutOfOrder
   dot1agCfmMepLbrOut
   dot1agCfmMepLbrBadMsdu
   dot1agCfmMepUnexpLtrIn
```

show ethoam config-error

Displays the configuration error for a specified VLAN and port or linkagg.

show ethoam config-error [vlan *vlan_id***] [{port** slot/port **| linkagg** *agg_id***}]**

Syntax Definitions

vlan_id	VLAN Identifier.
slot/port	Physical slot and port.
agg_id	Logical Linkagg Identifier.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
cli> show ethoam config-error
Vlan    Port   Error-type
------+------+------------
10       1/2    CFMleak
10       1/10   CFMleak
30       1/2    CFMleak

cli> show ethoam config-error vlan 10
vlan    port   error-type
------+------+------------
10       1/2    CFMleak
10       1/10   CFMleak

cli> show ethoam config-error port 1/2
vlan    port   error-type
------+------+------------
10       1/2    CFMleak
30       1/2    CFMleak

cli> show ethoam config-error vlan 10 port 1/2
vlan    port   error-type
------+------+------------
10       1/2    CFMleak
```

output definitions

vlan	VLAN identifier number.
port	Physical slot and port number.
error-type	Type of an error.

Release History

Release 6.3.4; command was introduced.

Related Commands

ethoam linktrace	Enables the maintenance entity to initiate transmitting of Link Trace Messages (LTM).

MIB Objects

```
dot1agCfmConfigErrorListTable
   dot1agCfmConfigErrorListVid
   dot1agCfmConfigErrorListIfIndex
   dot1agCfmConfigErrorListErrorType
```

show ethoam one-way-delay

Displays the one-way ETH-DM delay (latency) and jitter parameters either for all entries or for a specified MAC address for a particular source MEP-ID.

show ethoam one-way-delay domain *domain* **association** *association* **endpoint** *s-mepid* **[mac-address** *mac-add***]**

Syntax Definitions

domain	Specifies the domain name used while creating the management domain for which this management association is created.associationPhysical slot and port.
association	Association name for the created Ethernet OAM Association.
s-mepid	Source MEP-ID. Vaild Range 1-8191.
mac-add	MAC-Address of the remote MEP.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Dash (‘-‘) in the output in Jitter column signifies that the value can not be calculated as the previous delay value is unknown. This will happen only when 1DM is received for the first time.
- Maximum entries that Delay Result table can store are 1024. After that, the oldest entry is deleted from the table whenever a new entry is required.

Examples

```
cli> show ethoam one-way-delay domain MD association MA endpoint 10
Legend: Jitter: - = undefined value

Remote Mac address            Delay (us)  Jitter (us)
--------------------------+-------------+--------------------------------
00:d0:95:ef:44:44              2369          1258
00:d0:95:ef:66:88              5896           282
00:d0:95:ef:88:88              2584           -
00:d0:95:ef:66:55              2698          4782

cli> show ethoam one-way-delay domain MD association MA endpoint 10 mac-address
00:d0:95:ef:44:44
Legend: Jitter: - = undefined value

Remote Mac address       Delay (us)   Jitter (us)
-------------------+-------------+------------------
00:d0:95:ef:44:44        2369           1258
```

output definitions

Remote Mac address	Remote MAC address.
Delay	Physical slot and port number.
eJitter	Type of an error.

Release History

Release 6.4.3; command was introduced.

Related Commands

ethoam one-way-delay	Initiates one-way-delay messages from a particular MEP to an RMEP.

MIB Objects

```
dot1agCfmMdTable
       dot1agCfmMdName
dot1agCfmMaNetTable
       dot1agCfmMaNetName
dot1agCfmMepTable
       dot1agCfmMepIdentifier
alaDot1agCfmMepDelayRsltTable
       alaDot1agCfmMepDelayRMepMacAddress
       alaCfmMepDelayTestType
       alaCfmMepDelayTestDelay
       alaCfmMepDelayVariation
```

show ethoam two-way-delay

Displays the two-way ETH-DM delay and jitter parameters for a specific remote MAC-Address or for all the MAC-Addresses for which two-way-delay was initiated for a particular source MEP-ID.

show ethoam two-way-delay domain *domain* **association** *association* **endpoint** *s-mepid* **[mac-address** *mac-add***]**

Syntax Definitions

domain	Specifies the domain name used while creating the management domain for which this management association is created.associationPhysical slot and port.
association	Association name for the created Ethernet OAM Association.
s-mepid	Source MEP-ID. Vaild Range 1-8191.
mac-add	MAC-Address of the remote MEP.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- If ‘0’ appears in the output in RMEP-ID column signifies that the DMM was initiated with target-macaddress. As multiple RMEPs can have same mac-address.
- If a dash (‘-‘) appears in the output in Jitter column signifies that the value can not be calculated as the previous delay value is unknown, i.e. if only one reply for DMM (DMR) is received and this was the first time DMM was initiated from the MEP, then jitter will not be calculated.
- Maximum entries that Delay Result table can store are 1024. After that, the DMM request shall be rejected if a new entry needs to be created for the MEP. If entry for the MEP already exists in the table, that entry shall be updated with the new one.

Examples

```
cli> show ethoam two-way-delay domain MD association MA endpoint 10 mac-address
00:d0:95:ef:44:44
Legend: Jitter: - = undefined value
      : RMEP-ID: 0 = two-way-delay was initiated with target mac-address

Remote Mac address  RMEP-ID   Delay (us)     Jitter (us)
------------------+--------+--------------+--------------
 00:d0:95:ef:44:44   12         2369          1258
```

```
cli> show ethoam two-way-delay domain MD association MA endpoint 10 remote-mep 0
Legend: Jitter: - = undefined value
      : RMEP-ID: 0 = two-way-delay was initiated with target mac-address

Remote Mac address  RMEP-ID  Delay (us)  Jitter (us)
------------------+--------+-------------+-----------
 00:d0:95:ef:66:88    0         5896   282
 00:d0:95:ef:88:88    0         2584   1856

cli> show ethoam two-way-delay domain MD association MA endpoint 10 remote-mep 15
Legend: Jitter: - = undefined value
      : RMEP-ID: 0 = two-way-delay was initiated with target mac-address

Remote Mac address  RMEP-ID  Delay (us)  Jitter (us)
------------------+--------+-------------+-----------
 00:d0:95:ef:66:55   15         2736     -

cli> show ethoam two-way-delay domain MD association MA endpoint 10
Legend: Jitter: - = undefined value
      : RMEP-ID: 0 = two-way-delay was initiated with target mac-address

Remote Mac address  RMEP-ID  Delay (us)  Jitter (us)
------------------+--------+-------------+-----------
 00:d0:95:ef:44:44   12         2369  1258
 00:d0:95:ef:66:88    0         5896   282
 00:d0:95:ef:88:88    0         2584   1856
 00:d0:95:ef:66:55   15         2736     -
```

output definitions

Remote Mac address	Remote MAC address.
RMEP-ID	Value of RMEP-ID
Delay	Physical slot and port number.
Jitter	Type of an error.

Release History

Release 6.4.3; command was introduced.

Related Commands

ethoam two-way-delay	Initiate two-way-delay messages from a particular MEP to an RMEP using target-endpoint or target-MAC address.

MIB Objects

```
dot1agCfmMdTable
      dot1agCfmMdName
dot1agCfmMaNetTable
      dot1agCfmMaNetName
dot1agCfmMepTable
      dot1agCfmMepIdentifier
```

```
alaDot1agCfmMepDelayRsltTable
       alaCfmMepDelayRMepMacAddress
       alaCfmMepDelayTestType
       alaCfmMepDelayTestDelay
   alaDot1agCfmMepDelayVariation
```

52 LINK OAM Commands

Ethernet in the First Mile (EFM), also known as LINK OAM, is a collection of protocols specified in IEEE 802.3ah, defining Ethernet in the access networks that connects subscribers to their immediate service provider. EFM, EFM-OAM and LINKOAM refers to IEEE 802.3ah standard.

LINK OAM (operation, administration, and maintenance) is a tool which monitors Layer-2 link status on the network by sending OAM protocol data units (OAMPDUs) between the network devices. OAMPDUs contain control and status information used to monitor, test and troubleshoot OAM-enabled links. By enabling LINK OAM on switch ports, network administators can monitor the link-related issues on the first mile. LINK OAM provides network administrators the ability to monitor link performance, remote fault detection and remote loopback control.

Note. EFM (LINK OAM) does not include functions such as station management, bandwidth allocation or provisioning functions.

MIB information for the EFM (LINK OAM) commands is as

Filename: alcatel-ind1-dot3-oam-mib.mib
Module: ALCATEL-IND1-DOT3-OAM-MIB

Filename: dot3-oam-mib.mib
Module: DOT3-OAM-MIB

A summary of the available commands is listed here:

Global Configuration Commands	**efm-oam** **efm-oam multiple-pdu-count** **efm-oam errored-frame-seconds-summary** **efm-oam errored-frame-period** **efm-oam errored-frame**
Port Status Commands	**efm-oam port status** **efm-oam port mode** **efm-oam port propagate-events**
Port Event Notification Commands	**efm-oam errored-frame** **efm-oam errored-frame-period** **efm-oam errored-frame-seconds-summary**
Timer Interval Commands	**efm-oam port keepalive-interval** **efm-oam port hello-interval**

Remote Loopback Commands	**efm-oam port remote-loopback** **efm-oam port remote-loopback start** **efm-oam port l1-ping**
Show Commands	**show efm-oam port** **show efm-oam port detail** **show efm-oam port remote detail** **show efm-oam port history** **show efm-oam port l1-ping detail** **show efm-oam port statistics** **show efm-oam configuration**
Clear Commands	**clear efm-oam statistics** **clear efm-oam log-history**

efm-oam

Enables or disables the LINK OAM protocol on the switch.

efm-oam {enable | disable}

Syntax Definitions

enable	Enables the LINK OAM protocol.
disable	Disables the LINK OAM protocol.

Defaults

By default, the LINK OAM protocol is disabled for the switch.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- LINK OAM must be enabled globally for the OAM to be functional on all the ports.
- When LINK OAM is disabled globally, all dynamically learned information on the port, including peer information, is deleted. However, the LINK OAM configuration for the port is retained.

Examples

```
-> efm-oam enable
-> efm-oam disable
```

Release History

Release 6.4.2; command was introduced.

Related Commands

efm-oam port status	Enables or disables LINK OAM protocol on the specified port or on a range of ports.
efm-oam port mode	Configures the LINK OAM mode on the port or on the range of ports to active or passive.
show efm-oam configuration	Displays the global LINK OAM configuration.

MIB Objects

```
alaDot3OamStatus
```

efm-oam port status

Enables or disables LINK OAM protocol on the specified port or on a range of ports.

efm-oam port *slot/port* **[-***port2***] status {enable | disable}**

Syntax Definitions

slot/port	The slot number of the module and the physical port number on that module.
-port2	Specifies the last port in the range of ports.
enable	Enables LINK OAM protocol on the specified port.
disable	Disables LINK OAM protocol on the specified port.

Defaults

By default, the LINK OAM protocol is disabled on all ports for the switch.

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- LINK OAM must be enabled globally for the OAM to be functional on all the ports.
- If LINK OAM is disabled for the port or globally disabled for the switch, any OAMPDUs received are discarded.
- When LINK OAM is disabled for the port, all dynamically learned information on the port, including peer information, is deleted. However, the LINK OAM configuration for the port is retained.
- LINK OAM is not supported on the mirroring ports.
- In link aggregates, LINK OAM is supported on an individual aggregable port only.

Examples

```
-> efm-oam port 1/1 status enable
-> efm-oam port 1/1 status disable
-> efm-oam port 2/1-10 status enable
-> efm-oam port 2/1-4 status disable
```

Release History

Release 6.4.2; command was introduced.

Related Commands

efm-oam port mode	Configure a LINK OAM mode on the port or on the range of ports to active or passive.
show efm-oam configuration	Displays the global LINK OAM configuration.
show efm-oam port	Displays the status of LINK OAM on all the ports in the system, along with other relevant information such as OAM mode, operational status and loopback status of the port.
show efm-oam port detail	Displays the configuration and other related parameters for a port.

MIB Objects

```
dot3OamTable
   dot3OamAdminState
```

efm-oam port mode

Configures the LINK OAM mode on the port or on the range of ports to active or passive.

efm-oam port *slot/port***[**-*port2***] mode {active | passive}**

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).
-port2	Specifies the last port in the range of ports.
active	Configures the LINK OAM mode to active.
passive	Configures the LINK OAM mode to passive.

Defaults

By default, LINK OAM mode is set to active on all ports.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- LINK OAM discovery process is never initiated from a port when it is in passive mode. At least one of the two peer ports should be in active mode.
- An active port will respond to Loopback-control OAMPDUs only if the peer EFM-OAM client is also in active mode.

Examples

```
-> efm-oam port 1/1 mode active
-> efm-oam port 1/1 mode passive
-> efm-oam port 2/1-10 mode active
-> efm-oam port 2/1-4 mode passive
```

Release History

Release 6.4.2; command was introduced.

Related Commands

efm-oam port status	Enables or disables LINK OAM protocol on the specified port or on a range of ports.
show efm-oam port	Displays the status of LINK OAM on all the ports in the system, along with other relevant information such as OAM mode, operational status and loopback status of the port.
show efm-oam configuration	Displays the global LINK OAM configuration.

MIB Objects

```
dot3OamTable
   dot3OamMode
```

efm-oam port keepalive-interval

Configures the timeout interval for the dynamically learned neighboring devices on a port or on a range of ports. Keepalive-interval is the maximum time period for which a LINK OAM port shall wait for a hello message from its peer before resetting a discovery session.

efm-oam port *slot/port***[**-*port2***] keepalive-interval** *seconds*

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).
-*port2*	Specifies the last port in the range of ports.
seconds	Specifies the keep-alive interval value in seconds. The range for this interval is 5 to 120 seconds.

Defaults

By default, the keep-alive interval value is 5 seconds.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Even if unsupported OAMPDU is received on the port, keep-alive timer is reset on the port.
- To set the timer to its default value, set 5 seconds as the keepalive-interval.

Examples

```
-> efm-oam port 1/1 keepalive-interval 10
-> efm-oam port 2/1-10 keepalive-interval 10
```

Release History

Release 6.4.2; command was introduced.

Related Commands

efm-oam port hello-interval	Configures the time interval (in seconds) by which the information OAMPDUs are transmitted out of a LINK OAM enabled port.
show efm-oam port detail	Displays the configuration and other related parameters for a port.

MIB Objects

```
alaDot3OamTable
   alaDot3OamKeepAliveInterval
```

efm-oam port hello-interval

Configures the time interval (in seconds) by which the information OAMPDUs are transmitted out of an LINK OAM enabled port.

efm-oam port *slot/port***[**-*port2***] hello-interval** *seconds*

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).
-*port2*	Specifies the last port in the range of ports.
seconds	Specifies the time interval (in seconds) this port waits before sending out the next hello packet.The range for this timer is 1 to 60 seconds.

Defaults

By default, the hello-interval value is set to 1 second.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the hello-interval value of 1 second to reset the timer to its default value.
- On a given port, hello interval time period should not be more than half of keep alive timer on the peer port.

Examples

```
-> efm-oam port 1/1 hello-interval 5
-> efm-oam port 2/1-10 hello-interval 10
```

Release History

Release 6.4.2; command was introduced.

Related Commands

efm-oam port hello-interval	Configures the time interval (in seconds) by which the information OAMPDUs are transmitted out of a LINK OAM enabled port.
efm-oam port keepalive-interval	Configures the timeout interval for the dynamically learned neighboring devices on a port or on a range of ports. Keepalive-interval is the maximum time period for which a LINK OAM port shall wait for a hello message from its peer before resetting a discovery session.
show efm-oam port detail	Displays the configuration and other related parameters for a port.

MIB Objects

```
alaDot3OamTable
   alaDot3OamHelloInterval
```

efm-oam port remote-loopback

Specifies whether loopback requests from peers are processed or ignored on the specified port.

efm-oam port *slot/port***[**-*port2***] remote-loopback {process | ignore}**

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).
-port2	Specifies the last port in the range of ports.
process	Processes incoming loopback request from peer LINK OAM port.
ignore	Ignore (discard) incoming loopback requests.

Defaults

By default, the incoming loopback requests are ignored.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- When the remote-loopback is in **process** mode, the session started by peer LINK OAM client will be processed by local LINK OAM port. As a result, remote port will be in remote-loopback state and the local port will be local-loopback state.
- When the remote-loopback is in **ignore** mode, the session started by peer LINK OAM will not be processed by the local port.

Examples

```
-> efm-oam port 1/1 remote-loopback process
-> efm-oam port 1/1 remote-loopback ignore
-> efm-oam port 2/1-10 remote-loopback process
-> efm-oam port 2/1-4 remote-loopback ignore
```

Release History

Release 6.4.2; command was introduced.

Related Commands

efm-oam port remote-loopback start	Initiates the loopback control PDU towards the peer port to start or stop the loopback session on the specified port.
show efm-oam port detail	Displays the LINK OAM configuration and other related parameters for a port.
show efm-oam port remote detail	Displays the configuration and details of the related parameters of the remote port.

MIB Objects

```
dot3OamLoopbackTable
   dot3OamLoopbackIgnoreRx
```

efm-oam port remote-loopback start

Initiates the loopback control PDU towards the peer port to start or stop the loopback session on the specified port.

efm-oam port *slot/port* **remote-loopback {start | stop}**

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).
start	Specifies whether to start the loopback request.
stop	Specifies whether to stop the loopback request.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Before issuing this command, the LINK OAM port has to be in active mode and discovery of peer ports has to be completed.
- When loopback is started from a port towards a peer port which is configured to ignore the loopback request, the loopback response timer will timeout and no error is displayed. In such case, verify the loopback-state of two ports by using the command **show efm-oam port remote detail**.
- The maximum number of simultaneous loopback sessions supported per network interface is 2. If a third loopback is started through CLI, an error will be displayed at the CLI prompt.

Examples

```
-> efm-oam port 1/1 remote-loopback start
-> efm-oam port 1/1 remote-loopback stop
```

Release History

Release 6.4.2; command was introduced.

Related Commands

efm-oam port remote-loopback	Specifies an action that should perform when a loopback request is received from the peer on a port or on a range of ports.
show efm-oam port remote detail	Displays the configuration and details of the related parameters of the remote port.
show efm-oam configuration	Displays the global LINK OAM configuration.

MIB Objects

```
dot3OamLoopbackTable
   dot3OamLoopbackStatus
```

efm-oam port propagate-events

Configures whether or not the specified port or range of ports will propagate local event notifications to the remote peer.

efm-oam port *slot/port***[**-*port2***] propagate-events {critical-event | dying-gasp} {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).
-*port2*	Specifies the last port in the range of ports.
critical-event	Configures the notification status for critical events.
dying-gasp	Configures the notification status for dying gasp events.
enable	Enables the notification of critical-event or dying-gasp events to the peer.
disable	Disables the notification of critical-event or dying-gasp events to the peer.

Defaults

By default, the notification status for both critical-event and dying-gasp events is set to enabled.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- When the system is set for critical event or a dying-gasp event, the local OAM entity indicates the event through the OAMPDU flags to its peer OAM entity.
- In case of port admin down, the OAM IFU-PDU with dying-gasp bit set will be sent to peer as soon as a failure is detected and transmission will continue till the specific port actually goes down.
- In case of takeover or reload of the switch, the OAM IFU-PDU with dying-gasp bit set will be sent to peer as soon as a failure is detected and transmission will continue till the specific device actually goes down.
- The information PDUs with dying gasp bit set is transmitted towards peer as soon as link-down is detected at NI. However, if there is a link flap (i.e link comes again) before the expiry of link-flap timer, then normal information PDU transmission with dying-gasp bit reset shall resume. This will cause clearing of alarms or trap on the peer port.

Examples

```
-> efm-oam port 1/1 propagate-events critical-event enable
-> efm-oam port 1/1 propagate-events critical-event disable
-> efm-oam port 2/1-10 propagate-events dying-gasp enable
-> efm-oam port 2/1-4 propagate-events dying-gasp disable
```

Release History

Release 6.4.2; command was introduced.

Related Commands

show efm-oam port remote detail	Displays the configuration and details of the related parameters of the remote port.
show efm-oam port statistics	Displays the LINK OAM statistics on a port, or a range of ports or on all ports.

MIB Objects

```
dot3OamEventConfigTable
   dot3OamDyingGaspEnable
   dot3OamCriticalEventEnable
```

efm-oam errored-frame-period

Configures the threshold, window frame values and the status for notification when the number of frame-errors exceed the threshold in a given period of time (specified) by window. When the number of frame errors exceeds a threshold within a given window defined by a number of frames (for example, 10 frames out of 1000 had errors), an Errored Frame Period event is generated.

efm-oam port *slot/port***[-***port2***] errored-frame-period [threshold** *threshold_symbols***] [window** *window_frames***] [notify {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).
-port2	The last port number in a range of ports that you want to configure on the same slot. (e.g. 3/1-4 specifies ports 1,2,3 and 4 on slot 3).
threshold_symbols	Specifies the frame error threshold number. The range supported is 1 to maximum 4 byte integer value (4294967295).
window_frames	Specifies the number of frames used to define a window within which the frame period errors are measured.
enable	Enables notification of the Errored Frame Period event.
disable	Disables notification of the Errored Frame Period event.

Defaults

parameter	default
threshold_symbols	1 frame error
enable | disable	enable

The default for *window_frames* depends on the port-types. The default, minimum and maximum supported values for various port-types are:

port-type	default value	minimum value	maximum value
100 mbps	200000	20000	12000000
1000 X	2000000	200000	120000000
1000 T	2000000	200000	120000000
10 Gig	20000000	2000000	1200000000

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The command can be issued in any order like window, threshold, and notify. However, at least one option needs to be entered.
- To enter many ports in a single command, use a hyphen to specify a range of ports (e.g. 3/1-16).

Examples

```
-> efm-oam port 1/1 errored-frame-period threshold 1 window 3000000 notify enable
-> efm-oam port 1/1 errored-frame-period notify disable
-> efm-oam port 2/1-4 errored-frame-period threshold 1 window 3000000 notify enable
-> efm-oam port 2/1-2 errored-frame-period notify disable
```

Release History

Release 6.4.2; command was introduced.

Related Commands

efm-oam errored-frame	Configures the threshold, window and notify-status for errored-frame on a port. The frame-period measures the frame-errors, within a specified window of time.
efm-oam errored-frame-seconds-summary	Configures the threshold, window and notify-status for errored-frame-seconds-summary on a port. The Errored Seconds are the time in seconds in which at least one frame error has occurred.
show efm-oam port detail	Displays the Errored Frame Period Event threshold, window, and notification parameter values for a port.

MIB Objects

```
dot3OamEventConfigTable
   dot3OamErrFramePeriodWindow
   dot3OamErrFramePeriodThreshold
   dot3OamErrFramePeriodEvNotifEnable
```

efm-oam errored-frame

Configures an error frame threshold or window on a LINK OAM port and set notification status for errored frame events. When the number of frame errors exceeds a threshold within a given window defined by a period of time (for example, 10 frames in 1 second had errors), an Errored Frame Event is generated.

efm-oam port *slot/port***[-***port2***] errored-frame [threshold** *threshold_symbols***] [window** *window_seconds***] [notify {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).
-port2	The last port number in a range of ports that you want to configure on the same slot (e.g 3/1-4 specifies ports 1,2,3, and 4 on slot 3).
threshold_symbols	Specifies the frame error threshold number.
window_seconds	Specifies the window of time, in which the frame errors will be measured. The duration should be in units of 100ms.
enable	Enables notification of the Errored Frame event.
disable	Disables notification of the Errored Frame event.

Defaults

parameter	default
threshold_symbols	1 frame error
window_seconds	1 second (10 dsec)
enable | disable	enable

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The various options, threshold, window and notify can be issued in any order. However, at least one option has to be entered.
- To enter many ports in a single command, use a hyphen to specify a range of ports (e.g. 3/1-16).

Examples

```
-> efm-oam port 1/1 errored-frame threshold 10 window 32 notify enable
-> efm-oam port 1/1 errored-frame notify disable
-> efm-oam port 2/1-4 errored-frame threshold 10 window 32 notify enable
-> efm-oam port 2/1-2 errored-frame notify disable
```

Release History

Release 6.4.2; command was introduced.

Related Commands

efm-oam errored-frame-seconds-summary	Configures the threshold, window and notify-status for errored-frame-seconds-summary on a port.
efm-oam errored-frame-period	Configures the threshold, window and notify-status for errored-frame-period errors on a port. The errored-frame-period measures the frame-errors, within a specified window of frames.
show efm-oam port statistics	Displays the LINK OAM statistics on a port, or a range of ports or on all ports.

MIB Objects

```
dot3OamEventConfigTable
   dot3OamErrFrameWindow
   dot3OamErrFrameThreshold
   dot3OamErrFrameEvNotifEnable
```

efm-oam errored-frame-seconds-summary

Configures the threshold, window and notify-status for errored-frame-seconds-summary on a port. The Errored Seconds are the time in seconds in which at least one frame error has occurred.

efm-oam port *slot/port***[**-*port2***] errored-frame-seconds-summary [threshold** *threshold_seconds***] [window** *window_seconds***] [notify {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).
-*port2*	The last port number in a range of ports that you want to configure on the same slot (e.g 3/1-4 specifies ports 1,2,3, and 4 on slot 3).
threshold_symbols	Specifies the frame error threshold number.
window_seconds	Specifies the window of time in which the frame errors will be measured.
enable	Enables notification of the Errored Frame Seconds Summary event.
disable	Disables notification of the Errored Frame Seconds Summary event.

Defaults

parameter	default
threshold_symbols	1 errored frame second
window_seconds	60 seconds. (600 dsec).
enable | **disable**	enable

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The various options, threshold, window and notify can be issued in any order. However, at least one option has to be entered.
- To enter many ports in a single command, use a hyphen to specify a range of ports (e.g. 3/1-16).

Examples

```
-> efm-oam port 1/1 errored-frame-seconds-summary threshold 1 window 700 notify
enable
-> efm-oam port 1/1 errored-frame-seconds-summary notify disable
-> efm-oam port 2/1-4 errored-frame-seconds-summary threshold 1 window 700 notify
enable
-> efm-oam port 2/1-2 errored-frame-seconds-summary notify disable
```

Release History

Release 6.4.2; command was introduced.

Related Commands

efm-oam errored-frame	Configures the threshold, window and notify-status for errored-frame on a port. The frame-period measures the frame-errors, within a specified window of time.
efm-oam errored-frame-period	Configures the threshold, window and notify-status for errored-frame-period errors on a port. The errored-frame-period measures the frame-errors, within a specified window of frames.
show efm-oam port statistics	Displays the LINK OAM statistics on a port, or a range of ports or on all ports.

MIB Objects

```
dot3OamEventConfigTable
   dot3OamErrFrameSecsSummaryWindow
   dot3OamErrFrameSecsSummaryThreshold
   dot3OamErrFrameSecsEvNotifEnable
```

efm-oam multiple-pdu-count

Configures the value of multiple PDU count. When multiple PDU count is set to a specific number in case of any of the threshhold cross events, the same event notification PDU will be transmitted that many times towards the peer.

efm-oam multiple-pdu-count *count*

Syntax Definitions

count	Specifies the number of PDUs that have to be sent in case of event-notification TLVs. The range is 1 to 10 PDUs.

Defaults

By default, the PDU-count value is set to 3.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> efm-oam multiple-pdu-count 5
```

Release History

Release 6.4.2; command was introduced.

Related Commands

show efm-oam configuration	Displays the global LINK OAM configuration.
show efm-oam port remote detail	Displays the configuration and details of the related parameters of the remote port.

MIB Objects

```
alaDot3OamMultiplePduCount
```

efm-oam port l1-ping

Configures the number of frames to be sent by the current LINK OAM port to the remote port's MAC address (l1 ping) and the delay between each consecutive sent frames and to start the ping operation.

efm-oam port *slot/port* **l1-ping [num-frames** *number***] [delay** *milliseconds***] [start]**

Syntax Definitions

slot/port	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).
number	Specifies the number of frames that needs to be sent during ping operation. The allowed range of numbers is between 1 to 20.
milliseconds	Specifies time interval between two consecutive PDUs. The allowed range of delay is between 100 to 1000 milliseconds.
start	Specifies to start the ping operation.

Defaults

parameter	default
number	5 frames
milliseconds	1000 milliseconds

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The command is valid only when the LINK OAM is enabled globally, port is in active mode, discovery is done, and the port is in remote loopback mode.
- L1 ping can be started only when the port is in remote loopback mode.

Examples

```
-> efm-oam port 1/12 l1-ping num-frames 6 delay 300 start
-> efm-oam port 1/20 l1-ping num-frames 12 delay 500 start
-> efm-oam port 1/15 l1-ping num-frames 5 delay 100 start
-> efm-oam port 1/15 l1-ping num-frames 4 delay 200 start
-> efm-oam port 1/5 l1-ping num-frames 100 delay 300 start
```

Release History

Release 6.4.2; command was introduced.

Related Commands

show efm-oam port l1-ping detail	Displays the frames lost during a loopback session.
show efm-oam port statistics	Displays the LINK OAM statistics on a port, or a range of ports or on all ports.

MIB Objects

```
alaDot3OamLoopbackTable
   alaDot3OamPortL1PingFramesConf
   alaDot3OamPortL1PingFramesDelay
   alaDot3OamPortL1PingStatus
   alaDot3OamPortL1PingFramesSent
   alaDot3OamPortL1PingFramesReceived
   alaDot3OamPortL1PingAverageRoundTripDelay
```

show efm-oam configuration

Displays the global LINK OAM configuration.

show efm-oam configuration

Syntax Definitions

N/A

Defaults

N/A.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use this command to display the global configuration of LINK OAM.

Examples

```
-> show efm-oam configuration
EFM OAM Status                : enabled,
Multiple PDU Count            : 5
```

Output fields are described here:

output definitions

EFM OAM status	The current administrative status of LINK OAM on this switch (**Enabled** or **Disabled**).
Multiple PDU Count	The number of PDUs sent when LINK OAM needs to send multiple Event Notification.

Release History

Release 6.4.2; command was introduced.

Related Commands

efm-oam	Enables or disables the LINK OAM protocol on the switch.
show efm-oam port detail	Displays the LINK OAM configuration and other related parameters for a port.

MIB Objects

```
alaDot3OamStatus
   alaDot3OamMultiplePduCount
```

show efm-oam port

Displays the status of LINK OAM on all the ports in the system, along with other relevant information such as OAM mode, operational status and loopback status of the port.

show efm-oam port [*slot/port1-port2***] [enable | disable] [active | passive]**

Syntax Definitions

slot/port1	The slot number for the module and the physical port number on that module (e.g. 3/1 specifies port 1 on slot 3).
-port2	The last port number in a range of ports that you want to configure on the same slot (e.g. 3/1-4 specifies ports 1,2,3, and 4 on slot 3).
enable	Specifies whether to display the LINK OAM enabled ports.
disable	Specifies whether to display the LINK OAM disabled ports.
active	Specifies whether to display the LINK OAM active ports.
passive	Specifies whether to display the LINK OAM passive ports.

Defaults

By default, displays the LINK OAM status on all ports.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use this command to display the state of LINK OAM on the basis of enabled or disabled port and on the basis of active or passive port.

Examples

```
-> show efm-oam port
Port   EFM-OAM Status      Mode  Operational Status  Loopback Status
-------+---------------+---------+------------------+----------------
    1/1          enabled    active     operational           remoteLoopback
    1/2         disabled    active     activeSendLocal       noLoopback
    1/3          enabled   passive     activeSendLocal       noLoopback
    1/4         disabled    active     activeSendLocal       noLoopback
    1/5         disabled    active     activeSendLocal       noLoopback
    1/6         disabled    active     activeSendLocal       noLoopback
    1/7         disabled    active     activeSendLocal       noLoopback

-> show efm-oam port 1/1-5
Port   EFM-OAM Status      Mode  Operational Status  Loopback Status
-------+---------------+---------+------------------+----------------
    1/1          enabled    active     operational           remoteLoopback
    1/2         disabled    active     activeSendLocal       noLoopback
    1/3          enabled   passive     activeSendLocal       noLoopback
```

```
    1/4         disabled    active     activeSendLocal       noLoopback
    1/5         disabled    active     activeSendLocal       noLoopback

-> show efm-oam port 1/1-3 enabled
Port   Mode       Operational Status   Loopback Status
-------+---------------+---------+------------------+----------------
    1/1   active     operational          remoteLoopback
    1/3   passive    activeSendLocal      noLoopback

-> show efm-oam port enabled
Port         Mode  Operational Status  Loopback Status
---------+--------+------------------+----------------
   1/1      active     activeSendLocal   remoteLoopback
   1/3     passive     activeSendLocal       noLoopback
   1/7     passive     activeSendLocal       noLoopback

-> show efm-oam port disabled
Port         Mode  Operational Status  Loopback Status
---------+--------+------------------+----------------
   1/2      active     activeSendLocal       noLoopback
   1/4     passive     activeSendLocal       noLoopback
   1/5      active     activeSendLocal       noLoopback

-> show efm-oam port enabled passive
Port   Operational Status  Loopback Status
---------+--------+------------------+----------------
   1/3   activeSendLocal       noLoopback
   1/7   activeSendLocal       noLoopback

-> show efm-oam port active
Port   EFM-OAM Status   Operational Status  Loopback Status
------+---------------+--------------------+-------+---------------
    1/1    enabled         activeSendLocal      remoteLoopback
    1/2    disabled        activeSendLocal      noLoopback
    1/3    enabled         activeSendLocal      noLoopback
    1/4    disabled        activeSendLocal      noLoopback
    1/5    disabled        activeSendLocal      noLoopback
    1/6    disabled        activeSendLocal      noLoopback
    1/7    disabled        activeSendLocal      noLoopback
```

Output fields are described here:

output definitions

Port	Displays the slot/port number.
EFM-OAM Status	The state of the EFM-OAM. LINK OAM instance can have any of the following status. • **Enabled :** Specifies that the LINK OAM is disabled on the interface. • **Disabled** : Specifies that the LINK OAM is disabled on the interface.

output definitions (continued)

Operational Status	The status of the port in discovering whether the peer has LINK OAM capability or not.It has the following states: • **activeSendLocal**: Specifies that the LINK OAM port is actively trying to discover whether the peer has LINK OAM capability but has not yet made that determination. • **sendLocalAndRemote**: Specifies that the local LINK OAM port has discovered the peer but has not yet accepted or rejected the configuration of the peer. The local device will then decide that the peer device is acceptable or unacceptable and then accept or decline LINK OAM peering. • **sendLocalAndRemoteOk**: Specifies the state when LINK OAM peering is allowed by the local port. • **oamPeeringLocallyRejected**: Specifies the state when the local OAM entity rejects the peer OAM entity. • **oamPeeringRemotelyRejected**: Specifies the state when the remote LINK OAM port rejects the peering. • **operational**: Specifies the state when the local LINK OAM port learns that both the local LINK OAM entity and the remote LINK OAM entity have accepted the peering. • **nonOperHalfDuplex**: Specifies the value nonOperHalfDuplex is returned whenever LINK OAM is enabled. Since LINK OAM functions are not designed to work completely over half-duplex interfaces, the value nonOperHalfDuplex is returned whenever LINK OAM is enabled but the interface is in half-duplex operation. • **linkFault**: Specifies that the link between the host and the peer has detected a fault. • **passiveWait**: Specifies that the LINK OAM ports are in passive mode.
Loopback Status	The state of remote loopback. It can be **initiatingLoopback**, **terminatingLoopback**, **localLoopback**, **remoteLoopback, noLoopback**, or **unknown**.
Mode	The state of LINK OAM mode, **active** or **passive**.

Release History

Release 6.4.2; command was introduced.

Related Commands

efm-oam multiple-pdu-count	Configures the value of multiple PDU count. When multiple PDU count is set to a specific number in case of any of the threshhold cross events, the same event notification PDU will be transmitted that many times towards the peer.

MIB Objects

```
dot3OamTable
   dot3OamAdminState
   dot3OamMode
   dot3OamOperStatus
   dot3OamLoopbackTable
   dot3OamLoopbackStatus
```

show efm-oam port detail

Displays the LINK OAM configuration and other related parameters for a port.

show efm-oam port *slot/port* **detail**

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).

Defaults

N/A.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use this command when you want to get LINK OAM configuration details for a specific port.

Examples

```
-> show efm-oam port 1/1 detail
OAM Status                   : enable,
Operational Status           : activeSendLocal,
Mode                         : active,
Max OamPDU size              : 1518,
Config Revision              : 0,
Functions Supported          : loopback,event notification,
Loopback Status              : noLoopback,
Loopback Rx Status           : ignore,
Max OamPDUs                  : 10,
KeepAlive Interval(seconds)  : 10,
Hello Interval(seconds)      : 5,
Dying Gasp Notify Status     : enable,
Critical Event Notify Status : enable

    Link Monitoring             Window           Threshold       Notify
                                                  (errors)       Status
------------------+------------+-------------+------------+---------------
errored-frame                   10  dsec          10  frames       enable
errored-frame-period            2000000 frames    10  frames       enable
errored-frame-seconds-summary   600 dsec          1  framesec      enable
```

Output fields are described here:

output definitions

OAM Status	The state of LINK OAM on the port.
Operational Status	The state of the port in discovering whether the peer has LINK OAM capability or not.

output definitions (continued)

Mode	The state of LINK OAM mode on the port, **active** or **passive**.
Max OamPDU size	Displays the maximum OAMPDU that the LINK OAM port can support.
Config Revision	Displays the configuration revision of the LINK OAM port as reflected in the latest OAMPDU sent by the peer port.
Functions Supported	Displays the LINK OAM functions supported by the specified port.
Loopback Status	Displays the loopback status of the specified LINK OAM port.
Loopback Rx Status	The action that should be performed by the LINK OAM port when a loopback request is received from the peer port.
Max OamPDUs	Specifies the maximum OAMPDUs that can be exchanged between two peers.
KeepAlive Interval	Displays the timeout interval of the specified LINK OAM port for the dynamically learned peer port.
Hello Interval	Displays the time interval between two OAMPDUs in seconds.
Dying Gasp Notify Status	The state of notification for dying gasp events, **enable** or **disable**.
Critical Event Notify Status	The state of notification for critical events, **enable** or **disable.**
Link Monitoring	Displays the errors detected on the remote link.
Window	The frame error event window in the received OAMPDU.
Threshold	The number of errored frames in the period required for the event to be generated.
Notify Status	The state of notification for LINK OAM errors on the port, **enable** or **disable**.

Release History

Release 6.4.2; command was introduced.

Related Commands

show efm-oam port	Displays the status of LINK OAM on all the ports in the system, along with other relevant information like OAM mode, operational status and loopback status of the port.

MIB Objects

```
dot3OamTable
   dot3OamAdminState
   dot3OamOperStatus
   dot3OamMode
   dot3OamMaxOamPduSize
   dot3OamConfigRevision
   dot3OamFunctionsSupported
alaDot3OamTable
   alaDot3OamKeepAliveInterval
   alaDot3OamHelloInterval
dot3OamLoopbackTable
   dot3OamLoopbackStatus
```

```
   dot3OamLoopbackIgnoreRx
dot3OamEventConfigTable
   dot3OamDyingGaspEnable
   dot3OamCriticalEventEnable
   dot3OamErrFramePeriodWindow
   dot3OamErrFramePeriodThreshold
   dot3OamErrFramePeriodEvNotifEnable
   dot3OamErrFrameWindow
   dot3OamErrFrameThreshold
   dot3OamErrFrameEvNotifEnable
   dot3OamErrFrameSecsSummaryWindow
   dot3OamErrFrameSecsSummaryThreshold
   dot3OamErrFrameSecsEvNotifEnable
```

show efm-oam port statistics

Displays the LINK OAM statistics on a port, or a range of ports or on all ports.

show efm-oam port *slot/port***[**-*port2***] statistics**

show efm-oam port statistics

Syntax Definitions

slot/port	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).
-port2	The last port number in a range of ports that you want to configure on the same slot (e.g. 3/1-4 specifies ports 1,2,3, and 4 on slot 3).

Defaults

By default, the statistics of all ports are displayed.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the **port** parameter to display the statistics of a specific port.

Examples

```
-> show efm-oam port 1/1 statistics
Port 1/1:
  Information OAMPDU Tx                  : 1035,
  Information OAMPDU Rx                  : 988,
  Unique Event Notification OAMPDU Tx    : 0,
  Unique Event Notification OAMPDU Rx    : 0,
  Duplicate Event Notification OAMPDU TX : 0,
  Duplicate Event Notification OAMPDU Rx : 0,
  Loopback Control OAMPDU Tx             : 1,
  Loopback Control OAMPDU Rx             : 0,
  Unsupported OAMPDU Tx                  : 0,
  Unsupported OAMPDU Rx                  : 0,
  Frames Lost due to OAM                 : 0

-> show efm-oam port 1/1-4 statistics
Port 1/1:
  Information OAMPDU Tx                  : 1035,
  Information OAMPDU Rx                  : 988,
  Unique Event Notification OAMPDU Tx    : 0,
  Unique Event Notification OAMPDU Rx    : 0,
  Duplicate Event Notification OAMPDU TX : 0,
  Duplicate Event Notification OAMPDU Rx : 0,
  Loopback Control OAMPDU Tx             : 1,
  Loopback Control OAMPDU Rx             : 0,
  Unsupported OAMPDU Tx                  : 0,
```

```
  Unsupported OAMPDU Rx                  : 0,
  Frames Lost due to OAM                 : 0

Port 1/2:
  Information OAMPDU Tx                  : 1035,
  Information OAMPDU Rx                  : 988,
  Unique Event Notification OAMPDU Tx    : 0,
  Unique Event Notification OAMPDU Rx    : 0,
  Duplicate Event Notification OAMPDU Tx : 0,
  Duplicate Event Notification OAMPDU Rx : 0,
  Loopback Control OAMPDU Tx             : 1,
  Loopback Control OAMPDU Rx             : 0,
  Unsupported OAMPDU Tx                  : 0,
  Unsupported OAMPDU Rx                  : 0,
  Frames Lost due to OAM                 : 0

Port 1/3:
  Information OAMPDU Tx                  : 1035,
  Information OAMPDU Rx                  : 988,
  Unique Event Notification OAMPDU Tx    : 0,
  Unique Event Notification OAMPDU Rx    : 0,
  Duplicate Event Notification OAMPDU TX : 0,
  Duplicate Event Notification OAMPDU Rx : 0,
  Loopback Control OAMPDU Tx             : 1,
  Loopback Control OAMPDU Rx             : 0,
  Unsupported OAMPDU Tx                  : 0,
  Unsupported OAMPDU Rx                  : 0,
  Frames Lost due to OAM                 : 0

Port 1/4:
  Information OAMPDU Tx                  : 1035,
  Information OAMPDU Rx                  : 988,
  Unique Event Notification OAMPDU Tx    : 0,
  Unique Event Notification OAMPDU Rx    : 0,
  Duplicate Event Notification OAMPDU TX : 0,
  Duplicate Event Notification OAMPDU Rx : 0,
  Loopback Control OAMPDU Tx             : 1,
  Loopback Control OAMPDU Rx             : 0,
  Unsupported OAMPDU Tx                  : 0,
  Unsupported OAMPDU Rx                  : 0,
  Frames Lost due to OAM                 : 0


-> show efm-oam statistics
Port 1/1:
  Information OAMPDU Tx                  : 1035,
  Information OAMPDU Rx                  : 988,
  Unique Event Notification OAMPDU Tx    : 0,
  Unique Event Notification OAMPDU Rx    : 0,
  Duplicate Event Notification OAMPDU TX : 0,
  Duplicate Event Notification OAMPDU Rx : 0,
  Loopback Control OAMPDU Tx             : 1,
  Loopback Control OAMPDU Rx             : 0,
  Unsupported OAMPDU Tx                  : 0,
  Unsupported OAMPDU Rx                  : 0,
  Frames Lost due to OAM                 : 0

Port 1/2:
```

```
  Information OAMPDU Tx                  : 1035,
  Information OAMPDU Rx                  : 988,
  Unique Event Notification OAMPDU Tx    : 0,
  Unique Event Notification OAMPDU Rx    : 0,
  Duplicate Event Notification OAMPDU TX : 0,
  Duplicate Event Notification OAMPDU Rx : 0,
  Loopback Control OAMPDU Tx             : 1,
  Loopback Control OAMPDU Rx             : 0,
  Unsupported OAMPDU Tx                  : 0,
  Unsupported OAMPDU Rx                  : 0,
  Frames Lost due to OAM                 : 0

Port 1/3:
  Information OAMPDU Tx                  : 1035,
  Information OAMPDU Rx                  : 988,
  Unique Event Notification OAMPDU Tx    : 0,
  Unique Event Notification OAMPDU Rx    : 0,
  Duplicate Event Notification OAMPDU TX : 0,
  Duplicate Event Notification OAMPDU Rx : 0,
  Loopback Control OAMPDU Tx             : 1,
  Loopback Control OAMPDU Rx             : 0,
  Unsupported OAMPDU Tx                  : 0,
  Unsupported OAMPDU Rx                  : 0,
  Frames Lost due to OAM                 : 0
```

Output fields are described here:

output definitions

Information OAMPDU Tx	The number of OAM PDUx transmitted by the port.
Information OAMPDU Rx	The number of OAM PDUx received by the port.
Unique Event Notification OAMPDU Tx	The number of unique event notification OAM PDUs transmitted by the port.
Unique Event Notification OAMPDU Rx	The number of unique event notification OAM PDUs received by the port.
Duplicate Event Notification OAMPDU TX	The number of duplicate event notification OAM PDUs transmitted by the port.
Duplicate Event Notification OAMPDU Rx	The number of duplicate event notification OAM PDUs received by the port.
Unsupported OAMPDU Tx	The number of unsupported OAM PDUs transmitted by the port.
Unsupported OAMPDU Rx	The number of unsupported OAM PDUs received by the port.
Frames Lost due to OAM	The number of frames discarded by the OAM port.

Release History

Release 6.4.2; command was introduced.

Related Commands

show efm-oam port history	Displays the log of events that have occurred on a port. This command can also be used to display specific event logs on a port.

MIB Objects

```
dot3OamStatsTable
   dot3OamInformationTx
   dot3OamInformationRx
   dot3OamUniqueEventNotificationTx
   dot3OamUniqueEventNotificationRx
   dot3OamDuplicateEventNotificationTx
   dot3OamDuplicateEventNotificationRx
   dot3OamLoopbackControlTx
   dot3OamLoopbackControlRx
   dot3OamUnsupportedCodesTx
   dot3OamUnsupportedCodesRx
   dot3OamFramesLostDueToOam
```

show efm-oam port remote detail

Displays the LINK OAM configuration and details of the related parameters of the remote port.

show efm-oam port *slot/port* **remote detail**

Syntax Definitions

slot/port	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).

Defaults

N/A.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A.

Examples

```
-> show efm-oam port 1/1 remote detail
Remote MAC address  : 00:30:96:fd:6b:fa,
Remote Vendor (info): 0x15a1
Remote Vendor (oui) : XYZ
Mode                : active,
Max OAMPDU size     : 1518,
Config Revision     : 0,
Functions Supported : loopbackSupportEventSupport
```

Output fields are described here:

output definitions

Remote MAC address	Displays the MAC address of the remote peer.
Remote Vendor (info)	Displays the vendor number in hexadecimal of the remote peer.
Remote Vendor (oui)	Displays the Organizationally Unique Identifier (OUI) number of the remote peer.
Mode	The state of LINK OAM mode on the remote port, **active** or **passive**.
Max OAMPDU size	Displays the maximum OAMPDU size that the remote LINK OAM port can support.
Config Revision	Displays the configuration revision of the remote LINK OAM port.
Functions Supported	Displays the LINK OAM functions supported by the remote port.

Release History

Release 6.4.2; command was introduced.

Related Commands

show efm-oam port history	Displays the log of events that have occurred on a port. This command can also be used to display specific event logs on a port.
clear efm-oam statistics	Clears the LINK OAM statistics on a port.

MIB Objects

```
dot3OamPeerTable
   dot3OamPeerMacAddress
   dot3OamPeerVendorOui
   dot3OamPeerVendorInfo
   dot3OamPeerMode
   dot3OamPeerMaxOamPduSize
   dot3OamPeerConfigRevision
   dot3OamPeerFunctionsSupported
```

show efm-oam port history

Displays the log of events that have occurred on a port. Use this command to display specific event logs on a port.

show efm-oam port *slot/port* **history [log-type { link-fault | errored-frame | errored-frame-period | errored-frame-seconds | dying-gasp | critical }]**

Syntax Definitions

slot/port	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).
link-fault	Displays link fault event logs. Specifies the loss of signal is detected by the receiver. This is sent once per second in the Information OAMPDU
errored-frame	Displays errored-frame event log. an errored frame event occurs when the number of detected error frames over a specific interval exceeds the predefined threshold.
errored-frame-period	Displays an errored-frame-period event logs. An errored frame period event occurs if the number of frame errors in specific number of received frames exceeds the predefined threshold.
errored-frame-seconds	Displays errored-frame-seconds event logs. When the number of error frame seconds detected on a port over a detection interval reaches the error threshold, an errored frame seconds event occurs.
dying-gasp	Specifies an unrecoverable condition (e.g., a power failure).
critical	Specifies a crucial event that has occurred on the port.

Defaults

By default, all log types are displayed.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Timestamp will be in following format:

DAY MON Date hh:mm:ss yyyy

Examples

```
-> show efm-oam port 1/1 history
Legend: Location: * - Remote, # - Local
LogID   TimeStamp                Log Type          Event
                                                  Total
------+------------------------+-------------+-------+----+
*    1     TUE JAN 06 19:44:51 2009   linkFault       1
#    2     TUE JAN 06 19:45:51 2009   erroredFrame    1
```

```
-> show efm-oam port 1/1 history log-type link-fault
Legend: Location: * - Remote, # - Local
LogID   TimeStamp                    Event
                                     Total
-----+---------+---------+------+-----------+
*   1      TUE JAN 06 19:46:51 2009     1
#   2      TUE JAN 06 19:46:51 2009     1
```

Output fields are described here:

output definitions

LogID	Specifies individual events within the event log.
Timestamp	The value of actual time at the time of the logged event.
Log Type	Specifies the type of event log.
Event Total	Specifies the total number of times one or more of these occurrences have resulted in an Event Notification.

Release History

Release 6.4.2; command was introduced.

Related Commands

show efm-oam port statistics	Displays the LINK OAM statistics on a port, or a range of ports or on all ports.
clear efm-oam log-history	Clears the LINK OAM event logs history on a port.

MIB Objects

```
dot3OamEventLogTable
   dot3OamEventLogIndex
   dot3OamEventLogTimestamp
   dot3OamEventLogOui
   dot3OamEventLogType
   dot3OamEventLogLocation
   dot3OamEventLogWindowHi
   dot3OamEventLogWindowLo
   dot3OamEventLogThresholdHi
   dot3OamEventLogThresholdLo
   dot3OamEventLogValue
   dot3OamEventLogRunningTotal
   dot3OamEventLogEventTotal
```

show efm-oam port l1-ping detail

Displays the frames lost during a loopback session.

show efm-oam port *slot/port* **l1-ping detail**

Syntax Definitions

slot/port	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).

Defaults

N/A.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

The command can also be used even on a port on which LINK OAM is not enabled.

Examples

```
-> show efm-oam port 1/1 l1-ping detail
frames configured              = 5,
frames delay(msec)             = 100,
L1 ping status                 = Sucessful,
frames sent                    = 4,
frames received                = 4,
avg delay (msec)               = 5
-> show efm-oam port 1/4 l1-ping detail
frames configured              = 5,
frames delay(msec)             = 200,
L1 ping status                 = Successful,
frames sent                    = 4,
frames received                = 2,
avg delay (msec)               = 15
```

Output fields are described here:

output definitions

frames configured	Specifies the number of frames that are sent during l1-ping.
delay configured	Specifies the delay between transmission of two consecutive frames during L1 ping.
L1 ping status	The status of the L1 ping operation. The status can be **Successful**, **Unsuccessful** or **default.**
frames sent	Specifies the frames sent during last L1 ping.
frames received	Specifies the frames received during last L1 ping.
average delay	Specifies the average delay taken by frames during last L1 ping.

Release History

Release 6.4.2; command was introduced.

Related Commands

efm-oam port l1-ping	Configures the number of frames that needs to be sent during L1-ping, the delay between each consecutive sent frames and to start the L1-ping operation.

MIB Objects

```
alaDot3OamLoopbackTable
   alaDot3OamPortL1PingFramesConf
   alaDot3OamPortL1PingFramesDelay
   alaDot3OamPortL1PingStatus
   alaDot3OamPortL1PingFramesSent
   alaDot3OamPortL1PingFramesReceived
   alaDot3OamPortL1PingAverageRoundTripDelay
```

clear efm-oam statistics

Clears the LINK OAM statistics on a port, range of ports or all ports.

clear efm-oam statistics *port slot/port***[***-port2***]**

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).
-port2	Specifies the last port in the range of ports.

Defaults

By default, the statistics are cleared for all the ports if no port is specified in the command.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the port parameter with this command to clear the statistics for a specific port or range of ports.

Examples

```
-> clear efm-oam statistics
-> clear efm-oam statistics port 1/1
-> clear efm-oam statistics port 2/1-3
```

Release History

Release 6.4.2; command was introduced.

Related Commands

show efm-oam port statistics	Displays the LINK OAM statistics on a port, or a range of ports or on all ports.
clear efm-oam log-history	Clears the LINK OAM event logs history on a port.

MIB Objects

```
alaDot3OamGlobalClearStats
   alaDot3OamStatsTable
   alaDot3OamPortClearStats
```

clear efm-oam log-history

Clears the LINK OAM event logs history a port, range of ports or all ports.

clear efm-oam log-history *port slot/port***[***-port2***]**

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).
-port2	Specifies the last port in the range of ports.

Defaults

By default, the event logs are cleared for all the ports if no port is specified in the command.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the port parameter with this command to clear the statistics for a specific port or range of ports.

Examples

```
-> clear efm-oam log-history
-> clear efm-oam log-history port 1/1
-> clear efm-oam log-history port 2/1-3
```

Release History

Release 6.4.2; command was introduced.

Related Commands

show efm-oam port statistics	Displays the LINK OAM statistics on a port, or a range of ports or on all ports.
show efm-oam port history	Displays the log of events that have occurred on a port. Use this command to display specific event logs on a port.

MIB Objects

```
alaDot3OamGlobalClearEventLogs
   alaDot3OamEventLogTable
   alaDot3OamPortClearEventLogs
```

53 Service Assurance Agent Commands

Service Assurance Agent (SAA) enables customers to assure new business-critical applications, as well as services that utilize data, voice, and video.

With Service Assurance Agents, users can verify service guarantees, increase network reliability by validating network performance, proactively identify network issues, and increase return on investment (ROI) by easing the deployment of new services. Service Assurance Agent uses active monitoring to generate traffic in a continuous, reliable, and predictable manner, thus enabling the measurement of network performance and health.

IP SAAs enhance the service level monitoring to become IP application-aware by measuring both end-to-end and at the IP layer. IP SAA would allow performance measurement against any IP addresses in the network (switch, server, pc). ETH-LB/DMM can be used to measure delay and jitter by sending out frames with DM information to the peer MEP and receiving frames with DM information from the peer MEP.

MIB information for the SAA commands is as follows:

Filename: AlcatelIND1Eoam.MIB
Module: Alcatel-IND1-ETHERNET-OAM-MIB

Filename: IETF_802_1ag.MIB
Module: IEEE8021-CFM-MIB

Filename: Alcatel-IND1-SAA-MIB.MIB
Module: ALCATEL-IND1-SAA-MIB

A summary of the available commands is listed here:

EthOAM SAA Configuration Commands	**saa** **saa type ethoamloopback** **saa type ethoam-two-way-delay** **saa start** **saa stop**
IP SAA Configuration Command	**saa type ip-ping**
Layer 2 SAA Configuration Command	**saa type mac-ping**
EthOAM SAA Show Commands	**show saa** **show saa type config** **show saa statistics** **show saa statistics history index**

saa

Configures a Service Assurance Agent (SAA).

saa *string* **[descr** *description***] [interval** *interval***]**

no saa *string*

Syntax Definitions

string	SAA ID string up to 32 characters. Use quotes around string if SAA ID contains multiple words with spaces between them (e.g. “SAA 10”).
description	Text string up to 32 characters. Use quotes around string if description contains multiple words with spaces between them (e.g. “Alcatel-Lucent Marketing SAA”).
interval	The amount of time, in minutes, between two iterations of the SAA test. Valid range is from 1, 2, 5, 10 to 1500.

Defaults

parameter	default
description	DEFAULT
interval	150

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to remove an SAA from the switch configuration. Note that the SAA must be stopped before it can be deleted.
- The **desc** and **interval** parameters are optional. If these values are specified, the SAA is created with those values. If these values are not specified, the SAA is created with the default values.
- If the **desc** and/or **interval** parameters are specified for an existing SAA, then the values of the existing parameters are updated with those specified.
- If the session time interval is changed for an SAA that is already running and active, the interval value is immediately updated in the database but is not applied to the SAA until after the next iteration.
- If none of the optional parameters are specified and the given SAA already exists, the CLI will return an error message, as duplicate entries are not allowed.
- A maximum of 50 SAAs is recommended if the same interval value is configured (for example, the default of 10 minutes) for all the SAAs. If more than 50 are configured with the same interval value and all of them are started together, then the SAAs may not be scheduled exactly after the specified time interval. In this scenario, each SAA is scheduled only after all the other SAAs that are ahead of it in the scheduler. If the SAAs are configured with random interval values (values that are not multiples of other SAA values), then configuring more than 50 is allowed.

Examples

```
-> saa saa1 descr “saa for ip-ping”
-> saa saa2 descr “Monitoring Default VRF-interface” interval 160
-> saa saa2 interval 120
-> no saa saa1
```

Release History

Release 6.4.3; command was introduced.

Related Commands

show saa	Displays SAA configuration information.
show saa statistics	Displays SAA statistics.

MIB Objects

```
alaSaaCtrlTable
   alaSaaCtrlTestIndex
   alaSaaCtrlRowStatus
   alaSaaCtrlDescr
   alaSaaCtrlInterval
```

saa type ip-ping

Configure SAA for IP including the number of packets and inter-packet delay parameters.

saa *string* **type ip-ping destination-ip** *ipv4 addr* **source-ip** *ipv4 addr* **type-of-service** *tos* **[num-pkts** *count***] [inter-pkt-delay** *delay***] [payload-size** *size***]**

Syntax Definitions

string	SAA ID string up to 32 characters. Use quotes around string if SAA ID contains multiple words with spaces between them (e.g. “SAA 10”).
ipv4 addr	The IPv4 address of the destination to ping.
ipv4 addr	The IPv4 address of the source.
tos	The type of service.Valid range is 0 – 255.
count	The number of packets to send in one ping iteration. Valid range is 1–100.
delay	The delay between packets sent during a ping iteration, in milliseconds. Valid range is from 100ms to 1000ms in multiples of 100ms.
size	The size of the ICMP payload to be used for the ping iteration. Valid range is 24–1472 bytes.

Defaults

parameter	default
count	5
delay	1000ms
size	24 bytes

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The **num-pkts**, **inter-pkt-delay** and **payload-size** are optional parameters. If these values are specified, the SAA is created with the values entered. If none of them are specified, the SAA is created with the default values. The **num-pkts** and **inter-pkt-delay** can be modified, but **payload-size** cannot be modified later.
- The SAA must not be in a ‘started’ state at the time the **num-pkts** or **inter-pkt-delay** parameters are modified. Make sure the SAA is stopped before attempting to modify these parameters.
- The SAA must exist before issuing the CLI. If the SAA does not exist, the CLI will return an error.
- Do not specify a broadcast or multicast address for the source or destination IP. In addition, do not use 0.0.0.0 as the destination IP address.

- The timeout for each ping request packet is one second. This value is not configurable.

Examples

```
-> saa saa1 type ip-ping destination-ip 123.32.45.76 source-ip 123.35.42.124 type-
of-service 4
-> saa saa2 type ip-ping destination-ip 123.32.45.77 source-ip 123.35.42.124 type-
of-service 5
-> saa saa3 type ip-ping destination-ip 123.32.55.27 source-ip 123.35.42.125 type-
of-service 8 inter-pkt-delay 1000
-> saa saa4 type ip-ping destination-ip 123.46.45.77 source-ip 123.35.42.125 type-
of-service 2 num-pkts 5
-> saa saa5 type ip-ping destination-ip 12.53.45.77 source-ip 123.35.42.125 type-
of-service 35 payload-size 1518
-> saa saa6 type ip-ping destination-ip 123.22.45.66 source-ip 123.35.42.125 type-
of-service 5 inter-pkt-delay 1500 num-pkts 8 pkt-size 1000
```

Release History

Release 6.4.3; command was introduced.

Related Commands

show saa	Displays SAA configuration information.
show saa statistics	Displays SAA statistics.

MIB Objects

```
alaSaaIpCtrlTable
   alaSaaIpCtrlTestIndex
   alaSaaIpCtrlRowStatus
   alaSaaIpCtrlTestMode
   alaSaaIpCtrlTgtAddress
   alaSaaIpCtrlSrcAddress
   alaSaaIpCtrlTypeOfService
   alaSaaIpCtrlInterPktDelay
   alaSaaIpCtrlPayloadSize
   alaSaaIpCtrlNumPkts
```

saa type ethoamloopback

Configures the SAA for ETH-LB, including the number of packets and inter-packet delay parameters.

saa *string* **type ethoam-loopback {target-endpoint** *tmep_id* **| target-mac address** *mac***} source-endpoint** *smep_id* **domain** *domain* **association** *assoc* **vlan-priority** *priority* **[drop-eligible {true | false}] [data** *data***] [num-pkts** *num***] [inter-pkt-delay** *delay***]**

Syntax Definitions

string	SAA ID string up to 32 characters. Use quotes around string if SAA ID contains multiple words with spaces between them (e.g. “SAA 10”).
tmep-id	The ID of the destination MEP
mac	The MAC address of the destination.
smep-id	The ID of the source MEP.
domain	The domain to which the source MEP belongs.
assoc	The association to which the source MEP belongs.
priority	The VLAN priority to be used for the outgoing packet. Valid range is 0 – 7.
drop-eligible true	Sets the drop enable bit in the VLAN tag of the outgoing packet to true.
drop-eligible false	Sets the drop enable bit in the VLAN tag of the outgoing packet to false.
data	User specified string that is included in the packet.
delay	The delay between packets sent during a ping iteration in milliseconds. Valid range is 100ms - 1000ms in multiples of 100ms.
num	The number of packets to be sent during loopback. Valid range is 1 - 10.

Defaults

parameter	default
drop-eligible true | false	false
num-pkts	5
delay	1000

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The SAA must exist before issuing the CLI. If the SAA does not exist, the CLI will return error.
- Source MEP-ID, MD and MA must be created before initiating loopback.

- If the source MEP-Id/MA/MD does not exist, the configuration will be accepted and no error will be returned.
- When **target-endpoint** is specified then it must be learned before initiating loopback.
- When **target-endpoint** is specified and learned, Ethernet Loopback will be transmitted irrespective of whether the RMEP state is OK or failed.
- The **drop-eligible**, **data**, **num-pkts** and **inter-pkt-delay** are optional parameters. If these values are specified, the entry will be created with these values. If none of them are specified, the SAA will be created with default values. The **num-pkts** and **inter-pkt-delay** can be modified later.
- The SAA must not be in a 'started' state at the time the **num-pkts** or **inter-pkt-delay** parameters are modified. Make sure the SAA is stopped before attempting to modify these parameters.
- The Target MEP/MAC, source MEP, domain, association and priority parameters are mandatory. If they are not specified, the CLI will return an error.
- The **data** parameter is optional. If this parameter is not specified, then it is not sent in the loopback message.
- The timeout value for each LB packet is one second. This value is not configurable.

Examples

```
-> saa saa1 type ethoam-loopback target-endpoint 10 source endpoint 1 domain md1
association ma1 vlan-priority 5 drop-eligible false
-> saa saa2 type ethoam-loopback target-endpoint 10 source endpoint 2 domain md1
association ma1 vlan-priority 5 drop-eligible true data « monitor association ma1 »
num-pkts 6 inter-pkt-delay 500
-> saa saa3 type ethoam-loopback target-endpoint 15 source endpoint 1 domain md1
association ma1 vlan-priority 5 drop-eligible false data « monitor association ma1
» num-pkts 6
-> saa saa4 type ethoam-loopback target-endpoint 10 source endpoint 2 domain md1
association ma1 vlan-priority 5 drop-eligible true inter-pkt-delay 500
```

Release History

Release 6.4.3; command was introduced.

Related Commands

show saa	Displays SAA configuration information.
show saa statistics	Displays SAA statistics.

MIB Objects

```
alaSaaEthoamCtrlTable
   alaSaaEthoamCtrlTestIndex
   alaSaaEthoamCtrlRowStatus
   alaSaaEthoamCtrlTestMode
   alaSaaEthoamCtrlTgtMAC
   alaSaaEthoamCtrlSrcMepId
   alaSaaEthoamCtrlDomainName
   alaSaaEthoamCtrlAssociationName
   alaSaaEthoamCtrlNumPkts
   alaSaaEthoamCtrlInterPktDelay
```

```
alaSaaEthoamCtrlPktData
alaSaaEthoamCtrlVlanPriority
```

saa type ethoam-two-way-delay

Configures SAA for two-way Ethernet frame delay measurement (ETH-DM).

saa *string* **type {ethoam-two-way-delay} {target-endpoint** *tmep_id* **| target-mac address** *mac***} source-endpoint** *smep_id* **domain** *domain* **association** *assoc* **vlan-priority** *priority* **[num-pkts** *num***] [inter-pkt-delay** *delay***]**

Syntax Definitions

string	SAA ID string up to 32 characters. Use quotes around string if SAA ID contains multiple words with spaces between them (e.g. “SAA 10”).
tmep-id	The ID of the destination MEP.
mac	The MAC address of the destination.
smep-id	The ID of the source MEP.
domain	The domain to which the source MEP belongs.
assoc	The association to which the source MEP belongs.
priority	The VLAN priority to be used for the outgoing packet. Valid range is 0– 7.
delay	The delay between packets sent during a ping iteration, in milliseconds. Valid range is 100ms - 1000ms in multiples of 100ms.
num	The number of packets to be sent during loopback. Valid range is 1–10.

Defaults

parameter	default
num	5
delay	1000

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The SAA must exist before issuing the CLI. If the SAA does not exist, the CLI will return an error.
- The source MEP-ID, MD and MA must be created before initiating two-way ETH-DM.
- If the source MEP-ID/MA/MD does not exist, the configuration is still accepted and no error is returned.
- When the **target-endpoint** parameter is specified, then it must be learned before initiating two-way ETH-DM.

- When the **target-endpoint** parameter is specified and learned, two-way ETH-DM will transmit delay measurement message (DMM) frames and delay measurement reply (DMR) frames whether or not the RMEP state is OK.
- The **num-pkts** and **inter-pkt-delay** parameters are optional. If these values are specified, the entry will be created with those values. If none of them are specified, the SAA will be created with default values. The **num-pkts** and **inter-pkt-delay** values can be modified, but the **pkt-size** value cannot be modified later.
- The SAA must not be in a 'started' state at the time the **num-pkts** or **inter-pkt-delay** parameters are modified. Make sure the SAA is stopped before attempting to modify these parameters.
- Target MEP/MAC, source MEP, domain, association and priority parameters are mandatory. If they are not specified, the CLI will return an error.
- The timeout for each DMM packet is one second. This value is not configurable.

Examples

```
-> saa saa1 type ethoam-two-way-delay target-endpoint 10 source endpoint 1 domain
md1 association ma1 vlan-priority 5
-> saa saa2 type ethoam-two-way-delay target-endpoint 10 source endpoint 2 domain
md1 association ma1 vlan-priority 5 num-pkts 6 inter-pkt-delay 500
-> saa saa3 type ethoam-two-way-delay target-endpoint 15 source endpoint 1 domain
md1 association ma1 vlan-priority 5 num-pkts 6
-> saa saa4 type ethoam-two-way-delay target-endpoint 10 source endpoint 2 domain
md1 association ma1 vlan-priority 5 inter-pkt-delay 500
```

Release History

Release 6.4.3; command was introduced.

Related Commands

show saa	Displays SAA configuration information.
show saa statistics	Displays SAA statistics.

MIB Objects

```
alaSaaEthoamCtrlTable
   alaSaaEthoamCtrlTestIndex
   alaSaaEthoamCtrlRowStatus
   alaSaaEthoamCtrlTestMode
   alaSaaEthoamCtrlTgtMAC
   alaSaaEthoamCtrlSrcMepId
   alaSaaEthoamCtrlDomainName
   alaSaaEthoamCtrlAssociationName
   alaSaaEthoamCtrlNumPkts
   alaSaaEthoamCtrlInterPktDelay
   alaSaaEthoamCtrlVlanPriority
```

saa type mac-ping

Configure SAA for a MAC address including the VLAN, VLAN ID, number of packets and inter-packet delay parameters.

saa *string* **type mac-ping destination-macaddress** *mac* **vlan** *vlan-id* **[vlan-priority** *vlan-priority***] [drop-eligible** {**true** | **false**}**] [data** *data***] [num-pkts** *count***] [inter-pkt-delay** *delay***] [payload-size** *size***]**

Syntax Definitions

string	SAA ID string up to 32 characters. Use quotes around string if SAA ID contains multiple words with spaces between them (for example “SAA 10”).
mac	The destination MAC address to ping.
vlan-id	The VLAN on which the L2 SAA Packets will be sent out.Valid range is 1-4094.
vlan-priority	Specifies both the internal priority of the Mac ping and the 802.1p value on the vlan tag header. Valid range is 0-7.
true | **false**	Specifies both the internal drop precedence of the MAC ping and the CFI bit on the vlan tag header. Default is false.
data	User specified string to be included in the packet.
count	The number of packets to send in one ping iteration. Valid range is 1–100.
delay	The delay between packets sent during a ping iteration, in milliseconds. Valid range is from 100 ms to 1000 ms in multiples of 100 ms.
size	The size of the ICMP payload to be used for the ping iteration. Valid range is 32–1500 bytes.

Defaults

parameter	default
vlan-priority	0
drop-eligible	false
count	5
delay	1000 ms
size	32 bytes

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The **num-pkts**, **inter-pkt-delay**, and **payload-size** are optional parameters. If these values are specified, the SAA is created with the values entered. If none of them are specified, the SAA is created with the default values. The **num-pkts** and **inter-pkt-delay** can be modified, but **payload-size** cannot be modified later.
- The **num-pkts** and **inter-pkt-delay** parameters can be configured only if the total execution time (number of packets * inter-pkt-delay) is less than 10 sec.
- The SAA must not be in a 'started' state at the time the **num-pkts** or **inter-pkt-delay** parameters are modified. Make sure the SAA is stopped before attempting to modify these parameters.
- The SAA must exist before issuing the CLI. If the SAA does not exist, the CLI will return an error.
- If data-TLV is specified & payload size is not specified, then payload size will be increased internally to accommodate the data TLV.
- If data TLV & payload size both are specified and payload size is less than [dataTLV + 32] bytes (for time-stamping and other packet info), then the CLI will be rejected.
- Destination-MAC cannot be broadcast/multicast address.
- Timeout for each ping request packet is 1 sec. This value is non-configurable.

Examples

```
-> saa saa1 type mac-ping destination-macaddress 00:11:11:11:11:11 vlan 10
-> saa saa2 type mac-ping destination-macaddress 00:11:11:11:11:11 vlan 10
data "test_data"
-> saa saa3 type mac-ping destination-macaddress 00:11:11:11:11:11 vlan 10
drop-eligible true
->saa saa4 type mac-ping destination-macaddress 00:11:11:11:11:11 vlan 10
inter-pkt-delay 100
-> saa saa5 type mac-ping destination-macaddress 00:11:11:11:11:11 vlan 10
num-pkts 10
-> saa saa6 type mac-ping destination-macaddress 00:11:11:11:11:11 vlan 10
payload-size 400
-> saa saa7 type mac-ping destination-macaddress 00:11:11:11:11:11 vlan 10
vlan-priority 3
-> saa saa8 type mac-ping destination-macaddress 00:11:11:11:11:11 vlan 10
data "asdf" drop-eligible true vlan-priority 3 num-pkts 4
```

Release History

Release 6.4.5; command was introduced.

Related Commands

show saa	Displays SAA configuration information.
show saa statistics	Displays SAA statistics.

MIB Objects

```
alaSaaMacCtrlTable
   alaSaaMacCtrlDstAddress
```

```
alaSaaMacCtrlVlan
alaSaaMacCtrlVlanPriority
alaSaaMacCtrlPktData
alaSaaMacCtrlDropEligible
alaSaaMacCtrlPayloadSize
alaSaaMacCtrlNumPkts
alaSaaMacCtrlInterPktDelay
```

saa start

Starts the SAA test.

saa *string* **start [at** *yyyy-mm-dd,hh:mm:ss.ds* | **in** *minutes***]**

Syntax Definitions

string	An existing SAA ID string.
yyyy-mm-dd,hh:mm:ss.ds	The date and time to start the SAA.
minutes	The amount of time, in minutes.

Defaults

By default, the SAA test is started immediately.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- An existing SAA with the SAA type configured must be specified with this command.
- Use the **saa stop** command to stop an SAA test that is already running.
- Use the **at** option to specify a date and time for the test to start.
- If an SAA is scheduled to start at a specified time and another **saa start** command with a different value is given before the specified time, the subsequent command will over-ride the previous command.
- If the **saa start** command is given after an SAA is started, then the CLI will return an error.
- If the IP Ping SAA is configured with a source IP that does not exist or is not active, then the packet is not transmitted and no error is returned. Swlogs are updated.
- ICMP must be enabled on the switch. If ICMP is disabled and an IP Ping SAA is started, then the iteration will timeout and will be treated as failed iteration.
- Immediately after a CMM restart (reboot or takeover), the command to start SAA will be accepted, but the actual execution of the iteration will start 5 minutes after the CMM restart.
- If the ETH-DM or ETH-LB SAA type was configured with a source MEP that does not exist or is not active (admin down), then the packet is not transmitted and no error is returned on the CLI console. Swlogs are updated.
- It is recommended that all the SAAs be rescheduled if the system time is changed.

Examples

```
-> saa saa2 start at 2009-09-12,09:00:00
-> saa saa4 start
```

Release History

Release 6.4.3; command was introduced.

Related Commands

show saa	Displays SAA configuration information.
show saa statistics	Displays SAA statistics.

MIB Objects

```
alaSaaCtrlTable
   alaSaaCtrlTestIndex
   alaSaaCtrlStartAt
```

saa stop

Stops the SAA test.

saa *string* **stop [never | at** *yyyy-mm-dd,hh:mm:ss.d*s**]**

Syntax Definitions

string	An existing SAA ID string.
never	Specifies that the SAA test will not be stopped unless the **saa stop** command is used with the **at** option.
*yyyy-mm-dd,hh:mm:ss.d*s	The date and time to stop the SAA test.

Defaults

By default, the test is stopped immediately.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- An existing SAA with the SAA type configured must be specified with this command.
- The SAA must be in a ‘started’ state before giving the command unless the start and stop times are scheduled. If the SAA is not in a ‘started’ state, the CLI will return an error.
- Use the **at** option to specify a date and time for the test to stop.
- If the **never** option is specified, the SAA test will keep on running until the **saa stop** command is entered again with the **at** option.
- If SAA test is stopped while it is running an iteration, the current iteration is pre-empted. The statistics and history are updated for the partial iteration run.
- If an SAA is scheduled to stop at a specified time and another **saa stop** command with a different value is given before the specified time, the subsequent command will over-ride the previous command.

Examples

```
-> saa saa1 stop
-> saa saa2 stop never
```

Release History

Release 6.4.3; command was introduced.

Related Commands

show saa	Displays SAA configuration information.
show saa statistics	Displays SAA statistics.

MIB Objects

```
alaSaaCtrlTable
   alaSaaCtrlTestIndex
   alaSaaCtrlStopAt
```

show saa

Displays SAA configuration information.

show saa [*string* | **{descr** *description***}]**

Syntax Definitions

string	An existing SAA ID string.
description	An existing SAA description string.

Defaults

By default, information is displayed for all configured SAAs.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the *string* or *description* parameter to display information for a specific SAA.

Examples

```
-> show saa saa31
Legend: eth-lb = ethoam-loopback
          : eth-dmm = ethoam-two-way-delay
SAA   Type    Status Interval(Min.) Time of Last-Run Last-Run Result Description
-----+------+-------+--------------+---------------+--------------+-----------
Saa31 ip-ping started  180        2010-01-12,21:30:05.0  failed      Datacenter1

-> show saa
Legend: eth-lb = ethoam-loopback
          : eth-dmm = ethoam-two-way-delay
SAA   Type   Status  Interval(Min.)Time of Last-Run   Last-Run Result  Description
-----+-------+--------+------------+-----------------+---------------+-----------
Saa20 ip-ping started  130         2010-01-15,09:31:53.0  success      DEFAULT
Saa31 ip-ping started  180         2010-01-12,21:30:05.0  failed       Datacenter1
Saa89 ip-ping stopped  180         2010-01-12,09:45:00.0  success      Datacenter5
Saa90 eth-lb  stopped  150         NOT RUN              undetermined   Ethernet LB
Saa95 eth-lb  stopped  300         2010-01-16,11:31:53.0  success      Ethernet LB1
Saa98 eth-dmm stopped  120         NOT RUN                failed       DEFAULT
Saa99 eth-dmm started  200         2010-01-16,15:20:05.0  success      Two way test
```

Output fields are described here:

output definitions

SAA	Displays the configured SAA ID.
Type	Displays the SAA type configured.
Status	Displays the current status of the configured SAA.

output definitions (continued)

Interval (Min.)	Displays the interval, in minutes, between two iterations of the SAA test.
Time of Last-Run	Displays the date and time when the SAA was last run.
Last-Run Result	Displays the result of the SAA when it was last run.
Description	Displays the name of the configured SAA.

Release History

Release 6.4.3; command was introduced.

Related Commands

saa	Configures an SAA.

MIB Objects

```
alaSaaCtrlTable
   alaSaaCtrlTestIndex
   alaSaaCtrlDescr
   alaSaaCtrlInterval
   alaSaaCtrlTestMode
   alaSaaCtrlLastRunTime
   alaSaaCtrlLastRunResult
   alaSaaCtrlAdminStatus
```

show saa type config

Displays the SAA configuration for the specified SAA type.

show saa [*string***] type {ip-ping | ethoam-loopback | ethoam-two-way-delay | mac-ping} config**

Syntax Definitions

string	An existing SAA ID string.
ip-ping	Displays IP Ping SAAs.
ethoam-loopback	Displays ETH-LB SAAs.
ethoam-two-way-delay	Displays ETH-DMM SAAs.
mac-ping	Displays MAC Ping SAAs.

Defaults

By default, all SAAs with the specified type are displayed.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the *string* parameter to display information for a specific SAA.
- If the SAA ID string specified does not match the specified SAA type, the CLI will return an error.

Examples

```
-> show saa type ip-ping config
SAA : saa20
  SAA-type            : ip-ping,
  Status              : started,
  Start At            : -
  Stop At             : 2010-02-08,12:00:00.0
  Description         : datacenter1,
  Interval(minutes)   : 130,
  Source-IP           : 0.0.0.0,              Destination-IP      : 172.21.161.65,
  Payload-Size (bytes): 24,                   Type-of-Service     : 0,
  Num-pkts            : 5,                    Inter-pkt-delay     : 1000
SAA : saa31
  SAA-type            : ip-ping,
  Status              : started,
  Start At            : -
  Stop At             : -
  Description         : datacenter8,
  Interval(minutes)   : 180,
  Source-IP           : 0.0.0.0,              Destination-IP      : 172.21.161.65,
  Payload-Size (bytes): 24,                   Type-of-Service     : 0,
  Num-pkts            : 5,                    Inter-pkt-delay     : 1000
SAA-ID : 81
```

```
  SAA-type            : ip-ping,
  Status              : stopped,
  Start At            : -
  Stop At             : -
  Description         : abcdsdfsdfsfs,
  Interval(minutes)   : 300,
  Source-IP           : 0.0.0.0,              Destination-IP      : 172.21.161.65,
  Payload-Size (bytes): 24,                   Type-of-Service     : 0,
  Num-pkts            : 5,                    Inter-pkt-delay     : 1000
SAA : saa82
SAA-type            : ip-ping,
  Status              : stopped,
  Start At            : 2010-02-09,11:00:00.0,
  Stop At             : -,
  Description         : abcdsdfsdfsfs,
  Interval(minutes)   : 300,
  Source-IP           : 0.0.0.0,              Destination-IP      : 172.21.161.65,
  Payload-Size (bytes): 24,                   Type-of-Service     : 0,
  Num-pkts            : 5,                    Inter-pkt-delay     : 1000

-> show saa “saa20” type ip-ping config
SAA : saa20
  SAA-type            : ip-ping,
  Status              : started,
  Start At            : -
  Stop At             : -
  Description         : datacenter1,
  Interval(minutes)   : 130,
  Source-IP           : 0.0.0.0,              Destination-IP      : 172.21.161.65,
  Payload-Size (bytes): 24,                   Type-of-Service     : 0,
  Num-pkts            : 5,                    Inter-pkt-delay     : 1000
```

Output fields are described here:

output definitions

SAA	Displays the configured SAA ID.
SAA-type	Displays the SAA type configured.
Status	Displays the current status of the configured SAA.
Start At	Displays the date and time when the SAA was start.
Stop At	Displays the date and time when the SAA was stopped.
Description	Displays the name of the configured SAA.
Interval (minutes)	Displays the interval, in minutes, between two iterations of the SAA test.
Source-IP	Displays the source IP address used to perform the ip-ping operation.
Destination-IP	Displays the destination IP address used to perform the ip-ping operation.
Payload-Size (bytes)	Displays the payload size used for ip-ping operation.
Type-of-Service	Displays the type of service assigned to the configured SAA.
Num-pkts	Displays the number of packets sent in each ping.
Inter-pkt-delay	Displays the delay between packets sent during a ping iteration.

```
-> show saa type ethoam-loopback config
Legend: Destination Mep: - = SAA configured with target mac-address
        Destination MAC: - = SAA configured with target mep-id
SAA : saa90
  SAA-type            : ethoam-loopback,
  Status              : started,
  Description         : SAA for ethernet-loopback,
  Interval(minutes)   : 300,
  Destination MAC     : -,
  Destination Mep     : 5,                    Source Mep      : 1,
  Domain              : alcatel,              Association     : ma1,
  Num-pkts           : 7,                  Inter-pkt-delay : 1000,
  Vlan-priority       : 2
SAA : saa99
  SAA-type            : ethoam-loopback,
  Status              : started,
  Description         : SAA for ethernet-loopback,
  Interval(minutes)   : 300,
  Destination MAC     : 00:d0:b2:12:3c:a5,
  Destination Mep     : -,                    Source Mep      : 5,
  Domain              : alcatel               Association     : ma2,
  Num-pkts           : 5,                  Inter-pkt-delay : 500,
  Vlan-priority   : 7

-> show saa type ethoam-two-way-delay config
Legend: Destination Mep: - = SAA configured with target mac-address
        Destination MAC: - = SAA configured with target mep-id
SAA : saa100
  SAA-type            : ethoam-two-way-delay,
  Status              : stopped,
  Description         : SAA for ethernet-two-way-test,
  Interval(minutes)   : 200,
  Destination MAC     : 00:d0:b2:12:3c:a5,
  Destination Mep     : -,                    Source Mep      : 4,
  Domain              : aricent               Association     : ma1,
  Num-pkts           : 5,                  Inter-pkt-delay : 500,
  Vlan-priority    : 4
SAA : saa110
  SAA-type            : ethoam-two-way-delay,
  Status              : started,
  Description         : SAA for ethernet-two-way-delay,
  Interval(minutes)   : 300,
  Destination MAC     : -,
  Destination Mep     : 5,                    Source Mep      : 1,
  Domain              : aricent               Association     : ma2,
  Num-pkts           : 7,                  Inter-pkt-delay : 800,
  Vlan-priority       : 5
```

Output fields are described here:

output definitions

SAA	Displays the configured SAA ID.
SAA-type	Displays the SAA type configured.
Status	Displays the current status of the configured SAA.
Description	Displays the name of the configured SAA.

output definitions (continued)

Interval (minutes)	Displays the interval, in minutes, between two iterations of the SAA test.
Destination MAC	Displays the destination MAC address.
Destination Mep	Displays the ID of the destination MEP.
Source Mep	Displays the ID of the source MEP.
Domain	Displays the domain to which the source MEP belongs.
Association	Displays the association to which the source MEP belongs.
Num-pkts	Displays the number of packets sent in one iteration of Eth-LB/DMM test.
Inter-pkt-delay	Displays the delay between packets sent during a Eth-LB/DMM iteration.
Vlan-priority	Displays the VLAN priority used for the outgoing packet.

Release History

Release 6.4.3; command was introduced.

Related Commands

saa type ip-ping	Configures an IP ping SAA.
saa type ethoamloopback	Configures an ETH-LB SAA.
saa type ethoam-two-way-delay	Configures an ETH-DMM SAA.

MIB Objects

```
alaSaaCtrlTable
   alaSaaCtrlTestIndex
   alaSaaCtrlDescr
   alaSaaCtrlInterval
   alaSaaCtrlTestMode
alaSaaIpCtrlTable
   alaSaaIpCtrlTgtAddress
   alaSaaIpCtrlSrcAddress
   alaSaaIpCtrlPayloadSize
   alaSaaIpCtrlTypeOfService
   alaSaaIpCtrlInterPktDelay
   alaSaaIpCtrlNumPkts
alaSaaEthoamCtrlTable
   alaSaaEthoamCtrlTestMode
   alaSaaEthoamCtrlAdminStatus
   alaSaaEthoamCtrlTgtMepId
   alaSaaEthoamCtrlTgtMAC
   alaSaaEthoamCtrlSrcMepId
   alaSaaEthoamCtrlNumPkts
   alaSaaEthoamCtrlInterPktDelay
```

show saa statistics

Display SAA statistics.

show saa [*string***] statistics [aggregate | history]**

Syntax Definitions

string	An existing SAA ID string.
aggregate	Displays aggregate results for the specified SAA.
history	Displays a results history for the specified SAA.

Defaults

By default, statistics are displayed for all SAAs and only for the most recent SAA test run.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- If the **aggregate** parameter is specified, then only the aggregate results are displayed.
- If the **history** parameter is specified, then only the history results are displayed.
- Since results are only kept for the last five iterations, using the **history** option displays only the last five iterations.
- Use the *string* parameter to display statistics for a specific SAA.
- Statistics and history do not persist across a switch reboot or takeover.

Examples

```
-> show saa statistics
Legend: eth-lb = ethoam-loopback
          : eth-dmm = ethoam-two-way-delay
Legend: - = Delay or jitter value not available
Latest Record:
SAA    Type     Time of Last-Run      RTT    RTT   RTT  Jitter Jitter Jitter Pack-
ets   Description
                                     Min    Avg   Max   Min    Avg    Max
Sent Rcvd
------+----------+-------------------------+------+------+------+------+
------+------+----+----+------------
saa1  ip-ping   2009-09-05,20:18:34.0  970   1067  1432   1     99    455
7    7    DEFAULT
saa2  ip-pin    2009-09-05,20:18:48.0  1022  1180  1914   0    349    892
7    7    DEFAULT
saa3  ip-ping   2009-09-05,20:19:15.0  1016  1583  3794   8    703   2767
  5    5  DEFAULT
saa4  eth-lb    2009-09-05,22:15:30.0   -      -    -     -     -      -
  8    0  DEFAULT
```

```
saa5  eth-lb    2009-09-05,22:30:40.0  1243  1537  2166   23    42    96
 6     6  DEFAULT
saa6  eth-dmm   2009-09-05,22:45:15.0  1563  2654  3574   15    27    173
  5    5  DEFAULT


SAA    Type     Time of Last-Run      RTT    RTT   RTT  Jitter Jitter  Jitter
Packets   Description
                                     Min    Avg   Max   Min   Avg      Max
Sent Rcvd
------+----------+-------------------------+------+------+------+------+
------+------+----+----+------------
saa1  ip-ping   2009-09-05,20:18:34.0  970   1067  1432   1     99     455
 7    7   DEFAULT
```

Output fields are described here:

output definitions

SAA	Displays the configured SAA ID.
Type	Displays the SAA type configured.
Time of Last-Run	Displays the date and time when the SAA was last run.
RTT Min	Displays the minimum round trip time among all the iterations of the SAA.
RTT Avg	Displays the average round trip time among all the iterations of the SAA.
RTT Max	Displays the maximum round trip time among all the iterations of the SAA.
Jitter Min	Displays the minimum jitter among all the iterations of the SAA.
Jitter Avg	Displays the average jitter among all the iterations of the SAA.
Jitter Max	Displays the maximum jitter among all the iterations of the SAA.
Packets Sent	Displays the number of packets sent during a single iteration.
Packets Rcvd	Displays the number of packets received during a single iteration.
Description	Displays the name of the configured SAA.

```
-> show saa statistics aggregate
Legend: eth-lb = ethoam-loopback
          : eth-dmm = ethoam-two-way-delay
Legend: - = Delay or jitter value not available
Aggregate Record:
  Type         Time of Last-Run       RTT    RTT    RTT   Jitter Jitter
Jitter  Packets  Description
                                     Min    Avg    Max    Min    Avg
 Max   Sent Rcvd
----------+------------------------+------+------+------+------+------+
------+----+----+------------
ip-ping     2009-09-05.20:28:34.0        970  1067   1432      1     99
   455    7    7 DEFAULT
ip-ping     2009-09-05,20:28:24.0       1007  1846   4737      0    917
  3730    7    7 DEFAULT
ip-ping     2009-09-05,20:28:16.0        989  1121   1546     16    164
```

```
   533    6    6 DEFAULT
ip-ping     2009-09-05,22:28:09.0       1006  1136   1696     10    284
   690    6    6 DEFAULT
ip-ping     2009-09-05,22:18:34.0        970  1067  1432       1     99
   455    7    7 DEFAULT

-> show saa statistics history
Legend: eth-lb = ethoam-loopback
          : eth-dmm = ethoam-two-way-delay
Legend: - = Delay or jitter value not available
History records SAA : saa1
  Type         Time of Last-Run       RTT    RTT    RTT   Jitter Jitter
Jitter  Packets  Description
                                     Min    Avg    Max    Min    Avg
 Max   Sent Rcvd
----------+------------------------+------+------+------+------+------+
------+----+----+------------
ip-ping     2009-09-05,20:18:34.0        970  1067  1432       1     99
   455    7    7 DEFAULT
ip-ping     2009-09-05,20:28:24.0       1007  1846  4737       0     917
   3730   7    7 DEFAULT
ip-ping     2009-09-05,20:28:16.0        989  1121  1546       16    164
   533    6    6 DEFAULT
ip-ping     2009-09-05,20:28:09.0       1006  1136  1696       10    284
   690    6    6 DEFAULT
ip-ping     2009-09-05,20:18:34.0        970  1067  1432       1     99
   455    7    7 DEFAULT
History records SAA : saa2
Type      Time of Last-Run          RTT   RTT    RTT   Jitter Jitter Jitter  Pack-
ets   Description
                                    Min   Avg    Max    Min   Avg    Max
Sent Rcvd
----------+------------------------+------+------+------+------+------+
-------+----+----+------------
ip-ping   TUE 2010-09-05,20:18:48.0  1022  1180  1914     0    349   892
 7   7    DEFAULT

History records SAA : saa3
Type      Time of Last-Run          RTT    RTT   RTT   Jitter  Jitter Jitter  Pack-
ets  Description
                                    Min   Avg     Max   Min    Avg    Max
Sent Rcvd
----------+------------------------+------+------+------+------+------+
------+----+----+------------
ip-ping  TUE 2010-09-05,20:19:15.0  1016  1583   3794    8    703   2767
5    5    DEFAULT

History records SAA : saa4
Type   Time of Last-Run           RTT   RTT   RTT   Jitter  Jitter  Jitter
Packets  Description
                                  Min   Avg   Max    Min     Avg    Max
Sent Rcvd
----------+------------------------+------+------+------+------+------+
------+----+----+------------
eth-lb   2010-09-05,22:15:30.0     986   1023  1145   40    56      132
8    8   DEFAULT
eth-lb      2010-09-05,22:30:40.0  1243  1537  2166   23    42      96
8    8   DEFAULT
```

```
History records SAA : saa5
Type     Time of Last-Run        RTT    RTT    RTT   Jitter Jitter Jitter
Packets    Description
                                 Min    Avg    Max    Min    Avg   Max
Sent Rcvd
----------+------------------------+------+------+------+------+------+
------+----+----+------------
eth-dmm  2009-09-05,22:45:15.0     1563  2654  3574   15    27      173
5     5  DEFAULT
```

Output fields are described here:

output definitions

Type	Displays the SAA type configured.
Time of Last-Run	Displays the date and time when the SAA was last run.
RTT Min	Displays the minimum round trip time among all the iterations of the SAA.
RTT Avg	Displays the average round trip time among all the iterations of the SAA.
RTT Max	Displays the maximum round trip time among all the iterations of the SAA.
Jitter Min	Displays the minimum jitter among all the iterations of the SAA.
Jitter Avg	Displays the average jitter among all the iterations of the SAA.
Jitter Max	Displays the maximum jitter among all the iterations of the SAA.
Packets Sent	Displays the number of packets sent during a single iteration.
Packets Rcvd	Displays the number of packets received during a single iteration.
Description	Displays the name of the configured SAA.

```
-> show saa saa1 statistics aggregate
SAA: saa1
  Total numbers of iterations          : 5
  Aggregated Record:
    Total Packets Sent                 : 33,
    Total Packets Recieved             : 33,
    Avg RTT-Min/Avg/Max (micro sec)    : 970/1252/4737,
    Avg Jitter-Min/Avg/Max (micro sec) : 0/309/3730,
Timestamp-Min RTT                    : 2009-10-05,10:15:30.0,
Timestamp-Max RTT                    : 2009-10-05,08:15:30.0,
Timestamp-Min Jitter                 : 2009-10-05,13:15:30.0,
Timestamp-Max Jitter                 : 2009-10-05,20:28:39.0

-> show saa saa10 statistics
SAA: saa10
  Total numbers of iterations : 5
  Latest Record:
    Time of Run                      : 2009-09-05,20:28:39.0,
    Total Packets Sent               : 5,
    Total Packets Recieved           : 5,
    RTT-Min/Avg/Max (micro sec)      : 995/1059/1310,
    Jitter-Min/Avg/Max (micro sec)   : 5/56/267

-> show saa saa4 statistics aggregate
```

```
SAA: saa4
  Total numbers of iterations   : 2
  Aggregated Record:
    Total Packets Sent                : 16,
    Total Packets Recieved            : 16,
    Avg RTT-Min/Avg/Max (micro sec)   : 790/1185/2654,
    Avg Jitter-Min/Avg/Max (micro sec) : 37/583/1257,
    Timestamp-Min RTT                 : 2009-10-05,10:15:30.0,
    Timestamp-Max RTT                 : 2009-10-05,08:15:30.0,
    Timestamp-Min Jitter              : 2009-10-05,13:15:30.0,
    Timestamp-Max Jitter              : 2009-10-05,09:30:39.0

-> show saa saa14 statistics
SAA: saa14
  Total numbers of iterations   : 5
  Latest Record:
    Time of Run                     : 2009-10-15,09:30:39.0,
    Total Packets Sent              : 10,
    Total Packets Received          : 8,
    RTT-Min/Avg/Max (micro sec)     : 882/1547/2175,
    Jitter-Min/Avg/Max (micro sec)  : 15/87/165
```

Release History

Release 6.4.3; command was introduced.

Related Commands

saa	Configures a SAA.

MIB Objects

```
alaSaaIpResultsTable
   alaSaaIpResultsPktsSent
   alaSaaIpResultsPktsRcvd
   alaSaaIpResultsRunResultReason
   alaSaaIpResultsRunTime
   alaSaaIpResultsMinRTT
   alaSaaIpResultsAvgRTT
   alaSaaIpResultsMaxRTT
   alaSaaIpResultsMinJitter
   alaSaaIpResultsAvgJitter
   alaSaaIpResultsMaxJitter
alaSaaEthoamResultsTable
   alaSaaEthoamResultsPktsSent
   alaSaaEthoamResultsPktsRcvd
   alaSaaEthoamResultsRunResultReason
   alaSaaEthoamResultsRunTime
   alaSaaEthoamResultsMinRTT
   alaSaaEthoamResultsAvgRTT
   alaSaaEthoamResultsMaxRTT
   alaSaaEthoamResultsMinJitter
   alaSaaEthoamResultsAvgJitter
   alaSaaEthoamResultsMaxJitter
```

```
alaSaaIpCtrlTable
   alaSaaIpCtrlTotalPktsSent
   alaSaaIpCtrlTotalPktsRcvd
   alaSaaIpCtrlMinRTT
   alaSaaIpCtrlAvgRTT
   alaSaaIpCtrlMaxRTT
   alaSaaIpCtrlMinJitter
   alaSaaIpCtrlAvgJitter
   alaSaaIpCtrlMaxJitter
alaSaaEthoamCtrlTable
   alaSaaEthoamCtrlTotalPktsRcvd
   alaSaaEthoamCtrlTotalPktsSent
   alaSaaEthoamCtrlMinRTT
   alaSaaEthoamCtrlAvgRTT
   alaSaaEthoamCtrlMaxRTT
   alaSaaEthoamCtrlMinJitter
   alaSaaEthoamCtrlAvgJitter
   alaSaaEthoamCtrlMaxJitter
```

show saa statistics history index

Displays the information for individual packets of an iteration.

show saa [*string***] statistics history index** *history-id*

Syntax Definitions

string	The saa-id for which history statistics are requested.
history-id	The index of the history entry for which the individual packet information is requested. Valid range is from 1 to 5.

Defaults

By default, statistics are displayed for all SAAs and only for the most recent SAA test run.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The CLI can be used to display the information of individual packets of an iteration.
- Since the history results of only the last five iterations are kept, history-id can range from 1 to 5.
- If SAA given by the user does not match any configured SAA, then the CLI will return an error.
- Statistics and history do not persist across a switch reboot or takeover.

Examples

```
show saa "saa25" statistics history index 2
Legend: - = Jitter value not available
Result                            : pass,
Reason                            : success,
RTT-Min/Avg/Max (micro sec)       : 376/390/401,
Jitter-Min/Avg/Max (micro sec)    : 0/7/13,
            Seq. No.     Time of Pkt Tx        RTT    Jitter
            --------+----------------------+-------+---------
               1     2009-01-19,19:15:14.0     376      -
               2     2009-01-19,19:15:15.0     389     13
               3     2009-01-19,19:15:16.0     389     0
               4     2009-01-19,19:15:17.0     401     12
               5     2009-01-19,19:15:18.0     395     6
```

Output fields are described here:

output definitions

Result	Displays the result of the MAC-Ping iteration.
Reason	Displays the reason for iteration failure and success.
RTT-Min/Avg/Max (micro sec)	Displays the minimum, average, and maximum round trip time the iteration was run.

output definitions (continued)

Jitter-Min/Avg/Max (micro sec)	Displays the minimum, average, and maximum jitter value.
Seq. No.	Displays the sequence in which the iteration was run.
Time of Pkt Tx	Displays the date and time at which the iteraton was run.
RTT	Displays the round trip time taken by a single packet in an iteration.
Jitter	Displays the jitter value, in micro-seconds, for a single packet in an iteration.

Release History

Release 6.4.5; command was introduced.

Related Commands

saa	Configures a SAA.

MIB Objects

```
alaSaaMacHistoryTable
   alaSaaMacHistoryPktRTT
   alaSaaMacHistoryPktJitter
```

54 MPLS LDP Commands

The LDP (Label Distribution Protocol) is used to set up Label Switched Paths (LSPs), also referred to as Multiprotocol Label Switching (MPLS) tunnels. These tunnels are used to connect customer sites over a service provider network and form the basis of any multipoint service, such as a Virtual Private LAN Service (VPLS).

In addition to using LDP, configuring static LSPs is also supported. Both LDP and static LSPs provide the label switching mechanism required by MPLS. For more information about static LSPs, see the "Static LSP and FRR Commands" chapter in this guide.

MIB information for the LDP commands is as follows:

Filename: TIMETRA-LDP-MIB.mib
Module: TIMETRA-LDP-MIB

Filename: AlcatelIND1ServiceMgr.MIB
Module: Alcatel-IND1-SERVICE-MGR-MIB

A summary of the available commands is listed here:

Global Commands	**configure router ldp shutdown** **show router ldp parameters** **show router ldp peer** **show router ldp session** **show router ldp status**
Interface Commands	**configure router ldp interface-parameters interface** **configure router ldp interface-parameters interface shutdown** **configure router ldp interface-parameters hello** **configure router ldp interface-parameters keepalive** **configure router ldp interface-parameters transport-address** **show router ldp interface**
Targeted Session Commands	**configure router ldp targeted-session hello** **configure router ldp targeted-session keepalive**
Graceful Restart Commands	**configure router ldp graceful-restart-helper** **configure router ldp reconnect-time** **configure router ldp fwd-state-holding-time** **configure router ldp maximum-recovery-time** **configure router ldp neighbor-liveness-time**
LSP Ping and Traceroute Commands	**oam lsp-ping** **oam lsp-trace**

Show LDP Bindings Commands	**show router ldp bindings** **show router ldp bindings fec-type** **show router ldp bindings ingress-label** **show router ldp bindings egress-label** **show router ldp bindings prefix** **show router ldp bindings active** **show router ldp bindings vc-type** **show router ldp bindings service-id**
Show LDP Discovery Commands	**show router ldp discovery** **show router ldp discovery peer** **show router ldp discovery interface**

configure router ldp shutdown

Configures the administrative status of the Label Distribution Protocol (LDP) instance on the router.

configure router ldp {no shutdown | shutdown}

Syntax Definitions

no shutdown	Enables the LDP administrative status on the router.
shutdown	Disables the LDP administrative status on the router.

Defaults

By default, LDP is enabled for the switch.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Disabling the LDP administrative status also disables any associated Label Switch Paths (LSPs) and any Service Distribution Points (SDPs) that were attached to the LSPs.
- When LDP is disabled on the switch, attaching SDPs to any of the associated LSRs is not allowed.

Examples

```
-> configure router ldp shutdown
-> configure router ldp no shutdown
```

Release History

Release 6.4.2; command was introduced.

Related Commands

show router ldp status	Displays status information and statistics for the LDP instance on the local router.

MIB Objects

```
vRtrLdpGeneralTable
   vRtrLdpGenAdminState
```

configure router ldp interface-parameters interface

Configures LDP support on the specified IP interface.

configure router ldp interface-parameters interface *ip-intf-name*

configure router ldp interface-parameters no interface *ip-intf-name*

Syntax Definitions

ip-intf-name	The name of an existing IP interface.

Defaults

By default, the LDP interface is administratively enabled when the interface is created.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to remove the LDP configuration from the IP interface. Disable the administrative status of the interface before attempting to remove it.
- The IP interface name specified with this command must already exist in the router configuration.
- Until LDP support is configured on an IP interface, no other LDP configuration tasks are allowed on that interface.

Examples

```
-> configure router ldp interface-parameters interface vlan-14
-> configure router ldp interface-parameters no interface vlan-14
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure router ldp interface-parameters interface shutdown	Configures the administrative status for the specified LDP interface.
show router ldp interface	Displays the LDP interface configuration for the router.
show router ldp parameters	Displays global LDP parameter values for the router.

MIB Objects

```
vRtrLdpIfTable
   vRtrID
   vRtrLdpIfIndex
   vRtrLdpPeerAddress
   vRtrLdpIfRowStatus
```

configure router ldp interface-parameters interface shutdown

Configures the administrative status for the specified LDP interface.

configure router ldp interface-parameters interface *ip-intf-name* **{no shutdown | shutdown}**

Syntax Definitions

ip-intf-name	The name of an existing LDP interface.
no shutdown	Enables the LDP administrative status for the interface.
shutdown	Disables the LDP administrative status for the interface.

Defaults

By default, the administrative status of an LDP interface is enabled.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Disabling the administrative status for an LDP interface does not remove the LDP configuration from that interface.
- The LDP interface name specified with this command must already exist in the router configuration.

Examples

```
-> configure router ldp interface-parameters interface vlan-14 shutdown
-> configure router ldp interface-parameters interface vlan-14 no shutdown
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure router ldp interface-parameters interface	Configures LDP support on an IP interface.
show router ldp interface	Displays the LDP interface configuration for the router.

MIB Objects

```
vRtrLdpIfTable
   vRtrID
   vRtrLdpIfIndex
   vRtrLdpPeerAddress
   vRtrLdpIfRowStatus
```

configure router ldp interface-parameters hello

Configures the hello timeout (also referred to as the hold time) and the hello interval on a global (all LDP interfaces) basis or on a per-interface basis. The hello timeout determines how long LDP waits to receive hello messages from a peer before declaring that the peer is down. The hello interval determines how often LDP sends out hello messages, which advertise the hello timeout.

configure router ldp interface-parameters [interface *ip-intf-name***] hello** *timeout factor*

configure router ldp interface-parameters [interface *ip-intf-name***] no hello**

Syntax Definitions

ip-intf-name	The name of an existing LDP interface.
timeout	The hello timeout, in seconds. The valid range is 1–65535 seconds.
factor	The number of hello messages to send during the hello timeout. The valid range is 1–255. The factor number is divided into the hello timeout to determine the hello interval value.

Defaults

By default, the hello time is set to 15 seconds and the factor number is set to 3, which results in a default hello interval time of 5 seconds.

parameter	default
ip-intf-name	All LDP interfaces.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to set the hello timeout and factor parameters to the default values for these parameters. Note that if an interface name is specified with the **no** form of this command, the default values applied are the values defined globally for all interfaces.
- Use the optional **interface** *ip-intf-name* parameter to configure the hello time and hello interval for a specific LDP interface. Note that the hello parameter values configured for an interface override the global configuration of these values for the router.
- LDP uses hello messages to establish adjacencies with LDP peers. If no hello messages are received from a peer during the hello time that is advertised by that peer, the local LDP router will consider the peer as down and will not retain the adjacency with that peer.
- When LDP is establishing an adjacency between two peers, the hold time is negotiated to the lower time value of the two peers. Once an operational value is agreed upon, the hold time is divided by the factor number to determine the interval at which the peers will send each other hello messages.

Examples

```
-> configure router ldp interface-parameters hello 40 2
-> configure router ldp interface-parameters interface vlan-14 hello 50 10
-> configure router ldp interface-parameters no hello
-> configure router ldp interface-parameters interface vlan-14 no hello
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure router ldp interface-parameters interface	Configures LDP support on an IP interface.
show router ldp parameters	Displays global LDP parameter values for the switch.
show router ldp interface	Displays the LDP interface configuration for the switch.

MIB Objects

```
vRtrLdpGeneralTable
   vRtrLdpGenHelloFactor
   vRtrLdpGenHelloTimeout
vRtrLdpIfTable
   vRtrID
   vRtrLdpIfIndex
   vRtrLdpPeerAddress
   vRtrLdpIfHelloFactor
   vRtrLdpIfHelloTimeout
```

configure router ldp interface-parameters keepalive

Configures the keepalive timeout and the keepalive interval on a global (all LDP interfaces) basis or on a per-interface basis. The keepalive timeout determines how long LDP waits to receive keepalive messages from an LDP peer before tearing down the session with that peer. The keepalive interval determines how often LDP sends out keepalive messages, which advertise the keepalive time.

configure router ldp interface-parameters [interface *ip-intf-name***] keepalive** *timeout factor*

configure router ldp interface-parameters [interface *ip-intf-name***] no keepalive**

Syntax Definitions

ip-intf-name	The name of an existing LDP interface.
timeout	The keepalive timeout, in seconds. The valid range is 1–65535 seconds.
factor	The number of keepalive messages to send during the keepalive time-out. The valid range is 1–255. The factor number is divided into the keepalive timeout to calculate the keepalive interval value.

Defaults

By default, the keepalive time is set to 30 seconds and the factor number is set to 3, which results in a default keepalive interval of 10 seconds.

parameter	default
ip-intf-name	All LDP interfaces.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to set the keepalive time and factor parameters to the default values for these parameters. Note that if an interface name is specified with the **no** form of this command, the default values applied are the values defined globally for all interfaces.
- Use the optional **interface** *ip-intf-name* parameter to configure the keepalive time and interval for a specific LDP interface. Note that the keepalive parameter values configured for an interface override the global configuration of these values for the router.
- When LDP is establishing a session between two peers, the keepalive time is negotiated to the lower time value of the two peers. Once an operational value is agreed upon, the keepalive time is divided by the factor number to determine the interval at which the peers will send each other keepalive messages.
- If no keepalive messages are received from a peer during the keepalive time that is advertised by that peer, the local LDP router will tear down the session.

Examples

```
-> configure router ldp interface-parameters keepalive 40 2
```

```
-> configure router ldp interface-parameters interface vlan-14 keepalive 50 10
-> configure router ldp interface-parameters no keepalive
-> configure router ldp interface-parameters interface vlan-14 no keepalive
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure router ldp interface-parameters interface	Configures LDP support on an IP interface.
show router ldp parameters	Displays global LDP parameter values for the switch.
show router ldp interface	Displays the LDP interface configuration for the switch.

MIB Objects

```
vRtrLdpGeneralTable
   vRtrLdpGenKeepAliveFactor
   vRtrLdpGenKeepAliveTimeout
vRtrLdpIfTable
   vRtrID
   vRtrLdpIfIndex
   vRtrLdpPeerAddress
   vRtrLdpIfKeepAliveFactor
   vRtrLdpIfKeepAliveTimeout
```

configure router ldp interface-parameters transport-address

Configures the transport address for the specified LDP interface. This address is used to set up LDP TCP sessions.

configure router ldp interface-parameters interface *ip-intf-name* **transport-address {system** | **interface}**

configure router ldp interface-parameters interface *ip-intf-name* **no transport-address**

Syntax Definitions

ip-intf-name	The name of an existing LDP interface.
system	Sets the transport address to the system IP address, which is the Loopback0 IP address configured for the OmniSwitch.
interface	Sets the transport address to the IP address of the specified LDP interface.

Defaults

By default, the transport address for the LDP session is set to the system IP (Loopback0) address.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to set the transport address to the default value (system IP).
- Do not use the interface IP address as the transport address if multiple interfaces exist between two LDP neighbors.

Examples

```
-> configure router ldp interface-parameters transport-address interface
-> configure router ldp interface-parameters interface vlan-14 transport-address
system
-> configure router ldp interface-parameters no transport-address
-> configure router ldp interface-parameters interface vlan-14 no transport-address
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure router ldp interface-parameters interface	Configures LDP support on an IP interface.
show router ldp parameters	Displays global LDP parameter values for the switch.
show router ldp interface	Displays the LDP interface configuration for the switch.

MIB Objects

```
vRtrLdpGeneralTable
   vRtrLdpGenKeepAliveFactor
   vRtrLdpGenKeepAliveTimeout
vRtrLdpIfTable
   vRtrID
   vRtrLdpIfIndex
   vRtrLdpPeerAddress
   vRtrLdpIfKeepAliveFactor
   vRtrLdpIfKeepAliveTimeout
```

configure router ldp targeted-session hello

Configures the hello time (also referred to as the hold time) and the hello interval for targeted LDP sessions. A targeted session is an LDP session that exists between two peers that are not directly connected to each other. The hello time determines how long LDP waits to receive hello messages from a peer before declaring that the peer is down. The hello interval determines how often LDP sends out hello messages, which advertise the hello time.

configure router ldp targeted-session hello *time factor*

configure router ldp targeted-session no hello

Syntax Definitions

time	The hello time, in seconds. The valid range is 1–65535 seconds.
factor	The number of hello messages to send during the hello time. The valid range is 1–255. The factor number is divided into the hello time to determine the hello interval value.

Defaults

By default, the hello time is set to 45 seconds and the factor number is set to 3, which results in a default hello interval time of 15 seconds.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to set the hello timeout and factor parameters to the default values for these parameters.
- Specify a hello time value that is more than three times the value of the hello interval (hello time divided by factor).
- LDP uses hello messages to establish adjacencies with LDP peers. These messages contain a locally-configured hello time. The hello hold time is the amount of time a peer retains hello adjacencies without receiving another hello message from the adjacent peer.
- When LDP is establishing a session between two peers, the hold time is negotiated to the lower time value of the two peers. Once an operational value is agreed upon, the hold time is divided by the factor number to determine the interval at which the peers will send each other hello messages.

Examples

```
-> configure router ldp targeted-session hello 20 2
-> configure router ldp interface-parameters no hello
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure router ldp interface-parameters hello	Configures the hello time (also referred to as the hold time) and the hello interval on a global (all LDP interfaces) basis or on a per-interface basis.
configure router ldp targeted-session keepalive	Configures the keepalive time and the keepalive interval for targeted LDP sessions.
show router ldp parameters	Displays the LDP graceful restart, interface, and targeted session parameter values for the local router.

MIB Objects

```
vRtrLdpGeneralTable
   vRtrLdpGenTargHelloFactor
   vRtrLdpGenTargHelloTimeout
```

configure router ldp targeted-session keepalive

Configures the keepalive time and the keepalive interval for targeted LDP sessions. The keepalive time determines how long LDP waits to receive keepalive messages from an LDP peer before tearing down the session with that peer. The keepalive interval determines how often LDP sends out keepalive messages, which advertise the keepalive time.

configure router ldp targeted-session keepalive *timeout factor*

configure router ldp targeted-session no keepalive

Syntax Definitions

timeout	The keepalive time, in seconds. The valid range is 1–65535 seconds.
factor	The number of keepalive messages to send during the keepalive time. The valid range is 1–255. The factor number is divided into the keepalive time to determine the keepalive interval value.

Defaults

By default, the keepalive time is set to 40 seconds and the factor number is set to 4, which results in a default keepalive interval of 10 seconds.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to set the keepalive time and factor parameters to the default values for these parameters.
- Specify a keepalive time value that is more than three times the value of the keepalive interval (keepalive time divided by factor).
- When LDP is establishing a session between two peers, the keepalive time is negotiated to the lower time value of the two peers. Once an operational value is agreed upon, the keepalive time is divided by the factor number to determine the interval at which the peers will send each other keepalive messages.
- If no keepalive messages are received from a peer during the keepalive time that is advertised by that peer, the local LDP router will tear down the session.

Examples

```
-> configure router ldp targeted-session keepalive 40 2
-> configure router ldp interface-parameters no keepalive
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure router ldp interface-parameters keepalive	Configures the keepalive time and the keepalive interval on a global (all LDP interfaces) basis or on a per-interface basis.
configure router ldp targeted-session hello	Configures the hello time and the hello interval for targeted LDP sessions.
show router ldp parameters	Displays the LDP graceful restart, interface, and targeted session parameter values for the local router.

MIB Objects

```
vRtrLdpGeneralTable
   vRtrLdpGenTargKeepAliveFactor
   vRtrLdpGenTargKeepAliveTimeout
```

configure router ldp graceful-restart-helper

Configures the graceful restart helper status for the LDP router. When enabled, the router includes a fault tolerant (FT) TLV in LDP initialization messages. This signals to other LDP routers that this router is able to help with the graceful restart process.

configure router ldp graceful-restart-helper

configure router ldp no graceful-restart-helper

Syntax Definitions

N/A.

Defaults

By default, the graceful restart helper status is disabled for the LSR.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to disable graceful restart helper for the switch.
- Graceful Restart support for LDP is always enabled on the router, so it is not necessary to enable restart support before enabling the helper status.
- Only takeover

Examples

```
-> configure router ldp graceful-restart-helper enable
-> configure router ldp no graceful-restart-helper disable
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure router ldp reconnect-time	Configures the Reconnect Timeout value in the fault tolerant (FT) Session TLV that is advertised in LDP messages.
configure router ldp fwd-state-holding-time	Configures the amount of time that the LDP router retains its MPLS forwarding state after a graceful restart.
configure router ldp maximum-recovery-time	Configures the amount of time the router retains stale MPLS label-FEC bindings received from a neighboring LDP router as the result of a graceful restart process.
configure router ldp neighbor-liveness-time	The amount of time the router will wait for a neighboring router to re-establish an LDP session.

MIB Objects

```
vRtrLdpGeneralTable
   vRtrLdpGenGracefulRestart
```

configure router ldp reconnect-time

Configures the Reconnect Timeout value in the fault tolerant (FT) Session TLV that is advertised in LDP messages. This timeout value specifies the amount of time, in seconds, that neighboring LDP routers should wait for the sender of the LDP message to gracefully restart and resume sending LDP messages to the neighbor.

configure router ldp reconnect-time *seconds*

configure router ldp no reconnect-time

Syntax Definitions

seconds	The Reconnect Timeout, in seconds. The valid range is from 0–300.

Defaults

By default, the Reconnect Timeout is set to 120 seconds.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to set the Reconnect Timeout to the default value.
- An LDP router starts the reconnect timer when it first detects a loss of LDP communications with a peer router. The timer value is that advertised by the peer router in the FT session TLV of LDP messages sent by the peer.
- Setting the Reconnect Timeout value to zero indicates to peer routers that the local LDP router will not retain its forwarding state across a graceful restart.

Examples

```
-> configure router ldp reconnect-time 300
-> configure router ldp no reconnect-time
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure router ldp graceful-restart-helper	Configures the graceful restart helper status for the LDP router.
configure router ldp fwd-state-holding-time	Configures the amount of time that the LDP router retains its MPLS forwarding state after a graceful restart.
configure router ldp maximum-recovery-time	Configures the amount of time the router retains stale MPLS label-FEC bindings received from a neighboring LDP router as the result of a graceful restart process.
configure router ldp neighbor-liveness-time	The amount of time the router will wait for a neighboring router to re-establish an LDP session.

MIB Objects

```
alaVRtrExtendedLdpGeneralTable
   vRtrLdpGenGRReconnectTime
```

configure router ldp fwd-state-holding-time

Configures the MPLS Forwarding State Holding timer value for the local LDP router. This time value specifies the amount of time, in seconds, that the LDP router retains its MPLS forwarding state after a graceful restart.

configure router ldp fwd-state-holding-time *seconds*

configure router ldp no fwd-state-holding-time

Syntax Definitions

seconds	The Forwarding State Holding timer value, in seconds. The valid range is from 5–300.

Defaults

By default, the MPLS Forwarding State Holding time is set to 120 seconds.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to set the Forwarding State Holding timer to the default value.
- This timer is started if the MPLS forwarding state of the restarting router was preserved after a graceful restart. The router then marks the forwarding entries as “stale” for the length of this time value. When the timer expires, any entries that are still marked as stale are deleted.
- An LDP router is considered in the process of restarting if the Forwarding State Holding timer is still active. When the end of this holding time is reached, the restart process is considered complete for the router.
- The Recovery Time advertised in the FT Session TLV of the LDP message is set to the current value of the Forwarding State Holding timer at the time the message is sent. If the router did not retain its MPLS forwarding state after a restart, then the Recovery Time is set to zero.

Examples

```
-> configure router ldp fwd-state-holding-time 300
-> configure router ldp no fwd-state-holding-time
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure router ldp graceful-restart-helper	Configures the graceful restart helper status for the LDP router.
configure router ldp reconnect-time	Configures the Reconnect Timeout value in the fault tolerant (FT) Session TLV that is advertised in LDP messages.
configure router ldp maximum-recovery-time	Configures the amount of time the router retains stale MPLS label-FEC bindings received from a neighboring LDP router as the result of a graceful restart process.
configure router ldp neighbor-liveness-time	The amount of time the router will wait for a neighboring router to re-establish an LDP session.

MIB Objects

```
alaVRtrExtendedLdpGeneralTable
   vRtrLdpGenGRFwdStateHoldTime
```

configure router ldp maximum-recovery-time

Configures the Maximum Recovery Time value for the local LDP router. This time value specifies the amount of time the router retains stale MPLS label-forwarding equivalence class (FEC) bindings received from a neighboring LDP router as the result of a graceful restart process.

configure router ldp maximum-recovery-time *seconds*

configure router ldp no maximum-recovery-time

Syntax Definitions

seconds	The Maximum Recovery Time value, in seconds. The valid range is from 15–1800.

Defaults

By default, the Maximum Recovery Time is set to 120 seconds.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to set the Maximum Recovery Time to the default value.
- If the neighboring router advertises a Recovery Time that is less than the local Maximum Recovery Time value, then the local router applies the Recovery Time to the stale label-FEC bindings it receives from that same router instead of the Maximum Recovery time value.

Examples

```
-> configure router ldp maximum-recovery-time 300
-> configure router ldp no maximum-recovery-time
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure router ldp graceful-restart-helper	Configures the graceful restart helper status for the LDP router.
configure router ldp fwd-state-holding-time	Configures the amount of time that the LDP router retains its MPLS forwarding state after a graceful restart.
configure router ldp reconnect-time	Configures the Reconnect Timeout value in the fault tolerant (FT) Session TLV that is advertised in LDP messages.
configure router ldp neighbor-liveness-time	The amount of time the router will wait for a neighboring router to re-establish an LDP session.

MIB Objects

```
vRtrLdpGeneralTable
   vRtrLdpGenGRMaxRecoveryTime
```

configure router ldp neighbor-liveness-time

Configures the Neighbor Liveness Time value for the local LDP router. This timer value specifies the amount of time the router will wait for a neighboring router to re-establish an LDP session. If the neighboring router fails to establish a session within this amount of time, the local router will delete the stale label-forwarding equivalence class (FEC) bindings received from the neighboring router.

configure router ldp neighbor-liveness-time *seconds*

configure router ldp no neighbor-liveness-time

Syntax Definitions

seconds	The Maximum Recovery Time value, in seconds. The valid range is from 5–300.

Defaults

By default, the Neighbor Liveness Time is set to 120 seconds.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to set the Neighbor Liveness Time to the default value.
- If the neighboring router advertises a Reconnect Time that is less than the local Neighbor Liveness Time value, then the local router uses the Recovery Time to determine how long to wait for the neighbor to re-establish the LDP session.

Examples

```
-> configure router ldp neighbor-liveness-time 300
-> configure router ldp no neighbor-liveness-time
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure router ldp graceful-restart-helper	Configures the graceful restart helper status for the LDP router.
configure router ldp reconnect-time	Configures the Reconnect Timeout value in the fault tolerant (FT) Session TLV that is advertised in LDP messages.
configure router ldp fwd-state-holding-time	Configures the amount of time that the LDP router retains its MPLS forwarding state after a graceful restart.
configure router ldp maximum-recovery-time	Configures the amount of time the router retains stale MPLS label-FEC bindings received from a neighboring LDP router as the result of a graceful restart process.

MIB Objects

```
vRtrLdpGeneralTable
   vRtrLdpGenGRNbrLiveTime
```

oam lsp-ping

Performs an Operation Administration and Maintenance (OAM) in-band connectivity test for an MPLS Label Switched Path (LSP).

[configure] oam lsp-ping prefix *ip_prefix*/*mask* **[size** *octets***] [ttl** *label-ttl***] [timeout** *timeout***] [interval** *interval***] [send-count** *send-count***]**

Syntax Definitions

ip_prefix	The IP address of the destination node for the LSP.
mask	The subnet mask of the specified destination IP prefix.The value ranges from 1 to 32.
octets	The MPLS Echo request packet size in octets, expressed as a decimal integer. The value ranges from 84 to 9194.
label-ttl	The TTL value for the MPLS label, expressed as a decimal integer. The value ranges from 1 to 255.
timeout	The amount of time, in seconds, that the router will wait for a message reply after sending the MPLS Echo request message. The value ranges from 1 to 10.
interval	The minimum amount of time that must expire before the next MPLS Echo request message is sent. The value ranges from 1 to 10.
send-count	The number of Echo request messages to send, expressed as a decimal integer. The value ranges from 1 to 100.

Defaults

Parameter	Default
octets	84
label-ttl	255
timeout	5
interval	1
send-count	1

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- This command is used to test the path for an existing MPLS Label Distribution Protocol (LDP) signaled LSP. If the IP address specified is not the destination address for an existing LSP, the ping will fail.
- The in-band LSP connectivity test is performed as described in the *IETF RFC 4379*.

- This command does *not* support OAM ping for static LSPs.

Examples

```
-> oam lsp-ping prefix 5.5.5.5/32 send-count 5
LSP-PING 5.5.5.5/32: 80 bytes MPLS payload Seq=1, send from intf ip500, reply from
70.0.0.5
       udp-data-len=32 ttl=255 rtt=16ms rc=3 (EgressRtr) Seq=2, send from intf
ip500, reply from 70.0.0.5
       udp-data-len=32 ttl=255 rtt<10ms rc=3 (EgressRtr) Seq=3, send from intf
ip500, reply from 70.0.0.5
       udp-data-len=32 ttl=255 rtt<10ms rc=3 (EgressRtr) Seq=4, send from intf
ip500, reply from 70.0.0.5
       udp-data-len=32 ttl=255 rtt<10ms rc=3 (EgressRtr) Seq=5, send from intf
ip500, reply from 70.0.0.5
       udp-data-len=32 ttl=255 rtt<10ms rc=3 (EgressRtr)

---- LSP 5.5.5.5/32 PING Statistics ----
5 packets sent, 5 packets received, 0.00% packet loss round-trip min < 10ms, avg <
10ms, max = 16.0ms, stddev = 6.50ms

-> oam lsp-ping prefix 5.5.5.5/32 send-count 5 size 9000 interval 2
LSP-PING 5.5.5.5/32: 9000 bytes MPLS payload Seq=1, send from intf ip500, reply
from 70.0.0.5
       udp-data-len=32 ttl=255 rtt=866ms rc=3 (EgressRtr) Seq=2, send from intf
ip500, reply from 70.0.0.5
       udp-data-len=32 ttl=255 rtt<10ms rc=3 (EgressRtr) Seq=3, send from intf
ip500, reply from 70.0.0.5
       udp-data-len=32 ttl=255 rtt=966ms rc=3 (EgressRtr) Seq=4, send from intf
ip500, reply from 70.0.0.5
       udp-data-len=32 ttl=255 rtt<10ms rc=3 (EgressRtr) Seq=5, send from intf
ip500, reply from 70.0.0.5
       udp-data-len=32 ttl=255 rtt=966ms rc=3 (EgressRtr)

---- LSP 5.5.5.5/32 PING Statistics ----
5 packets sent, 5 packets received, 0.00% packet loss round-trip min < 10ms, avg =
559ms, max = 966ms, stddev = 459ms
```

output definitions

LSP-PING prefix or name	IP Prefix of the destination node for the LDP-signaled LSP.
MPLS payload	Size of the ping message in octets.
Seq	Sequence number of response.
Send from intf	Name of the interface on which the probe was sent.
reply from	The IPv4 address of the node that generated this reply.
udp-data-len	UDP data length of the echo reply.
ttl	TTL specified in ping.
rtt	Number of milliseconds from when a probe was sent to when its response was received.
rc	Number and type of return code in response.
packets sent	Number of probes sent for this entry.
packets received	Number of probes received for this entry.

packet loss	Percentage of probes sent that were not returned.
round-trip min	The minimum round-trip time received.
avg	The average round-trip time received.
max	The maximum round-trip time received.
stddev	The sum of the squares for all ping responses received. This value is used to enable standard deviation calculation.

Release History

Release 6.4.2; command was introduced.

Related Commands

oam lsp-trace	Performs OAM traceroute for an MPLS LDP LSP.

MIB Objects

```
tmnxOamPingCtlTable
   tmnxOamLspPingCtlLspName
   tmnxOamLspPingCtlLdpPrefixType
   tmnxOamLspPingCtlLdpPrefix
   tmnxOamLspPingCtlLdpPrefixLen
   tmnxOamPingCtlSize
   tmnxOamLspPingCtlTtl
   tmnxOamPingCtlTimeOut
   tmnxOamPingCtlInterval
   tmnxOamPingCtlProbeCount
tmnxOamLspPingCtlTable
   tmnxOamLspPingCtlLspName
   tmnxOamLspPingCtlLdpPrefixType
   tmnxOamLspPingCtlLdpPrefix
   tmnxOamLspPingCtlLdpPrefixLen
   tmnxOamPingCtlSize
   tmnxOamLspPingCtlTtl
   tmnxOamPingCtlTimeOut
   tmnxOamPingCtlInterval
   tmnxOamPingCtlProbeCount
```

oam lsp-trace

Performs an Operation Administration and Maintenance (OAM) traceroute for an existing MPLS Label Switched Path (LSP).

[configure] oam lsp-trace prefix *ip_prefix/mask* **[size** *octets***] [min-ttl** *min-label-ttl***] [max-ttl** *max-label-ttl***] [max-fail** *no-response-count***] [probe-count** *probes-per-hop***] [timeout** *timeout***] [interval** *interval***]**

Syntax Definitions

ip_prefix	The IP address of the destination node.
mask	The subnet mask of the specified destination IP prefix.The value ranges from 1 to 32.
octets	The MPLS Echo request packet size in octets, expressed as a decimal integer. The value ranges from 104 to 9194.
min-label-ttl	The minimum TTL value for the MPLS label for the LSP trace test, expressed as a decimal integer. The value ranges from 0 to 255.
max-label-ttl	The maximum TTL value for the MPLS label for the LSP trace test, expressed as a decimal integer. The value ranges from 1 to 255.
no-responce-count	The permissible maximum number of consecutive MPLS Echo requests that do not receive a reply before the trace operation fails for a given TTL, expressed as a decimal integer. The value ranges from 1 to 255.
probes-per-hop	The number of Echo request messages to send, expressed as a decimal integer. The value ranges from 1 to 10.
timeout	The amount of time, in seconds, that the router will wait for a message reply after sending the MPLS Echo request message. The value ranges from 1 to 60.
interval	The minimum amount of time that must expire before the next MPLS Echo request message is sent. A value of 0 implies the test will not be repeated. The value ranges from 0 to 10.

Defaults

Parameter	Default
octets	104
min-label-ttl	1
max-label-ttl	30
no-responce-count	5
probes-per-hop	1
timeout	3
interval	1

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- This command is used to perform a traceroute for an existing MPLS Label Distribution Protocol (LDP) signaled LSP. If the IP address specified is not the destination address for an existing LDP LSP, the traceroute will fail.
- The LSP traceroute is performed as described in the *IETF RFC 4379*.
- This command does *not* support OAM traceroute for static LSPs.

Examples

```
-> oam lsp-trace prefix 5.5.5.5/32
lsp-trace to 5.5.5.5/32: 1 hops min, 30 hops max, 104 byte packets
1  50.0.0.4  rtt<10ms rc=8(DSRtrMatchLabel)
     DS 1: IfAddr 80.0.0.5 MRU=1500 label=131070 proto=3(LDP)
2  70.0.0.5  rtt<10ms rc=3(EgressRtr)

-> oam lsp-trace prefix 5.5.5.5/32 size 9000
lsp-trace to 5.5.5.5/32: 1 hops min, 30 hops max, 9000 byte packets
1  50.0.0.4  rtt=966ms rc=8(DSRtrMatchLabel)
     DS 1: IfAddr 80.0.0.5 MRU=1500 label=131070 proto=3(LDP)
2  70.0.0.5  rtt=16ms rc=3(EgressRtr)
```

output definitions

lsp-trace to	IP Prefix of the destination node for the LDP-signaled LSP.
hops min	The initial TTL.
hops max	The max TTL.
byte packets	Size, in octets, of the probe request packet.
rtt	The round trip time, in milliseconds, of the trace request and response.
rc=# (EgressRtr)	Number and type of the last reply code received.

Release History

Release 6.4.2; command was introduced.

Related Commands

oam lsp-ping	Performs an OAM in-band connectivity test for an MPLS LDP LSP.

MIB Objects

```
tmnxOamTrCtlTable
   tmnxOamLspTrCtlLspName
   tmnxOamLspTrCtlLdpPrefixType
   tmnxOamLspTrCtlLdpPrefix
   tmnxOamLspTrCtlPrefixLen
   tmnxOamTrCtlDataSize
   tmnxOamTrCtlInitialTtl
   tmnxOamTrCtlMaxTtl
   tmnxOamTrCtlMaxFailures
   tmnxOamTrCtlProbesPerHop
   tmnxOamTrCtlTimeOut
   tmnxOamTrCtlInterval
tmnxOamLspTrCtlTable
   tmnxOamLspTrCtlLspName
   tmnxOamLspTrCtlLdpPrefixType
   tmnxOamLspTrCtlLdpPrefix
   tmnxOamLspTrCtlPrefixLen
   tmnxOamTrCtlDataSize
   tmnxOamTrCtlInitialTtl
   tmnxOamTrCtlMaxTtl
   tmnxOamTrCtlMaxFailures
   tmnxOamTrCtlProbesPerHop
   tmnxOamTrCtlTimeOut
   tmnxOamTrCtlInterval
```

show router ldp bindings

Displays the contents of the MPLS Label Information Base (LIB).

This section describes the base command (**show router ldp bindings**). Optional keywords are listed below and described as separate commands later in this chapter.

show router ldp bindings
[fec-type {services | prefixes | *fec-num***} [session** *ip-address***[**:*label-space***]]]**
[ingress-label *start-label* **[***end-label***]]**
[egress-label *start-label* **[***end-label***]]**
[prefix *ip-prefix/mask* **[session** *ip-address***[**:*label-space***]]]**
[active [prefix *ip-prefix/mask***]]**
[vc-type *vc-type* **[vc-id** *vc-id* **[session** *ip-address* **[**:*label-space***]]]]**
[service-id *service-id***]**

Syntax Definitions

N/A.

Defaults

By default, the entire contents of the LIB is displayed.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

Use the optional parameters provided with this command to display specific information for LDP label-FEC (Forwarding Equivalence Class) bindings.

Examples

```
-> show router ldp bindings
LDP LSR ID: 10.10.10.5

Legend: U = Label In Use, N = Label Not In Use, W = Label Withdrawn,
        S = Status Signaled Up,  D = Status Signaled Down,
        E = Epipe Service, V = VPLS Service, M = Mirror Service,
        A = Apipe Service, F = Fpipe Service, I = IES Service, R = VPRN service,
        P - Ipipe Service
        TLV = (Type, Length: Value)

LDP Prefix Bindings
Prefix           Peer           IngLbl  EgrLbl EgrIntf/LspId EgrNextHop
-----------------+--------------+-------+------+------------+--------------
10.10.10.5/32      10.11.0.6       131071U   --     --            --
10.11.0.6/32       10.11.0.6         --    131068   --            --

No. of Prefix Bindings: 2
```

```
LDP Service FEC 128 Bindings
Type   VCId      SvcId     SDPId  Peer           IngLbl  EgrLbl  LMTU  RMTU
------+----------+----------+------+--------------+-------+-------+-----+-----
V-Eth  100        100        10     10.11.0.6       131069U 131070  1514  1500

No. of VC Labels: 1


LDP Service FEC 129 Bindings
AGI                              SAII                  TAII
Type             SvcId     SDPId  Peer           IngLbl  EgrLbl  LMTU  RMTU
------+----------+----------+------+--------------+-------+-------+-----+-----
No Matching Entries Found
```

output definitions

Prefix	The IP network address and mask used to identify the prefix binding.
Peer	The IP address of the LDP peer.
Type	The type of service (**V-Eth**) exchanging labels through the Service Distribution Point (SDP).
VCId	The virtual connection (VC) ID number used by each end of the SDP tunnel to identify the VC.
SvcId	The unique service identification number used to identify the service.
SDPId	The SDP ID number associated with the service.
IngLbl	The ingress LDP label.
EgrLbl	The egress LDP label.
EgrIntf/LspId	The Label Switch Path (LSP) tunnel ID number (not the LSP path ID number).
EgrNextHop	The next hop IP address for the egress label.
LMTU	The local MTU number.
RMTU	The remote MTU number.

Release History

Release 6.4.2; command was introduced.

Related Commands

show router ldp bindings fec-type	Displays the LDP bindings for a specific type of FEC or for a specific service FEC number.
show router ldp bindings ingress-label	Displays ingress LDP bindings for a specific label number or for a range of label numbers.
show router ldp bindings egress-label	Displays egress LDP bindings for a specific label number or for a range of label numbers.
show router ldp bindings prefix	Displays the LDP bindings for a specific IP prefix.
show router ldp bindings active	Displays the LDP bindings for active IP prefixes.
show router ldp bindings vc-type	Displays the LDP bindings for the specified virtual circuit (VC) type.
show router ldp bindings service-id	Displays the LDP bindings for the specified service.

MIB Objects

```
alaEServiceInfo
   alaEServiceMode
```

show router ldp bindings fec-type

Displays the LDP bindings for a specific type of Forwarding Equivalence Class (FEC) or for a specific service FEC number.

show router ldp bindings fec-type {*fec-number* | **services | prefixes} [session** *ip-address***[***:label-space***]]**

Syntax Definitions

services	Displays bindings for service FECs.
prefixes	Displays bindings for address FECs.
fec-number	The service FEC number. Valid numbers are 128 and 129.
ip-address	The LDP router ID (Loopback0 IP address configured for the switch) for a specific LDP session.
:label-space	The label space ID number that the router advertises on the LDP interface. This value is appended to the LDP router ID address. The valid range is 0–65535.

Defaults

By default, LDP bindings are displayed for all LDP sessions associated with the specified FEC type.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Specify an FEC number to display label binding information for a specific FEC.
- Use the **services** parameter to display label binding information for service FECs. Note that only VPLS is supported.
- Use the **prefixes** parameter to display label binding information for address FECs. These are FECs that are associated with an IP address, instead of a service.
- Use the **session** parameter to display label binding information for a specific LDP router session. Note that entering a label-space value is optional with this parameter.

Examples

```
->show router ldp bindings fec-type 128
LDP LSR ID: 10.10.10.5

Legend: U = Label In Use, N = Label Not In Use, W = Label Withdrawn,
        S = Status Signaled Up,  D = Status Signaled Down,
        E = Epipe Service, V = VPLS Service, M = Mirror Service,
        A = Apipe Service, F = Fpipe Service, I = IES Service, R = VPRN service,
        P - Ipipe Service
        TLV = (Type, Length: Value)
```

```
LDP Service FEC 128 Bindings

Type   VCId      SvcId     SDPId  Peer           IngLbl  EgrLbl  LMTU  RMTU
------+----------+----------+------+--------------+-------+-------+-----+-----
V-Eth  100        100        10     10.11.0.6       131069U 131070  1500  1500

No. of VC Labels: 1

->show router ldp bindings fec-type services
LDP LSR ID: 10.11.0.6

Legend: U = Label In Use, N = Label Not In Use, W = Label Withdrawn,
        S = Status Signaled Up,  D = Status Signaled Down,
        R = VPRN Service, V = VPLS Service, W = VPWS Service
        TLV = (Type, Length: Value)

LDP Service FEC 128 Bindings
Type   VCId      SvcId     SDPId  Peer           IngLbl  EgrLbl  LMTU  RMTU
------+----------+----------+------+--------------+-------+-------+-----+-----
V-Eth  100        100        10     10.11.0.66      131068U 131068  1500  1500

No. of VC Labels: 1

LDP Service FEC 129 Bindings
AGI                              SAII                  TAII
Type             SvcId     SDPId  Peer           IngLbl  EgrLbl  LMTU  RMTU
------+----------+----------+------+--------------+-------+-------+-----+-----
No Matching Entries Found


->show router ldp bindings fec-type prefixes
LDP LSR ID: 10.11.0.6

Legend: U - Label In Use,  N - Label Not In Use
LDP Prefix Bindings

Prefix           Peer           IngLbl  EgrLbl EgrIntf/LspId EgrNextHop
-----------------+--------------+-------+------+-------------+--------------
10.10.0.7/32       10.10.0.7         --    131071   --            --
10.11.0.6/32       10.10.0.7       131071U   --     --            --
10.11.0.66/32      10.10.0.7       131069N 131070   --            --

No. of Prefix Bindings: 3


->show router ldp bindings fec-type prefixes session 10.10.0.7
LDP LSR ID: 10.11.0.6

Legend: U - Label In Use,  N - Label Not In Use
LDP Prefix Bindings

Prefix           Peer           IngLbl  EgrLbl EgrIntf      EgrNextHop
-----------------+--------------+-------+------+-------------+--------------
10.10.0.7/32       10.10.0.7         --    131071   --            --
10.11.0.6/32       10.10.0.7       131071U   --     --            --
10.11.0.66/32      10.10.0.7       131069N 131070   --            --

No. of Prefix Bindings: 3
```

output definitions

Prefix	The IP network address and mask used to identify the prefix binding.
Peer	The IP address of the LDP peer.
Type	The type of service (**V-Eth**) exchanging labels through the Service Distribution Point (SDP).
VCId	The virtual connection (VC) ID number used by each end of the SDP tunnel to identify the VC.
SvcId	The unique service identification number used to identify the service.
SDPId	The SDP ID number associated with the service.
IngLbl	The ingress LDP label.
EgrLbl	The egress LDP label.
EgrIntf/LspId	The Label Switch Path (LSP) tunnel ID number (not the LSP path ID number).
EgrNextHop	The next hop IP address for the egress label.
LMTU	The local MTU number.
RMTU	The remote MTU number.

Release History

Release 6.4.2; command was introduced.

Related Commands

show router ldp bindings	The base command used to display the entire contents of the LIB for the LDP router.

MIB Objects

show router ldp bindings ingress-label

Displays ingress LDP bindings for a specific label number or for a range of label numbers.

show router ldp bindings ingress-label *start-label* **[***end-label***]**

Syntax Definitions

start-label	The ingress label number to display. The valid range is 16–1048575.
end-label	The last ingress label number in a range of labels to display. The valid range is 17–1048575.

Defaults

By default, all ingress LDP bindings starting with the specified label number are displayed

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the optional *end-label* parameter along with the *start-label* parameter to specify a range of ingress label bindings to display.
- If an ending label number is not specified, then all ingress label bindings beginning with the starting label number forward are displayed. No range is specified.

Examples

```
->show router ldp bindings ingress-label 131068
LDP LSR ID: 10.11.0.6

Legend: U = Label In Use, N = Label Not In Use, W = Label Withdrawn,
        S = Status Signaled Up,  D = Status Signaled Down,
        R = VPRN Service, V = VPLS Service, W = VPWS Service
        TLV = (Type, Length: Value)

LDP Prefix Bindings
Prefix             Peer            IngLbl  EgrLbl EgrIntf       EgrNextHop
------------------+---------------+-------+------+------------+---------------
No Matching Entries Found

LDP Service FEC 128 Bindings
Type   VCId       SvcId      SDPId  Peer            IngLbl  EgrLbl  LMTU  RMTU
------+----------+----------+------+---------------+-------+-------+-----+-----
V-Eth  100        100        10     10.11.0.66      131068U 131068  1500  1500

No. of VC Labels: 1


LDP Service FEC 129 Bindings
AGI                              SAII                  TAII
Type            SvcId     SDPId  Peer           IngLbl  EgrLbl  LMTU  RMTU
```

```
------+----------+----------+------+---------------+-------+-------+-----+-----
No Matching Entries Found

->show router ldp bindings ingress-label 131068 139999
LDP LSR ID: 10.11.0.6

Legend: U = Label In Use, N = Label Not In Use, W = Label Withdrawn,
        S = Status Signaled Up,  D = Status Signaled Down,
        R = VPRN Service, V = VPLS Service, W = VPWS Service
        TLV = (Type, Length: Value)

LDP Prefix Bindings
Prefix             Peer             IngLbl  EgrLbl EgrIntf       EgrNextHop
-----------------+---------------+-------+------+-------------+---------------
10.11.0.6/32       10.10.0.7       131071U   --     --             --
10.11.0.66/32      10.10.0.7       131069N 131070   --             --

No. of Prefix Bindings: 2

LDP Service FEC 128 Bindings
Type   VCId       SvcId      SDPId  Peer            IngLbl  EgrLbl  LMTU  RMTU
------+----------+----------+------+---------------+-------+-------+-----+-----
V-Eth  100        100        10     10.11.0.66      131068U 131068  1500  1500

No. of VC Labels: 1


LDP Service FEC 129 Bindings
AGI                                SAII                    TAII
Type               SvcId      SDPId  Peer            IngLbl  EgrLbl  LMTU  RMTU
------+----------+----------+------+---------------+-------+-------+-----+-----
No Matching Entries Found
```

output definitions

Prefix	The IP network address and mask used to identify the prefix binding.
Peer	The IP address of the LDP peer.
Type	The type of service (**V-Eth**) exchanging labels through the Service Distribution Point (SDP).
VCId	The virtual connection (VC) ID number used by each end of the SDP tunnel to identify the VC.
SvcId	The unique service identification number used to identify the service.
SDPId	The SDP ID number associated with the service.
IngLbl	The ingress LDP label.
EgrLbl	The egress LDP label.
EgrIntf/LspId	The Label Switch Path (LSP) tunnel ID number (not the LSP path ID number).
EgrNextHop	The next hop IP address for the egress label.
LMTU	The local MTU number.
RMTU	The remote MTU number.

Release History

Release 6.4.2; command was introduced.

Related Commands

show router ldp bindings	The base command used to display the entire contents of the LIB for the LDP router.

MIB Objects

show router ldp bindings egress-label

Displays egress LDP bindings for a specific label number or for a range of label numbers.

show router ldp bindings egress-label *start-label* **[***end-label***]**

Syntax Definitions

start-label	The egress label number to display. The valid range is 16–1048575.
end-label	The last egress label number in a range of labels to display. The valid range is 17–1048575.

Defaults

By default, all egress LDP bindings starting with the specified label number are displayed.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the optional *end-label* parameter along with the *start-label* parameter to specify a range of egress label bindings to display.
- If an ending label number is not specified, then all egress label bindings beginning with the starting label number forward are displayed. No range is specified.

Examples

```
->show router ldp bindings egress-label 131071
LDP LSR ID: 10.11.0.6

Legend: U = Label In Use, N = Label Not In Use, W = Label Withdrawn,
        S = Status Signaled Up,  D = Status Signaled Down,
        R = VPRN Service, V = VPLS Service, W = VPWS Service
        TLV = (Type, Length: Value)

LDP Prefix Bindings

Prefix             Peer            IngLbl  EgrLbl EgrIntf       EgrNextHop
-----------------+---------------+-------+------+-------------+---------------
10.10.0.7/32       10.10.0.7         --    131071   --             --

No. of Prefix Bindings: 1

LDP Service FEC 128 Bindings
Type   VCId       SvcId      SDPId  Peer            IngLbl  EgrLbl  LMTU  RMTU
------+----------+----------+------+---------------+-------+-------+-----+-----
No Matching Entries Found


LDP Service FEC 129 Bindings
AGI                              SAII                  TAII
```

```
Type              SvcId      SDPId  Peer            IngLbl  EgrLbl  LMTU  RMTU
------+----------+----------+------+---------------+-------+-------+-----+-----
No Matching Entries Found


->show router ldp bindings egress-label 131070 199999
LDP LSR ID: 10.11.0.6

Legend: U = Label In Use, N = Label Not In Use, W = Label Withdrawn,
        S = Status Signaled Up,  D = Status Signaled Down,
        R = VPRN Service, V = VPLS Service, W = VPWS Service
        TLV = (Type, Length: Value)

LDP Prefix Bindings
Prefix             Peer            IngLbl  EgrLbl EgrIntf       EgrNextHop
------------------+---------------+-------+------+------------+---------------
10.10.0.7/32       10.10.0.7         --    131071   --            --
10.11.0.66/32      10.10.0.7       131069N 131070   --            --

No. of Prefix Bindings: 2

LDP Service FEC 128 Bindings
Type   VCId       SvcId      SDPId  Peer            IngLbl  EgrLbl  LMTU  RMTU
------+----------+----------+------+---------------+-------+-------+-----+-----
No Matching Entries Found

LDP Service FEC 129 Bindings
AGI                                SAII                    TAII
Type              SvcId      SDPId  Peer            IngLbl  EgrLbl  LMTU  RMTU
------+----------+----------+------+---------------+-------+-------+-----+-----
No Matching Entries Found
```

output definitions

Prefix	The IP network address and mask used to identify the prefix binding.
Peer	The IP address of the LDP peer.
Type	The type of service (**V-Eth**) exchanging labels through the Service Distribution Point (SDP).
VCId	The virtual connection (VC) ID number used by each end of the SDP tunnel to identify the VC.
SvcId	The unique service identification number used to identify the service.
SDPId	The SDP ID number associated with the service.
IngLbl	The ingress LDP label.
EgrLbl	The egress LDP label.
EgrIntf/LspId	The Label Switch Path (LSP) tunnel ID number (not the LSP path ID number).
EgrNextHop	The next hop IP address for the egress label.
LMTU	The local MTU number.
RMTU	The remote MTU number.

Release History

Release 6.4.2; command was introduced.

Related Commands

show router ldp bindings	The base command used to display the entire contents of the LIB for the LDP router.

MIB Objects

show router ldp bindings prefix

Displays the LDP bindings for a specific IP prefix.

show router ldp bindings prefix *ip-prefix/mask* **[session** *ip-address***[***:label-space***]]]**

Syntax Definitions

ip-prefix	The IP address prefix used to identify the IP network. Specify 0 for the host bits.
mask	The IP address mask used to identify the subnet address within the IP address prefix.
ip-address	The LDP router ID (Loopback0 IP address configured for the switch) for a specific LDP session.
:label-space	The label space ID number that the router advertises on the LDP interface. This value is appended to the LDP router ID address. The valid range is 0–65535.

Defaults

By default, LDP bindings are displayed for all sessions associated with the specified prefix.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

Use the **session** parameter to display prefix binding information for a specific LDP router session. Note that entering a label-space value is optional with this parameter.

Examples

```
->show router ldp bindings prefix 10.11.0.6/32
LDP LSR ID: 10.11.0.66

Legend: U - Label In Use,  N - Label Not In Use

LDP Prefix Bindings

Prefix             Peer            IngLbl  EgrLbl EgrIntf       EgrNextHop
-----------------+---------------+-------+------+-------------+---------------
10.11.0.6/32       10.10.0.7       131069N 131069   --          55.55.55.77

No. of Prefix Bindings: 1
```

output definitions

Prefix	The IP network address and mask used to identify the prefix binding.
Peer	The IP address of the LDP peer.
IngLbl	The ingress LDP label.
EgrLbl	The egress LDP label.
EgrIntf/LspId	The Label Switch Path (LSP) tunnel ID number (not the LSP path ID number).
EgrNextHop	The next hop IP address for the egress label.

Release History

Release 6.4.2; command was introduced.

Related Commands

show router ldp bindings	The base command used to display the entire contents of the LIB for the LDP router.

MIB Objects

show router ldp bindings active

Displays the LDP bindings for active IP prefixes.

show router ldp bindings active [prefix *ip-prefix/mask***]**

Syntax Definitions

ip-prefix	The IP address prefix used to identify the IP network. Specify 0 for the host bits.
mask	The IP address mask used to identify the subnet address within the IP address prefix.

Defaults

By default, active LDP bindings are displayed for all prefixes.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

Use the optional **prefix** parameter to display active bindings for a specific prefix.

Examples

```
->show router ldp bindings prefix 10.11.0.6/32
LDP LSR ID: 10.11.0.66

Legend: U - Label In Use,  N - Label Not In Use

LDP Prefix Bindings

Prefix             Peer            IngLbl  EgrLbl EgrIntf       EgrNextHop
-----------------+---------------+-------+------+-------------+---------------
10.11.0.6/32       10.10.0.7       131069N 131069   --          55.55.55.77

No. of Prefix Bindings: 1
```

output definitions

Prefix	The IP network address and mask used to identify the prefix binding.
Peer	The IP address of the LDP peer.
IngLbl	The ingress LDP label.
EgrLbl	The egress LDP label.
EgrIntf/LspId	The Label Switch Path (LSP) tunnel ID number (not the LSP path ID number).
EgrNextHop	The next hop IP address for the egress label.

Release History

Release 6.4.2; command was introduced.

Related Commands

show router ldp bindings	The base command used to display the entire contents of the LIB for the LDP router.

MIB Objects

show router ldp bindings vc-type

Displays the LDP bindings for the specified virtual circuit (VC) type.

show router ldp bindings vc-type *vc-type* **[vc-id** *vc-id* **[session** *ip-address* **[**:*label-space***]]**

Syntax Definitions

vc-type	The virtual circuit type. Valid types are **ethernet**, **vlan**, and **mirror**.
vc-id	The virtual circuit ID number. The valid range is 1–4294967295.
ip-address	The LDP router ID (Loopback0 IP address configured for the switch) for a specific LDP session.
:label-space	The label space ID number that the router advertises on the LDP interface. This value is appended to the LDP router ID address. The valid range is 0–65535.

Defaults

By default, LDP bindings for all VC IDs and all sessions for each VC ID are displayed for the specified VC type.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **vc-id** parameter to display the LDP bindings for a specific VC ID number.
- Use the **session** parameter to display the LDP bindings for a specific session associated with the specified VC ID number.

Examples

```
->show router ldp bindings vc-type ethernet
LDP LSR ID: 10.11.0.6

Legend: U = Label In Use, N = Label Not In Use, W = Label Withdrawn,
        S = Status Signaled Up,  D = Status Signaled Down,
        R = VPRN Service, V = VPLS Service, W = VPWS Service
        TLV = (Type, Length: Value)

LDP Service FEC 128 Bindings
Type   VCId       SvcId      SDPId  Peer            IngLbl  EgrLbl  LMTU  RMTU
------+----------+----------+------+---------------+-------+-------+-----+-----
V-Eth  100        100        10     10.11.0.66      131068U 131068  1500  1500


LDP Service FEC 129 Bindings
AGI                              SAII                  TAII
Type               SvcId      SDPId  Peer            IngLbl  EgrLbl  LMTU  RMTU
------+----------+----------+------+---------------+-------+-------+-----+-----
```

```
->show router ldp bindings vc-type ethernet vc-id 100
LDP LSR ID: 10.11.0.6

Legend: U = Label In Use, N = Label Not In Use, W = Label Withdrawn,
        S = Status Signaled Up,  D = Status Signaled Down,
        R = VPRN Service, V = VPLS Service, W = VPWS Service
        TLV = (Type, Length: Value)

LDP Service FEC 128 Bindings

Type   VCId       SvcId      SDPId  Peer            IngLbl  EgrLbl  LMTU  RMTU
------+----------+----------+------+---------------+-------+-------+-----+-----
V-Eth  100        100        10     10.11.0.66      131068U 131068  1500  1500

No. of VC Labels: 1

->show router ldp bindings vc-type ethernet vc-id 100 session 10.11.0.66
LDP LSR ID: 10.11.0.6

Legend: U = Label In Use, N = Label Not In Use, W = Label Withdrawn,
        S = Status Signaled Up,  D = Status Signaled Down,
        R = VPRN Service, V = VPLS Service, W = VPWS Service
        TLV = (Type, Length: Value)

LDP Service FEC 128 Bindings

Type   VCId       SvcId      SDPId  Peer            IngLbl  EgrLbl  LMTU  RMTU
------+----------+----------+------+---------------+-------+-------+-----+-----
V-Eth  100        100        10     10.11.0.66      131068U 131068  1500  1500

No. of VC Labels: 1
```

output definitions

Type	The type of service (**V-Eth**) exchanging labels through the Service Distribution Point (SDP).
VCId	The virtual connection (VC) ID number used by each end of the SDP tunnel to identify the VC.
SvcId	The unique service identification number used to identify the service.
SDPId	The SDP ID number associated with the service.
Peer	The IP address of the LDP peer.
IngLbl	The ingress LDP label.
EgrLbl	The egress LDP label.
LMTU	The local MTU number.
RMTU	The remote MTU number.

Release History

Release 6.4.2; command was introduced.

Related Commands

show router ldp bindings	The base command used to display the entire contents of the LIB for the LDP router.

MIB Objects

show router ldp bindings service-id

Displays the LDP bindings for the specified service.

show router ldp bindings service-id *service-id*

Syntax Definitions

service-id	The service ID number. The valid range is 1–2147483647.

Defaults

N/A.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

The service ID is a unique number that identifies a specific service. All LDP bindings associated with the service ID are displayed.

Examples

```
# show router ldp bindings service-id 100
LDP LSR ID: 10.11.0.6

Legend: U = Label In Use, N = Label Not In Use, W = Label Withdrawn,
        S = Status Signaled Up,  D = Status Signaled Down,
        R = VPRN Service, V = VPLS Service, W = VPWS Service
        TLV = (Type, Length: Value)

LDP Service FEC 128 Bindings
Type   VCId       SvcId      SDPId  Peer            IngLbl  EgrLbl  LMTU  RMTU
------+----------+----------+------+---------------+-------+-------+-----+-----
V-Eth  100        100        10     10.11.0.66      131068U 131068  1500  1500

No. of VC Labels: 1


LDP Service FEC 129 Bindings
AGI                                SAII                    TAII
Type               SvcId      SDPId  Peer            IngLbl  EgrLbl  LMTU  RMTU
------+----------+----------+------+---------------+-------+-------+-----+-----

No. of FEC 129s: 1
```

output definitions

Type	The type of service (**V-Eth**) exchanging labels through the Service Distribution Point (SDP).
VCId	The virtual connection (VC) ID number used by each end of the SDP tunnel to identify the VC.

output definitions

SvcId	The unique service identification number used to identify the service.
SDPId	The SDP ID number associated with the service.
Peer	The IP address of the LDP peer.
IngLbl	The ingress LDP label.
EgrLbl	The egress LDP label.
LMTU	The local MTU number.
RMTU	The remote MTU number.

Release History

Release 6.4.2; command was introduced.

Related Commands

show router ldp bindings	The base command used to display the entire contents of the LIB for the LDP router.

MIB Objects

show router ldp discovery

Displays the discovery status of the LDP Hello adjacencies between the local router and LDP peers.

show router ldp discovery [state {trying | established | down}] [detail]

Syntax Definitions

trying	Displays LDP interfaces that are trying to establish an adjacency with peers.
established	Displays LDP interfaces that have established adjacencies with peers.
down	Displays LDP interfaces with adjacencies that are down.
detail	Displays detailed information for LDP hello adjacencies.

Defaults

By default, the discovery status for all the LDP Hello adjacencies is displayed.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **state** parameter with the **trying**, **established**, or **down** options to display LDP adjacencies that are in a specific state of discovery.
- Use the **detail** parameter to display additional discovery information and statistics for the adjacencies.

Examples

```
->show router ldp discovery
LDP Hello Adjacencies

Interface Name                   Local Addr      Peer Addr       AdjType State
---------------------------------+---------------+---------------+-------+------
N/A                              10.10.10.5      10.11.0.6       Targ    Estab
N/A                              10.10.10.5      20.1.2.3        Targ    Trying
N/A                              10.10.10.5      30.1.2.3        Targ    Trying
vlan-30                          10.10.10.5      10.11.0.6       Link    Estab

No. of Hello Adjacencies: 4

->show router ldp discovery detail
LDP Hello Adjacencies (Detail)
    Peer 10.11.0.66
      Local Address:      10.11.0.6,         Peer Address:        10.11.0.66,
      Adjacency Type:     Targeted,          State:               Established,
      Up Time:            0d 03:11:09,       Hold Time Remaining:  34,
      Hello Mesg Recv:    821,               Hello Mesg Sent:     819,
      Local IP Address:   10.11.0.6,         Remote IP Address:   10.11.0.66,
      Local Hello Timeout: 45,               Remote Hello Timeout: 45,
```

```
      Local Cfg Seq No:    2,                 Remote Cfg Seq No:    2265099808

    Interface "vlan-30"
      Local Address:      10.11.0.6,          Peer Address:         10.10.0.7,
      Adjacency Type:     Link,               State:               Established,
      Up Time:           0d 03:12:03,         Hold Time Remaining:  14,
      Hello Mesg Recv:    2882,               Hello Mesg Sent:      2882,
      Local IP Address:   30.30.30.66,        Remote IP Address:    30.30.30.77,
      Local Hello Timeout: 15,                Remote Hello Timeout: 15,
       Local Cfg Seq No:    3,                   Remote Cfg Seq No:    3

->show router ldp discovery state down
Interface Name                  Local Addr      Peer Addr       AdjType State
--------------------------------+---------------+---------------+-------+------
N/A                               10.11.0.6       10.11.0.66      Targ    Down
vlan-30                           10.11.0.6       10.10.0.7       Link    Down

No. of Hello Adjacencies: 2


->show router ldp discovery state established
Interface Name                  Local Addr      Peer Addr       AdjType State
--------------------------------+---------------+---------------+-------+------
N/A                               10.11.0.6       10.11.0.66      Targ    Estab
vlan-30                           10.11.0.6       10.10.0.7       Link    Estab

No. of Hello Adjacencies: 2


->show router ldp discovery state trying
Interface Name                  Local Addr      Peer Addr       AdjType State
--------------------------------+---------------+---------------+-------+------
N/A                               10.11.0.6       10.11.0.66      Targ    Trying
vlan-30                           10.11.0.6       10.10.0.7       Link    Trying

No. of Hello Adjacencies: 2
```

output definitions

Interface Name	The name of the local LDP IP interface.
Local Addr	The IP address of the local router.
Peer Addr	The IP address of the LDP peer.
AdjType	The type of adjacency between the local LDP interface and the LDP peer (**Link**–peers directly connected establish linked sessions or **Targ**–peers not directly connected establish targeted sessions).
State	The status of the LDP hello adjacency (**Estab**, **Trying**, or **Down**).
No. of Hello Adjacencies	The number of LDP hello adjacencies discovered.
Up Time	The amount of time the adjacency has been established.
Hold Time Remaining	The amount of time left before the peer for this adjacency is declared down.
Hello Mesg Recv	The number of Hello messages received from this adjacency.
Hello Mesg Sent	The number of Hello messages sent for this adjacency.
Local IP Address	The IP address of the local IP interface for this adjacency.

output definitions

Remote IP Address	The IP address of the peer IP interface for this adjacency.
Local Hello Timeout	The Hello Timeout value configured for the local router.
Remote Hello Timeout	The Hello Timeout value configured for the peer.
Local Cfg Seq No	The configuration sequence number that was in the Hello received when this adjacency started up. This configuration sequence number changes when there is a change of configuration.
Remote Cfg Seq No	The configuration sequence number that was in the Hello received when this adjacency started up. This configuration sequence number changes when there is a change of configuration.

Release History

Release 6.4.2; command was introduced.

Related Commands

show router ldp discovery peer	Displays the discovery status for adjacencies that are associated with a specific LDP peer.
show router ldp discovery interface	Displays the discovery status for adjacencies that are associated with a specific LDP interface.

MIB Objects

```
vRtrLdpHelloAdjTable
   vRtrLdpPeerLdpId
   vRtrLdpHelloAdjLocalLdpId
   vRtrLdpHelloAdjEntityIndex
   vRtrLdpHelloAdjIndex
   vRtrLdpHelloAdjHoldTimeRemaining
   vRtrLdpHelloAdjType
   vRtrLdpHelloAdjRemoteConfSeqNum
   vRtrLdpHelloAdjRemoteIpAddress
   vRtrLdpHelloAdjUpTime
   vRtrLdpHelloAdjLocalConfSeqNum
   vRtrLdpHelloAdjLocalIpAddress
   vRtrLdpHelloAdjInHelloMsgCount
   vRtrLdpHelloAdjOutHelloMsgCount
   vRtrLdpHelloAdjLocalHelloTimeout
   vRtrLdpHelloAdjRemoteHelloTimeout
```

show router ldp discovery peer

Displays the discovery status of the LDP Hello adjacencies associated with the specified LDP peer.

show router ldp discovery peer *ip-address* **[state {trying | established | down}] [detail]**

Syntax Definitions

ip-address	The IP address of the LDP peer.
trying	Displays LDP interfaces that are trying to establish an adjacency with peers.
established	Displays LDP interfaces that have established adjacencies with peers.
down	Displays LDP interfaces with adjacencies that are down.
detail	Displays detailed information for LDP hello adjacencies.

Defaults

By default, the discovery status for the LDP Hello adjacencies with the specified LDP peer is displayed.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **state** parameter with the **trying**, **established**, or **down** options to display LDP adjacencies that are in a specific state of discovery.
- Use the **detail** parameter to display additional discovery information and statistics for the adjacencies.

Examples

```
->show router ldp discovery peer 10.11.0.6
LDP Hello Adjacencies

Interface Name                   Local Addr      Peer Addr       AdjType State
---------------------------------+---------------+---------------+--------------
vlan-30                          10.11.0.66      10.11.0.6       Targ    Estab

No. of Hello Adjacencies: 1


->show router ldp discovery peer 10.11.0.6 detail
LDP Hello Adjacencies (Detail)

    Peer 10.11.0.6
      Local Address:      10.11.0.6,         Peer Address:        10.10.0.7,
      Adjacency Type:     Link,              State:               Established,
      Up Time:           0d 03:14:22,        Hold Time Remaining:  15,
      Hello Mesg Recv:    2917,              Hello Mesg Sent:     2917,
     Local IP Address:   30.30.30.66,       Remote IP Address:   30.30.30.77,
      Local Hello Timeout: 15,              Remote Hello Timeout: 15,
```

```
      Local Cfg Seq No:    3,                  Remote Cfg Seq No:    3

->show router ldp discovery peer 10.11.0.6 state down
Interface Name                  Local Addr      Peer Addr       AdjType State
--------------------------------+---------------+---------------+-------+------

No Matching Entries Found

->show router ldp discovery peer 10.11.0.6 state established
Interface Name                  Local Addr      Peer Addr       AdjType State
--------------------------------+---------------+---------------+-------+------
vlan-30                           10.11.0.6       10.10.0.7       Link    Estab

No. of Hello Adjacencies: 1

->show router ldp discovery peer 10.11.0.6 state trying
Interface Name                  Local Addr      Peer Addr       AdjType State
--------------------------------+---------------+---------------+-------+------

No Matching Entries Found
```

output definitions

Interface Name	The name of the local LDP IP interface.
Local Addr	The IP address of the local router.
Peer Addr	The IP address of the LDP peer.
AdjType	The type of adjacency between the local LDP interface and the LDP peer (**Link**–peers directly connected establish linked sessions or **Targ**–peers not directly connected establish targeted sessions).
State	The status of the LDP hello adjacency (**Estab**, **Trying**, or **Down**).
No. of Hello Adjacencies	The number of LDP hello adjacencies discovered.
Up Time	The amount of time the adjacency has been established.
Hold Time Remaining	The amount of time left before the peer for this adjacency is declared down.
Hello Mesg Recv	The number of Hello messages received from this adjacency.
Hello Mesg Sent	The number of Hello messages sent for this adjacency.
Local IP Address	The IP address of the local IP interface for this adjacency.
Remote IP Address	The IP address of the peer IP interface for this adjacency.
Local Hello Timeout	The Hello Timeout value configured for the local router.
Remote Hello Timeout	The Hello Timeout value configured for the peer.
Local Cfg Seq No	The configuration sequence number that was in the Hello received when this adjacency started up. This configuration sequence number changes when there is a change of configuration.
Remote Cfg Seq No	The configuration sequence number that was in the Hello received when this adjacency started up. This configuration sequence number changes when there is a change of configuration.

Release History

Release 6.4.2; command was introduced.

Related Commands

show router ldp discovery	Displays the discovery status for all the adjacencies associated with the local LDP interfaces.
show router ldp discovery interface	Displays the discovery status for adjacencies that are associated with a specific LDP interface.

MIB Objects

```
vRtrLdpHelloAdjTable
   vRtrLdpPeerLdpId
   vRtrLdpHelloAdjLocalLdpId
   vRtrLdpHelloAdjEntityIndex
   vRtrLdpHelloAdjIndex
   vRtrLdpHelloAdjHoldTimeRemaining
   vRtrLdpHelloAdjType
   vRtrLdpHelloAdjRemoteConfSeqNum
   vRtrLdpHelloAdjRemoteIpAddress
   vRtrLdpHelloAdjUpTime
   vRtrLdpHelloAdjLocalConfSeqNum
   vRtrLdpHelloAdjLocalIpAddress
   vRtrLdpHelloAdjInHelloMsgCount
   vRtrLdpHelloAdjOutHelloMsgCount
   vRtrLdpHelloAdjLocalHelloTimeout
   vRtrLdpHelloAdjRemoteHelloTimeout
```

show router ldp discovery interface

Displays the discovery status of the LDP Hello adjacencies associated with the specified LDP interface.

show router ldp discovery interface *ip-intf-name* **[state {trying | established | down}] [detail]**

Syntax Definitions

ip-intf-name	The name of an existing LDP interface.
trying	Displays adjacencies that the specified interface is trying to establish.
established	Displays established adjacencies for the specified interface.
down	Displays adjacencies for the specified interface that are down.
detail	Displays detailed information about the LDP interface.

Defaults

By default, this command displays the discovery status for all the LDP Hello adjacencies associated with the specified interface.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **state** parameter with the **trying**, **established**, or **down** options to display LDP adjacencies that are in a specific state of discovery.
- Use the **detail** parameter to display additional discovery information and statistics for the adjacencies.

Examples

```
->show router ldp discovery interface vlan-30
LDP Hello Adjacencies

Interface Name                   Local Addr      Peer Addr       AdjType State
---------------------------------+---------------+---------------+-------+------
vlan-30                          10.11.0.6       10.10.0.7       Link    Estab

No. of Hello Adjacencies: 1

->show router ldp discovery interface vlan-30 detail
LDP Hello Adjacencies (Detail)
    Interface "vlan-30"
      Local Address:      10.11.0.6,         Peer Address:        10.10.0.7,
      Adjacency Type:      Link,             State:              Established,
      Up Time:            0d 03:14:22,       Hold Time Remaining:  15,
      Hello Mesg Recv:     2917,             Hello Mesg Sent:     2917,
      Local IP Address:   30.30.30.66,       Remote IP Address:   30.30.30.77,
      Local Hello Timeout: 15,               Remote Hello Timeout: 15,
       Local Cfg Seq No:    3,                Remote Cfg Seq No:    3
```

```
->show router ldp discovery interface vlan-30 state down
LDP Hello Adjacencies

Interface Name                  Local Addr      Peer Addr       AdjType State
--------------------------------+---------------+---------------+-------+------

No Matching Entries Found

->show router ldp discovery interface vlan-30 state established
LDP Hello Adjacencies

Interface Name                  Local Addr      Peer Addr       AdjType State
--------------------------------+---------------+---------------+-------+------
vlan-30                           10.11.0.6       10.10.0.7       Link    Estab

No. of Hello Adjacencies: 1

->show router ldp discovery interface vlan-30 state trying
LDP Hello Adjacencies

Interface Name                  Local Addr      Peer Addr       AdjType State
--------------------------------+---------------+---------------+-------+------

No Matching Entries Found
```

output definitions

Interface Name	The name of the local LDP IP interface.
Local Addr	The IP address of the local router.
Peer Addr	The IP address of the LDP peer.
AdjType	The type of adjacency between the local LDP interface and the LDP peer (**Link**–peers directly connected establish linked sessions or **Targ**–peers not directly connected establish targeted sessions).
State	The status of the LDP hello adjacency (**Estab**, **Trying**, or **Down**).
No. of Hello Adjacencies	The number of LDP hello adjacencies discovered.
Up Time	The amount of time the adjacency has been established.
Hold Time Remaining	The amount of time left before the peer for this adjacency is declared down.
Hello Mesg Recv	The number of Hello messages received from this adjacency.
Hello Mesg Sent	The number of Hello messages sent for this adjacency.
Local IP Address	The IP address of the local IP interface for this adjacency.
Remote IP Address	The IP address of the peer IP interface for this adjacency.
Local Hello Timeout	The Hello Timeout value configured for the local router.
Remote Hello Timeout	The Hello Timeout value configured for the peer.

output definitions

Local Cfg Seq No	The configuration sequence number that was in the Hello received when this adjacency started up. This configuration sequence number changes when there is a change of configuration.
Remote Cfg Seq No	The configuration sequence number that was in the Hello received when this adjacency started up. This configuration sequence number changes when there is a change of configuration.

Release History

Release 6.4.2; command was introduced.

Related Commands

show router ldp discovery	Displays the discovery status for all the adjacencies associated with the local LDP interfaces.
show router ldp discovery peer	Displays the discovery status for adjacencies that are associated with a specific LDP peer.

MIB Objects

```
vRtrLdpHelloAdjTable
   vRtrLdpPeerLdpId
   vRtrLdpHelloAdjLocalLdpId
   vRtrLdpHelloAdjEntityIndex
   vRtrLdpHelloAdjIndex
   vRtrLdpHelloAdjHoldTimeRemaining
   vRtrLdpHelloAdjType
   vRtrLdpHelloAdjRemoteConfSeqNum
   vRtrLdpHelloAdjRemoteIpAddress
   vRtrLdpHelloAdjUpTime
   vRtrLdpHelloAdjLocalConfSeqNum
   vRtrLdpHelloAdjLocalIpAddress
   vRtrLdpHelloAdjInHelloMsgCount
   vRtrLdpHelloAdjOutHelloMsgCount
   vRtrLdpHelloAdjLocalHelloTimeout
   vRtrLdpHelloAdjRemoteHelloTimeout
```

show router ldp interface

Displays the LDP interface configuration for the local router.

show router ldp interface [*ip-intf-name* | *ip-address***] [detail]**

Syntax Definitions

ip-intf-name	The name of an existing LDP interface.
ip-address	The IP address of an existing LDP interface.
detail	Displays detailed adjacency information for the specified interface.

Defaults

By default, the configuration for all LDP interfaces is displayed.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the *ip-intf-name* and *ip-address* parameters to display information for a specific interface.
- Use the **detail** parameter to display additional information and statistics for LDP interfaces.

Examples

```
->show router ldp interface
LDP Interfaces

Interface                       Adm Opr  Hello  Hold  KA     KA      Transport
                                         Factor Time  Factor Timeout Address
--------------------------------+---+----+------+-----+------+-------+---------
vlan-30                         Up  Up   3      15    3      30      System

No. of Interfaces: 1

->show router ldp interface detail
LDP Interfaces (Detail)

    Interface "vlan-30"
      Admin State:        Up,               Oper State:       Up,
      Hold Time:          15,               Hello Factor:     3,
      Keepalive Timeout:  30,               Keepalive Factor:  3,
       Transport Addr:     System,           Last Modified: 05/26/2009 23:14:27,
      Active Adjacencies:  1,
      Tunneling:          Disabled,
       Lsp Name          : None
```

```
->show router ldp interface vlan-30
LDP Interfaces

Interface                        Adm Opr  Hello  Hold  KA     KA      Transport
                                          Factor Time  Factor Timeout Address
---------------------------------+---+----+------+-----+------+-------+---------
vlan-30                          Up  Up   3      15    3      30      System

No. of Interfaces: 1

->show router ldp interface vlan-30 detail
LDP Interfaces (Detail)

    Interface "vlan-30"
      Admin State:         Up,                 Oper State:        Up,
      Hold Time:           15,                 Hello Factor:      3,
      Keepalive Timeout:   30,                 Keepalive Factor:  3,
       Transport Addr:      System,               Last Modified:     05/26/2009
23:14:27,
      Active Adjacencies:  1,
      Tunneling:           Disabled,
      Lsp Name           : None

->show router ldp interface 10.11.0.66
LDP Interfaces

Interface                        Adm Opr  Hello  Hold  KA     KA      Transport
                                          Factor Time  Factor Timeout Address
---------------------------------+---+----+------+-----+------+-------+---------
vlan-30                          Up  Up   3      15    3      30      System

No. of Interfaces: 1
```

output definitions

Interface	The name of the local LDP IP interface. Configured through the **configure router ldp interface-parameters interface** command.
Adm	The administrative state of the LDP interface (Up or Down). Configured through the **configure router ldp interface-parameters interface shutdown** command.
Opr	The operational state of the LDP interface (Up or Down).
Hello Factor	The Hello factor value that is divided into the Hold Time value to determine the interval at which Hello messages are sent from this interface. Configured through the **configure router ldp interface-parameters hello** command.
Hold Time	The Hold Time value (also referred to as Hello Timeout) determines the amount of time, in seconds, LDP waits to receive hello messages from a peer before declaring that the peer is down. Configured through the **configure router ldp interface-parameters hello** command.
KA Factor	The Keepalive Factor value. This value is divided into the Keepalive Timeout value to determine the interval at which Keepalive messages are sent from this interface. Configured through the **configure router ldp interface-parameters keepalive** command.

output definitions

KA Timeout	The amount of time, in seconds, LDP waits to receive keepalive messages from an LDP peer before tearing down the session with that peer. Configured through the **configure router ldp interface-parameters keepalive** command.
Transport Address	The IP address used to set up an LDP session (**System** or **Interface**). The **System** value indicates that the Loopback0 address for the switch is used. The **Interface** value indicates that the IP address for the interface is used.
Last Modified	The date and time the interface configuration was last modified.
Active Adjacencies	The number of active adjacencies between this interface and LDP peers.
Tunneling	The tunneling status for the interface (**Enabled** or **Disabled**).
Lsp Name	The name of the Label Switch Path associated with this interface.

Release History

Release 6.4.2; command was introduced.

Related Commands

show router ldp parameters	Displays the LDP graceful restart, interface, and targeted session parameter values for the local router.
show router ldp discovery interface	Displays the discovery status of the LDP Hello adjacencies associated with the specified LDP interface.
show router ldp peer	Displays configuration information for LDP peers.

MIB Objects

```
vRtrLdpHelloAdjTable
   vRtrLdpPeerLdpId
   vRtrLdpHelloAdjLocalLdpId
   vRtrLdpHelloAdjEntityIndex
   vRtrLdpHelloAdjIndex
   vRtrLdpHelloAdjHoldTimeRemaining
   vRtrLdpHelloAdjType
   vRtrLdpHelloAdjRemoteConfSeqNum
   vRtrLdpHelloAdjRemoteIpAddress
   vRtrLdpHelloAdjUpTime
   vRtrLdpHelloAdjLocalConfSeqNum
   vRtrLdpHelloAdjLocalIpAddress
   vRtrLdpHelloAdjInHelloMsgCount
   vRtrLdpHelloAdjOutHelloMsgCount
   vRtrLdpHelloAdjLocalHelloTimeout
   vRtrLdpHelloAdjRemoteHelloTimeout
```

show router ldp parameters

Displays the global LDP parameter values (graceful restart, interface, and targeted session) for the local router.

show router parameters

Syntax Definitions

N/A.

Defaults

N/A.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

The interface parameters displayed with this command are global values that serve as default values for individual LDP interfaces. Note that parameter values configured for a specific interface override the global values.

Examples

```
->show router ldp parameters
LDP Parameters (LSR ID 10.10.0.7)

 Graceful Restart Parameters
   Fwd State Hold Time (sec):  120,                  Reconnect Time (sec):    120,
   Nbor Liveness Time (sec):   120,                  Max Recovery Time (sec): 120

 Interface Parameters
   Keepalive Timeout (sec):    30,                   Keepalive Factor:   3,
   Hold Time (sec):            15,                   Hello Factor:       3,
   Propagate Policy:           system,               Transport Address:  system,
   Deaggregate FECs:           False,                Route Preference:   9,
   Label Distribution:         downstreamUnsolicited, Label Retention:   liberal,
   Control Mode:               ordered,              Loop Detection:     none

 Targeted Session Parameters
   Keepalive Timeout (sec):    40,                   Keepalive Factor:   4,
   Hold Time (sec):            45,                   Hello Factor:       3,
   Passive Mode:               False,                Targeted Sessions:  Enabled
```

output definitions

Graceful Restart Parameters:	
Fwd State Hold Time (sec)	The amount of time, in seconds, that the LDP router retains its MPLS forwarding state after a graceful restart. Configured through the **configure router ldp fwd-state-holding-time** command.

output definitions

Reconnect Time (sec)	The amount of time, in seconds, that neighboring LDP routers should wait for the sender of the LDP message to gracefully restart and resume sending LDP messages. Configured through the **configure router ldp reconnect-time** command.
Nbor Liveness Time (sec)	The amount of time, in seconds, the router will wait for a neighboring router to re-establish an LDP session. Configured through the **configure router ldp neighbor-liveness-time** command.
Max Recovery Time (sec)	The amount of time, in seconds, the router retains stale MPLS label-forwarding equivalence class (FEC) bindings received from a neighboring LDP router as the result of a graceful restart process. Configured through the **configure router ldp maximum-recovery-time** command.
Interface Parameters:	
Keepalive Timeout (sec)	The amount of time, in seconds, LDP waits to receive keepalive messages from an LDP peer before tearing down the session with that peer. Configured through the **configure router ldp interface-parameters keepalive** command.
Keepalive Factor	The Keepalive factor value that is divided into the Keepalive Timeout value to determine the interval at which Keepalive messages are sent from this interface. Configured through the **configure router ldp interface-parameters keepalive** command.
Hold Time (sec)	The Hold Time value (also referred to as Hello Timeout) determines the amount of time, in seconds, LDP waits to receive hello messages from a peer before declaring that the peer is down. Configured through the **configure router ldp interface-parameters hello** command.
Hello Factor	The Hello factor value that is divided into the Hold Time value to determine the interval at which Hello messages are sent from this interface. Configured through the **configure router ldp interface-parameters hello** command.
Propagate Policy	Indicates whether or not the Label Switch Router (LSR) should generate FECs and which FECs to generate (**system**, **interface**, **all**, or **none**). ***(Note to reviewer: Is this supported on AOS switch?)***
Transport Address	The IP address used to set up an LDP session (**System** or **Interface**). The **System** value indicates that the Loopback0 address for the switch is used. The **Interface** value indicates that the IP address for the interface is used.
Deaggregate FECs	Indicates whether or not LDP aggregates multiple prefixes into a single (FEC) and advertises a single label for the FEC (**True** or **False**). This value only applies to LDP interfaces but is not used for targeted sessions.
Route Preference	The route preference assigned to LDP routes. When multiple routes are available to a destination, the route with the lowest preference will be used. This value only applies to LDP interfaces but is not used for targeted sessions.
Label Distribution	The label distribution method.

output definitions

Label Retention	The type of advertised label mappings that the router will retain (**liberal** or **conservative**). The **liberal** value indicates that all advertised label mappings are retained whether or not they are from a valid next hop. When the label distribution value is downstream unsolicited, a router may receive label bindings for the same destination for all its neighbors. Labels for the non-next hops for the FECs are retained in the software but not used. When a network topology change occurs where a non-next hop becomes a valid next hop, the label received earlier is then used The **conservative** value indicates that advertised label mappings are retained only if they will be used to forward packets; for example if the label came from a valid next hop. Label bindings received from non-next hops for each FEC are discarded.
Control Mode	The response to label request (**ordered** or **independent**). The **ordered** value indicates that label bindings are not distributed in response to a label request until a label binding has been received from the next hop for the destination The **independent** value indicates that label bindings are distributed immediately in response to a label request, even if a label binding has not yet been received from the next hop for the destination
Loop Detection	The status of loop detection for this router. This field displays one of the following values: • **Enabled**—Loop detection is enabled. • **Disabled**—Loop detection is disabled. • **None**—Loop detection is not supported. • **Other**—Loop detection is supported by a method other than hopCount, pathVector, or hopCountAndPathVector. • **hopCount**—Loop detection by hop count only. • **pathVector**—Loop detection by path vector only. • **hopCountAndPathVector**—Loop detection by hop count and path vector.
Targeted Session Parameters:	
Keepalive Timeout (sec)	The amount of time, in seconds, LDP waits to receive keepalive messages from an LDP peer before tearing down the session with that peer. Configured through the **configure router ldp interface-parameters keepalive** command.
Keepalive Factor	The Keepalive factor value that is divided into the Keepalive Timeout value to determine the interval at which Keepalive messages are sent from this interface. Configured through the **configure router ldp interface-parameters keepalive** command.
Hold Time (sec)	The Hold Time value (also referred to as Hello Timeout) determines the amount of time, in seconds, LDP waits to receive hello messages from a peer before declaring that the peer is down. Configured through the **configure router ldp interface-parameters hello** command.

output definitions

Hello Factor	The Hello factor value that is divided into the Hold Time value to determine the interval at which Hello messages are sent from this interface. Configured through the **configure router ldp interface-parameters hello** command.
Passive Mode	Whether or not passive mode is active (**True** or **False**). When passive mode is active, LDP responds only when a connect request is received from a peer and does not actively try to connect with peers. When this mode is not active, LDP actively tries to connect to peers.
Targeted Sessions	The status of targeted sessions (**Enabled** or **Disabled**).

Release History

Release 6.4.2; command was introduced.

Related Commands

show router ldp interface	Displays the LDP interface configuration for the local router.
show router ldp discovery interface	Displays the discovery status of the LDP Hello adjacencies associated with the specified LDP interface.

MIB Objects

show router ldp peer

Displays configuration information for LDP peers.

show router ldp peer [*ip-address***] [detail]**

Syntax Definitions

ip-address	The IP address of an LDP peer.
detail	Displays detailed information for the specified peers.

Defaults

By default, the configuration for all LDP peers is displayed.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the *ip-address* parameter to display information for a specific LDP peer.
- Use the **detail** parameter to display additional information and statistics for the specified LDP peers.

Examples

```
->show router ldp peer
LDP Peers

Peer              Adm  Opr  Hello   Hold    KA      KA       Passive   Auto
                            Factor  Time    Factor  Timeout  Mode      Created
------------------+----+----+-------+-------+-------+--------+---------+--------
10.11.0.6         Up   Up   3       45      4       40       Disabled  Yes
20.1.2.3          Up   Up   3       45      4       40       Disabled  Yes
30.1.2.3          Up   Up   3       45      4       40       Disabled  Yes

No. of Peers: 3

->show router ldp peer detail
LDP Peers (Detail)

    Peer 10.11.0.66
      Admin State:         Up,              Oper State:        Up,
      Hold Time:           45,              Hello Factor:      3,
      Keepalive Timeout:   40,              Keepalive Factor:  3,
      Passive Mode:        Disabled,       Last Modified:     05/26/2009 23:14:27,
      Active Adjacencies:  1,               d:      Yes,
      Tunneling:           Disabled,
      Lsp Name:            None
```

```
->show router ldp peer 10.11.0.6
LDP Peers

Peer              Adm  Opr  Hello   Hold    KA      KA       Passive   Auto
                            Factor  Time    Factor  Timeout  Mode      Created
------------------+----+----+-------+-------+-------+--------+---------+--------
10.11.0.6         Up   Up   3       45      4       40       Disabled  Yes

No. of Peers: 1

->show router ldp peer 10.11.0.66 detail
LDP Peers (Detail)

    Peer 10.11.0.66
      Admin State:         Up,              Oper State:        Up,
      Hold Time:           45,              Hello Factor:      3,
      Keepalive Timeout:   40,              Keepalive Factor:  4,
      Passive Mode:        Disabled,        Last Modified:     05/26/2009 23:14:27,
      Active Adjacencies:  1,               d:      Yes,
      Tunneling:           Disabled,
      Lsp Name:            None
```

output definitions

Peer	The IP address of the LDP peer.
Adm	The administrative state of the LDP peer (**Up** or **Down**).
Opr	The operational state of the LDP peer (**Up** or **Down**).
Hello Factor	The Hello factor value that is divided into the Hold Time value to determine the interval at which Hello messages are sent. LDP uses hello messages to discover neighbors and to detect loss of connectivity with its neighbors.
Hold Time	The Hold Time value (also referred to as Hello Timeout) determines the amount of time, in seconds, LDP waits to receive hello messages from a peer before declaring that the peer is down.
KA Factor	The Keepalive Factor value that is divided into the Keepalive Timeout value to determine the interval at which Keepalive messages are sent. LDP keepalive messages are sent to keep the LDP session from timing out when no other LDP traffic is sent between neighbors.
KA Timeout	The amount of time, in seconds, LDP waits to receive keepalive messages from an LDP peer before tearing down the session with that peer.
Passive Mode	Whether or not passive mode is active (**True** or **False**). When passive mode is active, LDP responds only when a connect request is received from a peer and does not actively try to connect with peers. When this mode is not active, LDP actively tries to connect to peers.
Auto Created	Indicates if a targeted peer was automatically created through service manager (**Yes** or **No**). This value is always **No** for an LDP interface.
Last Modified	The date and time the interface configuration was last modified.
Active Adjacencies	The number of active adjacencies between this interface and LDP peers.

output definitions

Tunneling	The tunneling status for the peer (**Enabled** or **Disabled**).
Lsp Name	The name of the Label Switch Path (LSP) associated with the peer.

Release History

Release 6.4.2; command was introduced.

Related Commands

show router ldp discovery peer	Displays the discovery status of the LDP Hello adjacencies associated with the specified LDP peer.
show router ldp discovery interface	Displays the discovery status of the LDP Hello adjacencies associated with the specified LDP interface.

MIB Objects

show router ldp session

Displays configuration information and statistics for LDP sessions.

show router ldp session [*ip-address***[***:label-space***]] [detail | statistics [***packet-type***]]**

Syntax Definitions

ip-address	The IP address of an LDP peer.
:label-space	The label space ID number that the router advertises on the LDP interface. This value is appended to the LDP router ID address. The valid range is 0–65535.
detail	Displays detailed information for the specified sessions.
packet-type	Displays session information for a specific packet type. Valid packet type entries for this parameter are **hello**, **keepalive**, **init**, **label**, **notification**, and **address**.

Defaults

By default, information is displayed for all LDP sessions.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the *ip-address* and *:label-space* parameters to display information for a specific LDP session. Note that entering a label-space value is not required when specifying an IP address.
- The **detail** parameter is available for use with the base command (**show router ldp session**) and in combination with the *ip-address* parameter to show additional information for a specific LDP session.
- The **statistics** parameter is available for use with the base command (**show router ldp session**), but is not used in combination with the *ip-address* parameter. Note that specifying a packet type with this parameter is optional; if no type is specified, statistics are displayed for all types.

Examples

```
->show router ldp session
LDP Sessions

Peer LDP Id        Adj Type   State         Msg Sent  Msg Recv  Up Time
------------------+----------+-------------+---------+---------+-------------
10.11.0.6:0        Both       Established   73211     73213     1d 23:00:59
10.11.0.66:0       Targeted   Established   2417      2419      0d 03:40:28

No. of Sessions: 2

->show router ldp session 10.11.0.66
LDP Sessions
```

```
Peer LDP Id       Adj Type   State        Msg Sent  Msg Recv  Up Time
------------------+----------+------------+---------+---------+-------------
10.11.0.66:0       Targeted   Established   2451      2453      0d 03:43:32

No. of Sessions: 1

->show router ldp session detail
LDP Sessions (Detail)

    Session with Peer 10.10.0.7:0
      Adjacency Type:     Link,           State:                  Established,
      Up Time:            0d 03:42:56,
      Max PDU Length:     4096,           KA/Hold Time Remaining: 25,
      Link Adjacencies:   1,              Targeted Adjacencies:   0,
      Local Address:      10.11.0.6,      Peer Address:           10.10.0.7,
      Local TCP Port:     2364,           Peer TCP Port:          646,
      Local KA Timeout:   30,             Peer KA Timeout:        30,
      Mesg Sent:          4830,           Mesg Recv:              4829,
      FECs Sent:          2,              FECs Recv:              2,
      GR In Progress:     No,             GR Helper State:        Capable,
      Advrt Reconn Time:  120,            Advrt Recovery Time:    0,
      Nbr Liveness Time:  0,              Max Recovery Time:      0,
       Number of Restart:  0,              Last Restart Time:      01/01/1970
00:00:00,
      Advertise:          Address

    Session with Peer 10.11.0.66:0
      Adjacency Type:     Targeted,       State:                  Established,
      Up Time:            0d 03:42:02,
      Max PDU Length:     4096,           KA/Hold Time Remaining: 38,
      Link Adjacencies:   0,              Targeted Adjacencies:   1,
      Local Address:      10.11.0.6,      Peer Address:           10.11.0.66,
      Local TCP Port:     646,            Peer TCP Port:          50353,
      Local KA Timeout:   40,             Peer KA Timeout:        40,
      Mesg Sent:          2435,           Mesg Recv:              2437,
      FECs Sent:          1,              FECs Recv:              1,
      GR In Progress:     No,             GR Helper State:        Not Capable,
      Advrt Reconn Time:  120,            Advrt Recovery Time:    0,
      Nbr Liveness Time:  0,              Max Recovery Time:      0,
       Number of Restart:  0,              Last Restart Time:      01/01/1970
00:00:00,
      Advertise:          Service

->show router ldp session statistics
LDP Session Statistics

    Session 10.10.0.7:0
      Hello_Tx:           3378,           Hello_Rx:               3377,
      Keepalive_Tx:       1496,           Keepalive_Rx:           1496,
      Init_Tx:            1,              Init_Rx:                1,
      Label_Mapping_Tx:   2,              Label_Mapping_Rx:       2,
      Label_Request_Tx:   0,              Label_Request_Rx:       0,
      Label_Release_Tx:   0,              Label_Release_Rx:       0,
      Label_Withdraw_Tx:  0,              Label_Withdraw_Rx:      0,
      Label_Abort_Tx:     0,              Label_Abort_Rx:         0,
      Notification_Tx:    0,              Notification_Rx:        0,
      Address_Tx:         1,              Address_Rx:             1,
      Address_Withdraw_Tx:0,              Address_Withdraw_Rx:    0
```

```
    Session 10.11.0.66:0
      Hello_Tx:           960,            Hello_Rx:              962,
      Keepalive_Tx:       1495,           Keepalive_Rx:          1495,
      Init_Tx:            1,              Init_Rx:               1,
      Label_Mapping_Tx:   1,              Label_Mapping_Rx:      1,
      Label_Request_Tx:   0,              Label_Request_Rx:      0,
      Label_Release_Tx:   0,              Label_Release_Rx:      0,
      Label_Withdraw_Tx:  0,              Label_Withdraw_Rx:     0,
      Label_Abort_Tx:     0,              Label_Abort_Rx:        0,
      Notification_Tx:    0,              Notification_Rx:       0,
      Address_Tx:         1,              Address_Rx:            1,
      Address_Withdraw_Tx:0,              Address_Withdraw_Rx:   0

->show router ldp session statistics address
LDP Session Statistics (Address)

    Session 10.10.0.7:0
      Address_Tx:         1,              Address_Rx:            1,
      Address_Withdraw_Tx:0,              Address_Withdraw_Rx:   0

    Session 10.11.0.66:0
      Address_Tx:         1,              Address_Rx:            1,
      Address_Withdraw_Tx:0,              Address_Withdraw_Rx:   0

->show router ldp session statistics init
LDP Session Statistics (Init)

    Session 10.10.0.7:0
      Init_Tx:            1,              Init_Rx:               1

    Session 10.11.0.66:0
      Init_Tx:            1,              Init_Rx:               1

->show router ldp session statistics keepalive
LDP Session Statistics (Keepalive)
    Session 10.10.0.7:0
      Keepalive_Tx:       1496,           Keepalive_Rx:          1496

    Session 10.11.0.66:0
      Keepalive_Tx:       1495,           Keepalive_Rx:          1495

->show router ldp session statistics label
LDP Session Statistics (Label)
    Session 10.10.0.7:0
      Label_Mapping_Tx:   2,              Label_Mapping_Rx:      2,
      Label_Request_Tx:   0,              Label_Request_Rx:      0,
      Label_Release_Tx:   0,              Label_Release_Rx:      0,
      Label_Withdraw_Tx:  0,              Label_Withdraw_Rx:     0,
      Label_Abort_Tx:     0,              Label_Abort_Rx:        0

    Session 10.11.0.66:0
      Label_Mapping_Tx:   1,              Label_Mapping_Rx:      1,
      Label_Request_Tx:   0,              Label_Request_Rx:      0,
      Label_Release_Tx:   0,              Label_Release_Rx:      0,
      Label_Withdraw_Tx:  0,              Label_Withdraw_Rx:     0,
      Label_Abort_Tx:     0,              Label_Abort_Rx:        0
```

output definitions

Peer LDP Id	The IP address of the LDP peer.
Adj Type	The type of adjacency (**Link**—adjacency is the result of a Link Hello; **Targeted**—the adjacency is the result of a Targeted Hello).
State	The state of the adjacency (**Established** or **Trying**).
Msg Sent	The number of messages sent for this adjacency.
Msg Rcvd	The number of messages received for this adjacency.
Up Time	The amount of time the adjacency has been enabled.

Release History

Release 6.4.2; command was introduced.

Related Commands

show router ldp status	Displays status information and statistics for the LDP instance on the local router.
show router ldp parameters	Displays the LDP graceful restart, interface, and targeted session parameter values for the local router.
show router ldp interface	Displays the LDP interface configuration for the local router.

MIB Objects

show router ldp status

Displays status information and statistics for the LDP instance on the local router.

show router ldp status

Syntax Definitions

N/A.

Defaults

N/A.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

Use the information and statistics displayed with this command to determine the status of the local LDP instance.

Examples

```
->show router ldp status
LDP Status for LSR ID 10.10.0.7
  Admin State:         Up,                   Oper State:                Up,
  Created at:           03/25/2009 16:08:06,  Up Time:                     0d
18:38:14,
  Last Change:         03/25/2009 16:08:06,  Tunn Down Damp Time (sec):  N/A,
  Import Policies:      None,                Export Policies:           None,
  Active Adjacencies:  2,                    Active Sessions:           2,
  Active Interfaces:   1,                    Inactive Interfaces:       0,
  Active Peers:        1,                    Inactive Peers:            0,
  Addr FECs Sent:      1,                    Addr FECs Recv:            2,
  Serv FECs Sent:      1,                    Serv FECs Recv:            1,
  Attempted Sessions:  0,
  No Hello Err:        0,                    Param Adv Err:             0,
  Max PDU Err:         0,                    Label Range Err:           0,
  Bad LDP Id Err:      0,                    Bad PDU Len Err:           0,
  Bad Mesg Len Err:    0,                    Bad TLV Len Err:           0,
  Malformed TLV Err:   0,                    Keepalive Expired Err:     0,
  Shutdown Notif Sent: 0,                     Shutdown Notif Recv:       0
```

output definitions

Adm	The administrative state of the LDP instance (**Up** or **Down**).
Opr	The operational state of the LDP instance (**Up** or **Down**).
Created at	The date and time the LDP instance was created.
Up Time	The length of time, in hundredths of seconds, that the LDP instance has been operationally up.

output definitions

Last Change	The date and time the LDP instance was last modified.
Tunn Down Damp Time (sec)	The amount of time, in seconds, the tunnel has been down.
Import Policies	None (not supported).
Export Policies	None (not supported).
Active Adjacencies	The number of active adjacencies (established sessions) associated with this LDP instance.
Active Sessions	The number of sessions in the process of actively attempting to establish a session.
Active Interfaces	The number of active (operationally up) interfaces associated with this LDP instance.
Inactive Interfaces	The number of inactive (operationally down) interfaces associated with this LDP instance.
Active Peers	The number of active LDP peers.
Inactive Peers	The number of inactive LDP peers.
Addr FECs Sent	The number of address (prefix) FEC labels sent to the peer associated with the FEC.
Addr FECs Recv	The number of address (prefix) FEC labels received from the peer associated with the FEC.
Serv FECs Sent	The number of service FEC labels sent to the peer associated with the FEC.
Serv FECs Recv	The number of service FEC labels received from the peer associated with the FEC.
Attempted Sessions	The number of attempted sessions for this LDP instance.
No Hello Err	The number of “Session Rejected” or “No Hello Error” notification messages sent or received by this LDP instance.
Param Adv Err	The number of “Session Rejected” or “Parameters Advertisement Mode Error” notification messages sent or received by this LDP instance.
Max PDU Err	The number of “Session Rejected” or “Parameters Max PDU Length Error” notification messages sent or received by this LDP instance.
Label Range Err	The total number of “Session Rejected” or “Parameters Label Range Error” notification messages sent or received by this LDP instance.
Bad LDP Id Err	The number of bad LDP identifier fatal errors detected for sessions associated with this LDP instance.
Bad PDU Len Err	The number of bad PDU length fatal errors detected for sessions associated with this LDP instance.
Bad Mesg Len Err	The number of bad message length fatal errors detected for sessions associated with this LDP instance.
Bad TLV Len Err	The number of bad TLV length fatal errors detected for sessions associated with this LDP instance.
Malformed TLV Err	The number of malformed TLV value fatal errors detected for sessions associated with this LDP instance.

output definitions

Keepalive Expired Err	The number of session Keepalive timer expired errors detected for sessions associated with this LDP instance.
Shutdown Notif Sent	The number of shutdown notifications sent related to sessions associated with this LDP instance.
Shutdown Notif Recv	The number of shutdown notifications received related to sessions associated with this LDP instance.

Release History

Release 6.4.2; command was introduced.

Related Commands

show router ldp session	Displays configuration information and statistics for LDP sessions.
show router ldp parameters	Displays the LDP graceful restart, interface, and targeted session parameter values for the local router.
show router ldp interface	Displays the LDP interface configuration for the local router.

MIB Objects

55 MPLS Static LSP and FRR Commands

MPLS forwarding is performed by routers called Label Switching Routers (LSRs). A Label Switched Path (LSP) is a path through one or more LSRs.

There are two types of LSPs that are configurable using MPLS:

- **Static LSPs**. A Static LSP specifies a statically defined path of LSRs. Configuration of label mappings and MPLS actions is required on each router that will participate in the static path. No signaling protocol, such as the Label Distribution Protocol (LDP), is required, and there is no dependence on a gateway protocol topology or local forwarding table. Static LSPs are able to cross an Autonomous System (AS) boundary.
- **Signaled LSP**. The LSPs are set up using a signaling protocol, such as LDP. The signaling protocol allows the automatic assignment of labels from an ingress router to the egress router. Signaling is triggered by the ingress router, therefore configuration is only required on this router. A signaled LSP is confined to one gateway protocol area and, therefore, cannot cross an AS boundary.

In addition to static LSPs, a static Fast Reroute feature is available that allows the configuration of backup static LSP tunnels.FRR uses the backup tunnels for alternate routes in the event an LSP goes down.

This chapter provides information about the Command Line Interface (CLI) commands used to configure static LSPs and backup static LSPs used by the FRR mechanism. For information about LDP commands used to configure signaled LSPs, see Chapter 54, “MPLS LDP Commands.”

MIB information for static LSP is as follows:

Filename: TIMETRA-MPLS-MIB.mib
Module: TIMETRA-MPLS-MIB

MIB information for static FRR is as follows:

Filename: AlcatelStaticFrr.mib file
Module: ALCATEL-STATIC-FRR-MIB

The following table summarizes the available static LSP and static FRR commands:

Static LSP Commands for All Routers	**configure router mpls shutdown** **configure router mpls interface** **configure router mpls interface shutdown**
Static LSP Commands for Transit Router Configuration	**configure router mpls interface label-map** **configure router mpls interface label-map swap next-hop** **configure router mpls interface label-map shutdown**
Static LSP Commands for Egress Router Configuration	**configure router mpls interface label-map pop** **configure router mpls interface label-map shutdown**
Static LSP Commands for Ingress Router Configuration	**configure router mpls static-lsp** **configure router mpls static-lsp to** **configure router mpls static-lsp push next-hop** **configure router mpls static-lsp shutdown**
Static FRR Command	**configure router mpls interface label-map protect-swap next-hop**
Show Commands	**show router mpls interface** **show router mpls label** **show router mpls label-range** **show router mpls static-lsp** **show router mpls status**

configure router mpls shutdown

Configures the administrative status of the MPLS protocol instance.

configure router mpls {no shutdown | shutdown}

Syntax Definitions

no shutdown	Enables the MPLS protocol instance.
shutdown	Disables the MPLS protocol instance.

Defaults

By default, MPLS is enabled for the switch.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Disabling the MPLS instance disables the Label Switched Paths attached to the instance, as well as any Service Distribution Points (SDPs) and SDP bindings associated with the LSP. When the MPLS instance is once again enabled, the attached LSPs will attempt to re-activate.
- Note that deleting the MPLS instance is not allowed; there is no command for this purpose. Only changing the administrative status of the instance is allowed.

Examples

```
-> configure router mpls no shutdown
-> configure router mpls shutdown
```

Release History

Release 6.4.2; command was introduced.

Related Commands

show router mpls status	Displays the status of the MPLS instance on the router.

MIB Objects

```
vRtrMplsGeneralTable
   vRtrMplsGeneralAdminState
```

configure router mpls interface

Configures MPLS support on an IP interface.

configure router mpls interface *ip-intf-name*

configure router mpls no interface *ip-intf-name*

Syntax Definitions

ip-intf-name	The name of an existing IP interface.

Defaults

By default, the MPLS interface is administratively enabled when the interface is created.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to remove the MPLS interface. Disable the administrative status of the interface before attempting to remove it.
- When the MPLS interface configuration is removed, any label maps or protect-swap label maps associated with the interface are also removed. However, static LSPs associated with the interface are not removed; the static LSP configuration on the router remains in tact.
- The IP interface name specified with this command must already exist in the router configuration.
- Until MPLS support is configured on an IP interface, no other MPLS configuration tasks are allowed on that interface.

Examples

```
-> configure router mpls interface vlan-20
-> configure router mpls no interface vlan-20
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure router mpls interface shutdown	Configures the administrative status for the specified MPLS interface.
show router mpls interface	Displays the MPLS interface configuration.

MIB Objects

```
vRtrIfTable
   vRtrIfMplsStatus
```

configure router mpls interface shutdown

Configures the administrative status for specified MPLS interface.

configure router mpls interface *ip-intf-name* **{no shutdown | shutdown}**

Syntax Definitions

ip-intf-name	The name of an existing MPLS IP interface.
no shutdown	Enables the MPLS administrative status for the interface.
shutdown	Disables the MPLS administrative status for the interface.

Defaults

By default, the administrative status of an MPLS interface is enabled.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Disabling the administrative status for an MPLS interface does not remove the MPLS configuration from that interface. However, any Label Switched Paths (LSPs) associated with the MPLS interface are also administratively disabled.
- When a disabled MPLS interface is enabled, any associated LSPs are also enabled.
- The MPLS interface name specified with this command must already exist in the router configuration.

Examples

```
-> configure router mpls interface vlan-20 no shutdown
-> configure router mpls interface vlan-20 shutdown
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure router mpls interface	Configures MPLS support on an IP interface.
show router mpls interface	Displays the MPLS interface configuration.

MIB Objects

```
vRtrMplsIfTable
   vRtrMplsIfAdminState
```

configure router mpls interface label-map

Configures an incoming label number that the specified MPLS interface will process. Use this command to provide this information on each transit and egress router that participates in a static Label Switched Path (LSP).

configure router mpls interface *ip-intf-name* **label-map** *in-label*

configure router mpls interface *ip-intf-name* **no label-map** *in-label*

Syntax Definitions

ip-intf-name	The name of an existing MPLS IP interface.
in-label	An incoming label number. The valid range is 32–1023.

Defaults

N/A

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to remove the incoming label map.
- Once created, the incoming label-map number is then associated with a swap (transit router) or pop (egress router) action.
- The label-map number and associated action is not active until the label-map is administratively enabled.

Examples

```
-> configure router mpls interface vlan-20 label-map 700
-> configure router mpls interface vlan-20 no label-map 700
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure router mpls interface	Configures MPLS support on an IP interface.
configure router mpls interface label-map swap next-hop	Configures the outgoing label number that is swapped for the specified incoming label number and the IP address for the next router in the static LSP.
configure router mpls interface label-map pop	Configures a pop (remove) label operation to identify the router as an egress (endpoint) router for the static LSP.
configure router mpls interface label-map shutdown	Configures the administrative status for the label mapping.
show router mpls label	Displays the MPLS labels that are exchanged.

MIB Objects

```
mplsInSegmentTable
   mplsInSegmentRowStatus
```

configure router mpls interface label-map swap next-hop

Configures the outgoing label number that is swapped for the specified incoming label number. Also configures the next-hop IP address in the static Label Switched Path (LSP). Use this command to provide this information on each transit router that participates in the static LSP.

configure router mpls interface *ip-intf-name* **label-map** *in-label* **swap** *out-label* **next-hop** *ip-address*

configure router mpls interface *ip-intf-name* **label-map** *in-label* **no swap**

Syntax Definitions

ip-intf-name	The name of an existing MPLS IP interface.
in-label	An incoming label number. The valid range is 32–1023.
out-label	An outgoing label number. The valid range is 32–1023.
ip-address	The IP address for the next-hop router.

Defaults

N/A

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to remove the outgoing label and the associated next-hop IP address.
- If an ARP entry for the next hop exists, then the static LSP is marked as operational. If an ARP entry does not exist, then the static LSP is marked as operationally down and the local router continues to ARP for the configured next hop at a fixed interval..

Examples

```
-> configure router mpls interface vlan-20 label-map 700 swap 555 next-hop
192.168.10.2
-> configure router mpls interface vlan-20 no label-map 700 no swap
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure router mpls interface	Enables MPLS Protocol support on an IP interface.
configure router mpls interface label-map	Configures an incoming label number that the specified MPLS interface will process.
configure router mpls interface label-map pop	Configures a pop (remove) label operation to identify the router as an egress (endpoint) router for the static LSP.
configure router mpls interface label-map shutdown	Configures the administrative status for the label mapping.
show router mpls label	Displays the MPLS labels that are exchanged.

MIB Objects

```
mplsInSegmentTable
   mplsInSegmentXCIndex
mplsOutSegmentTable
   mplsOutSegmentTopLabel
   mplsOutSegmentNextHopIpAddrType
   mplsOutSegmentNextHopIpv4Addr
   mplsOutSegmentXCIndex
   mplsOutSegmentRowStatus
mplsXCTable
   mplsXCRowStatus
```

configure router mpls interface label-map pop

Configures a label pop operation for the packet containing the specified incoming label number. This action is configured on an egress Label Edge Router (LER) to identify the end of MPLS switching and the static Label Switched Path (LSP).

configure router mpls interface *ip-intf-name* **label-map** *in-label* **pop**

configure router mpls interface *ip-intf-name* **label-map** *in-label* **no pop**

Syntax Definitions

ip-intf-name	The name of an existing MPLS IP interface.
in-label	Incoming label number. The valid range is 32–1023.

Defaults

N/A

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to stop the label pop operation and remove the egress router designation for this router.
- When the egress LER receives a packet with the specified label number, the label is popped off (removed from) the packet. Once the label is removed from the packet, the associated service directs any further action with the packet.

Examples

```
-> configure router mpls interface vlan-20 label-map 800 pop
-> configure router mpls interface vlan-20 no label-map 800 no pop
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure router mpls interface	Enables MPLS Protocol support on an IP interface.
configure router mpls interface label-map	Configures an incoming label number that the specified MPLS interface will process.
configure router mpls interface label-map swap next-hop	Configures the outgoing label number that is swapped for the specified incoming label number and the IP address for the next router in the static LSP.
configure router mpls interface label-map shutdown	Configures the administrative status for the label mapping.
show router mpls label	Displays the MPLS labels that are exchanged.

MIB Objects

```
mplsInSegmentTable
   mplsInSegmentXCIndex
mplsOutSegmentTable
   mplsOutSegmentXCIndex
   mplsOutSegmentRowStatus
mplsXCTable
   mplsXCRowStatus
```

configure router mpls interface label-map shutdown

Configures the administrative status for an incoming label-map on a transit Label Switch Router (LSR) or on an egress Label Edge Router (LER).

configure router mpls interface *ip-intf-name* **label-map** *in-label* **{no shutdown | shutdown}**

Syntax Definitions

ip-intf-name	The name of an existing MPLS IP interface.
in-label	Incoming label-map number. The valid range is 32–1023.
no shutdown	Enables the administrative status of the specified label-map.
shutdown	Disables the administrative status of the specified label-map.

Defaults

By default, the incoming label-map is disabled at the time the label-map is created.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- The MPLS interface and incoming label-map number specified with this command must already exist in the router configuration.
- Disabling the administrative status of the label-map does not remove the label-map configuration from the router.
- When the label-map is disabled, any packets ingressing on the router that contain the label-map number are dropped.

Examples

```
-> configure router mpls interface vlan-20 label-map 700 shutdown
-> configure router mpls interface vlan-20 label-map 700 no shutdown
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure router mpls interface	Enables MPLS Protocol support on an IP interface.
configure router mpls interface label-map	Configures an incoming label number that the specified MPLS interface will process.
configure router mpls interface label-map swap next-hop	Configures the outgoing label number that is swapped for the specified incoming label number and the next-hop router IP address for the static LSP.
configure router mpls interface label-map pop	Configures a pop (remove) label operation to identify the router as an egress (endpoint) router for the static LSP.
show router mpls interface	Displays the MPLS interface configuration.

MIB Objects

```
mplsInSegmentTable
   mplsInSegmentXCIndex
mplsXCTable
   mplsXCAdminStatus
```

configure router mpls static-lsp

Configures a static Label Switched Path (LSP) instance on an ingress Label Edge Router (LER).

configure router mpls static-lsp *lsp-name*

configure router mpls no static-lsp *lsp-name*

Syntax Definitions

lsp-name	An alphanumeric name, up to 32 characters, to assign to the static LSP.

Defaults

N/A

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- To remove this static LSP configuration from the ingress router, administratively disable (shutdown) the LSP and then use the **no** form of this command to remove the configuration from the router.
- The Static LSP instance is identified by the LSP name on the ingress router and by the MPLS interface name and ingress label combination on both transit and egress routers.
- Configuring the static LSP instance is done only on the ingress LER to identify the origination point of the LSP.
- Once the static LSP is created and associated with a name, configuring the destination IP address, the push operation, and the next-hop router IP address for the LSP is required.

Examples

```
-> configure router mpls static-lsp to-R3
-> configure router mpls no static-lsp to-R3
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure router mpls static-lsp shutdown	Configures the administrative status of the static LSP.
configure router mpls static-lsp to	Configures the destination System IP address for the static LSP.
configure router mpls static-lsp push next-hop	Pushes the specified label on to the label stack and specifies the IP address for the next-hop router in the static LSP.
show router mpls static-lsp	Displays static LSP configuration information.

MIB Objects

```
vRtrMplsLspTable
   vRtrMplsLspRowStatus
   vRtrMplsLspName
```

configure router mpls static-lsp shutdown

Configures the administrative status for the specified static Label Switched Path (LSP).

configure router mpls static-lsp *lsp-name* **{no shutdown | shutdown}**

Syntax Definitions

lsp-name	The name of an existing static LSP.
no shutdown	Enables the administrative status of the specified static LSP.
shutdown	Disables the administrative status of the specified static LSP.

Defaults

By default, the static LSP is disabled when the LSP is created.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- The LSP name specified with this command must already exist in the router configuration.
- Disabling the administrative status of the static LSP does not remove the LSP configuration from the router, however, packet forwarding to the next-hop router is stopped. When a disabled static LSP is enabled, packet forarding continues.

Examples

```
-> configure router mpls static-lsp to-R3 no shutdown
-> configure router mpls static-lsp to-R3 shutdown
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure router mpls static-lsp	Configures a static LSP on an ingress router.
configure router mpls static-lsp to	Configures the destination System IP address for the static LSP.
configure router mpls static-lsp push next-hop	Pushes the specified label on to the label stack and specifies the IP address for the next-hop router in the static LSP.
show router mpls static-lsp	Displays static LSP configuration information.

MIB Objects

```
vRtrMplsLspTable
   vRtrMplsLspAdminState
```

configure router mpls static-lsp to

Configures the destination system IP address for the specified static LSP. This is configured on the ingress router to identify the destination router for the static LSP.

configure router mpls static-lsp *lsp-name* **to** *ip-address*

Syntax Definitions

lsp-name	The name of an existing static LSP.
ip-address	The system IP address of the egress router. This is the configured Loopback0 address on an OmniSwitch.

Defaults

N/A

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- The System IP address specified with this command should match the System IP address for the far-end router of the SDP to which the static LSP is attached.
- The LSP name specified with this command must already exist in the router configuration.
- This command is also used to configure backup static LSP tunnels. To create a backup tunnel, configure a static LSP with the same destination system IP address as the protected (primary) tunnel, but with a different LSP name.
- Up to 16 backup LSP tunnels are supported per Service Distribution Point (SDP).
- Configuring a backup static LSP activates the static Fast ReRoute (FRR) mechanism that will redirect traffic to a backup tunnel should the protected LSP tunnel goes down.

Examples

```
-> configure router mpls static-lsp to-R3 to 10.10.10.3
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure router mpls static-lsp	Configures a static LSP on an ingress LER.
configure router mpls static-lsp shutdown	Configures the administrative status of the static LSP.
configure router mpls static-lsp push next-hop	Pushes the specified label on to the label stack and specifies the system IP address for the next-hop router in the static LSP.
show router mpls static-lsp	Displays static LSP configuration information.

MIB Objects

```
vRtrMplsLspTable
   vRtrMplsLspToAddr
```

configure router mpls static-lsp push next-hop

Pushes the specified label on to the label stack and specifies the IP address for the next-hop router in the static Label Switched Path (LSP). After the push operation is complete, the packet is then forwarded to the specified next-hop router.

configure router mpls static-lsp *lsp-name* **push** *out-label* **next-hop** *ip-address*

configure router mpls static-lsp *lsp-name* **no push** *out-label*

Syntax Definitions

lsp-name	The existing LSP name.
out-label	An outgoing label number. The valid range is 32–1023.
ip-address	The next-hop router IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to remove the push label configuration associated with the static LSP.
- The LSP name specified with this command must already exist in the router configuration.
- If an ARP entry for the next hop exists, then the static LSP is marked as operational. If an ARP entry does not exist, then the static LSP is marked as operationally down and the local router continues to ARP for the configured next hop at a fixed interval.

Examples

```
-> configure router mpls static-lsp to-R3 push 777 next-hop 192.168.10.2
-> configure router mpls static-lsp to-R3 no push 777
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure router mpls static-lsp	Configures a static LSP on an ingress LER.
configure router mpls static-lsp shutdown	Configures the administrative status of the static LSP.
configure router mpls static-lsp to	Configures the system IP address of the static LSP egress router.
show router mpls static-lsp	Displays static LSP configuration information.

MIB Objects

```
vRtrMplsLspTable
   vRtrMplsLspOutSegIndx
mplsOutSegmentTable
   mplsOutSegmentTopLabel
   mplsOutSegmentNextHopIpAddrType
   mplsOutSegmentNextHopIpv4Addr
   mplsOutSegmentXCIndex
   mplsOutSegmentRowStatus
mplsXCTable
   mplsXCRowStatus
```

configure router mpls interface label-map protect-swap next-hop

Configures static Fast Reroute (FRR) protection on a transit Label Switch Router (LSR). This command defines an alternate static swap label-map that FRR will use if the next-hop segment goes down.

configure router mpls interface *ip-intf-name* **label-map** *in-label* **protect-swap** *out-label* **next-hop** *ip-address*

configure router mpls interface *ip-intf-name* **label-map** *in-label* **no protect-swap**

Syntax Definitions

ip-intf-name	The name of an existing MPLS IP interface.
in-label	An incoming label number. The valid range is 32–1023.
out-label	An outgoing label number. The valid range is 32–1023.
ip-address	The next-hop router IP address.

Defaults

N/A.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to remove the FRR configuration.
- Dynamic FRR is not supported on the OmniSwitch; only static FRR is supported. Static FRR is not compatible with dynamic FRR, which is supported on other Alcatel-Lucent platforms. As a result, a router with dynamic FRR enabled cannot set up backup paths with a downstream node that is an OmniSwitch router.

Examples

```
-> configure router mpls interface vlan-20 label-map 556 protect-swap 557 next hop
192.168.10.2
-> configure router mpls interface vlan-20 label-map 556 no protect-swap
```

Release History

Release 6.4.2; command was introduced.

Related Commands

show router mpls label	Displays information about MPLS labels.
show router mpls static-lsp	Displays the static LSP configuration.

MIB Objects

```
vRtrStaticFrrMplsInSegmentTable
   vRtrStaticFrrMplsInSegmentXCIndex
   mplsInSegmentRowStatus
vRtrStaticFrrMplsOutSegmentTable
   vRtrStaticFrrMplsOutSegmentTopLabel
   vRtrStaticFrrMplsOutSegmentNextHopIpAddrType
   vRtrStaticFrrMplsOutSegmentNextHopIpv4Addr
   vRtrStaticFrrMplsOutSegmentXCIndex
   vRtrStaticFrrMplsOutSegmentRowStatus
vRtrStaticFrrMplsXCTable
   vRtrStaticFrrMplsXCRowStatus
```

show router mpls interface

Displays the MPLS interface configuration.

show router mpls interface [*ip-intf-nam***e] [label-map** *label* **[protect-swap [***out-label***]]]**

Syntax Definitions

ip-intf-name	The name of an existing MPLS IP interface.
label	A label number. The valid range is 32–131071.
out-label	The outgoing label number for a protected LSP association. The valid range is 32–131071.

Defaults

By default, the configuration for all MPLS interfaces is displayed.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the command parameters provided to display information for specific interfaces.
- Fields that contain “N/A” are not supported.

Examples

```
-> show router mpls interface

MPLS Interfaces

Interface                        Port-id           Adm    Opr Te-metric
---------------------------------+-----------------+------+------+-------
vlan-20                           N/A               Up     Up     N/A
vlan-40                           N/A               Up     Up     N/A
vlan-22                           N/A               Up     Up     N/A
vlan-23                           N/A               Up     Up     N/A

Interfaces : 4

-> show router mpls interface vlan-20

Interface                         Port-id           Adm    Opr Te-metric
---------------------------------+-----------------+------+------+-------
vlan-20                           N/A               Up     Up     N/A

Interfaces : 1
```

```
-> show router mpls interface label-map

MPLS Interfaces (Label-Map)

In Label  In I/F     Out Label Out I/F    Next Hop          Type     Adm  Opr
---------+----------+---------+----------+-----------------+---------+----+----
400       vlan-20    440       vlan-22    22.22.22.1*       Static    Up  Up
728       vlan-20    730       vlan-20    20.20.20.1*       Static    Up  Up
732       vlan-20    N/A       N/A        N/A               Static    Up  Up
800       vlan-20    840       vlan-22    22.22.22.1*       Static    Up  Up
840       vlan-20    N/A       N/A        N/A               Static   Down Up
900       vlan-20    920       vlan-22    22.22.22.1*       Static    Up  Up
1000      vlan-20   1020       vlan-22    22.22.22.1*       Static    Up  Up

Interfaces : 7

-> show router mpls interface label-map 400

MPLS Interfaces

Interface                         Port-id         Adm    Opr    Te-metric
----------------------------------+---------------+------+----------+-
vlan-20                            N/A             Up     Up     N/A
vlan-40                            N/A             Up     Up     N/A
vlan-21                            N/A             Up     Up     N/A
vlan-22                            N/A             Up     Up     N/A
vlan-23                            N/A             Up     Up     N/A

Interfaces : 5

-> show router mpls interface label-map protect-swap

MPLS Interfaces (Label-Map)

                   Protected   Protected  Protected
In Label  In I/F   Out Label   Out I/F       Next Hop       Type Adm  Opr
---------+----------+---------+-------------+-----------------+---------+--
400      N/A      480        N/A         23.23.23.1    Static    Up    Up
1000     N/A      1080       N/A         40.40.40.1    Static    Up    Up

Interfaces : 2

-> show router mpls interface label-map 400 protect-swap 480

MPLS Interface (Label-Map 400)

                   Protected Protected  Protected
In Label  In I/F     Out Label Out I/F    Next Hop          Type  Adm  Opr
---------+----------+---------+----------+-----------------+---------+----+----
```

output definitions

Interface	The name of an existing MPLS IP interface.
Port-id	The existing port-id.
Adm	The administrative state of the LSP peer (**Up** or **Down**).

Opr	The operational state of the LSP peer (**Up** or **Down**).
In Label	An incoming label number.
Protected Out Label	An outgoing label number.
Protected Next Hop	Ip address of the next hop.
Type	Type of label to display.

Release History

Release 6.4.2; command was introduced.

Related Commands

configure router mpls interface	Configures MPLS support on an IP interface.

MIB Objects

show router mpls label

Displays the MPLS labels that are exchanged.

show router mpls label *start-label* **[***end-label* **[***label-filter***]]**

Syntax Definitions

start-label	The label value assigned to the ingress router**.**
end-label	The label value assigned to the egress router.
label-filter	The types of labels to display. The valid entries for this parameter are **in-use**, **bgp**, **ildp**, **mirror**, **rsvp**, **static**, **svcmgr**, **tldp**, or **vprn**. Enter one type per command.

Defaults

N/A

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

Use the command parameters provided to display information for specific types of labels.

Examples

```
-> show router mpls label 500

MPLS Label 500

Label              Label Type            Label Owner
---------------+------------------+------------------
500                static-lsp            STATIC

In-use labels in entire range                   : 8

-> show router mpls label 32 80 static

MPLS Labels from 32 to 80 (Owner: STATIC)

Label               Label Type             Label Owner
------------------+------------------+-----------------------

In-use labels (Owner: STATIC) in specified range: 0
In-use labels (Owner: All) in specified range   : 0
In-use labels in entire range                   : 9
```

```
-> show router mpls label 400 500

MPLS Labels from 400 to 500

Label               Label Type          Label Owner
--------------------+-------------------+------------------------
400                 static-lsp          STATIC
401                 static-lsp          Not-in-use
402                 static-lsp          Not-in-use
403                 static-lsp          Not-in-use
404                 static-lsp          Not-in-use
405                 static-lsp          Not-in-use
406                 static-lsp          Not-in-use
407                 static-lsp          Not-in-use
408                 static-lsp          Not-in-use
409                 static-lsp          Not-in-use
410                 static-lsp          Not-in-use
411                 static-lsp          Not-in-use
412                 static-lsp          Not-in-use
413                 static-lsp          Not-in-use
414                 static-lsp          Not-in-use
415                 static-lsp          Not-in-use
416                 static-lsp          Not-in-use
417                 static-lsp          Not-in-use
418                 static-lsp          Not-in-use
419                 static-lsp          Not-in-use
420                 static-lsp          Not-in-use
421                 static-lsp          Not-in-use
422                 static-lsp          Not-in-use
423                 static-lsp          Not-in-use
424                 static-lsp          Not-in-use
425                 static-lsp          Not-in-use
426                 static-lsp          Not-in-use
427                 static-lsp          Not-in-use
428                 static-lsp          Not-in-use
429                 static-lsp          Not-in-use
430                 static-lsp          Not-in-use
431                 static-lsp          Not-in-use
432                 static-lsp          Not-in-use
433                 static-lsp          Not-in-use
434                 static-lsp          Not-in-use
435                 static-lsp          Not-in-use
436                 static-lsp          Not-in-use
437                 static-lsp          Not-in-use
438                 static-lsp          Not-in-use
439                 static-lsp          Not-in-use
440                 static-lsp          Not-in-use
441                 static-lsp          Not-in-use
442                 static-lsp          Not-in-use
443                 static-lsp          Not-in-use
444                 static-lsp          Not-in-use
445                 static-lsp          Not-in-use
446                 static-lsp          Not-in-use
447                 static-lsp          Not-in-use
448                 static-lsp          Not-in-use
449                 static-lsp          Not-in-use
450                 static-lsp          Not-in-use
451                 static-lsp          Not-in-use
```

```
452                 static-lsp          Not-in-use
453                 static-lsp          Not-in-use
454                 static-lsp          Not-in-use
455                 static-lsp          Not-in-use
456                 static-lsp          Not-in-use
457                 static-lsp          Not-in-use
458                 static-lsp          Not-in-use
459                 static-lsp          Not-in-use
460                 static-lsp          Not-in-use
461                 static-lsp          Not-in-use
462                 static-lsp          Not-in-use
463                 static-lsp          Not-in-use
464                 static-lsp          Not-in-use
465                 static-lsp          Not-in-use
466                 static-lsp          Not-in-use
467                 static-lsp          Not-in-use
468                 static-lsp          Not-in-use
469                 static-lsp          Not-in-use
470                 static-lsp          Not-in-use
471                 static-lsp          Not-in-use
472                 static-lsp          Not-in-use
473                 static-lsp          Not-in-use
474                 static-lsp          Not-in-use
475                 static-lsp          Not-in-use
476                 static-lsp          Not-in-use
477                 static-lsp          Not-in-use
478                 static-lsp          Not-in-use
479                 static-lsp          Not-in-use
480                 static-lsp          Not-in-use
481                 static-lsp          Not-in-use
482                 static-lsp          Not-in-use
483                 static-lsp          Not-in-use
484                 static-lsp          Not-in-use
485                 static-lsp          Not-in-use
486                 static-lsp          Not-in-use
487                 static-lsp          Not-in-use
488                 static-lsp          Not-in-use
489                 static-lsp          Not-in-use
490                 static-lsp          Not-in-use
491                 static-lsp          Not-in-use
492                 static-lsp          Not-in-use
493                 static-lsp          Not-in-use
494                 static-lsp          Not-in-use
495                 static-lsp          Not-in-use
496                 static-lsp          Not-in-use
497                 static-lsp          Not-in-use
498                 static-lsp          Not-in-use
499                 static-lsp          Not-in-use
500                 static-lsp          Not-in-use

In-use labels (Owner: All) in specified range   : 1
In-use labels in entire range                   : 9
```

```
-> show router mpls label 400 500 static

MPLS Labels from 400 to 500 (Owner: STATIC)

Label               Label Type          Label Owner
--------------------+-------------------+------------------------
400                 static-lsp          STATIC

In-use labels (Owner: STATIC) in specified range: 1
In-use labels (Owner: All) in specified range   : 1
In-use labels in entire range                   : 9

-> show router mpls label 400 500 in-use

MPLS Labels from 400 to 500 (In-use)

Label               Label Type          Label Owner
--------------------+-------------------+------------------------
400                 static-lsp          STATIC

In-use labels (Owner: All) in specified range   : 1
In-use labels in entire range                   : 9
```

output definitions

Label	Label value assigned to the router.
Label Type	Type of Label to display.
Label Owner	Type of Label owner.

Release History

Release 6.4.2; command was introduced.

Related Commands

show router mpls label-range	Displays the MPLS label ranges, which includes the label type, start and end label values, aging, and the number of labels available.

MIB Objects

```
vRtrMplsStaticSvcLabelTable
vRtrMplsStaticSvcLabelTable
```

show router mpls label-range

Displays the MPLS label ranges, which includes the label type, start and end label values, aging, and the number of labels available.

show router mpls label-range

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

N/A.

Examples

```
-> show router mpls label-range

Label Ranges

Label Type     Start Label     End Label       Aging       Total Available
-------------+--------------+-------------+--------------+------------------
Static-lsp      32              1023            -             986
Static-svc      2048            18431           -             16383
Dynamic         32768           131071          0             98303
```

output definitions

Label Type	Type of Label to display.
Start Label	The label value assigned to the ingress router**.**
End Label	The label value assigned to the egress router**.**
Aging	Label aging to be displayed.
Total Available	Total Label ranges available

Release History

Release 6.4.2; command was introduced.

Related Commands

show router mpls label	Displays the MPLS labels that are exchanged.

MIB Objects

vRtrMplsLabelRangeTable

show router mpls static-lsp

Displays static Label Switched Path (LSP) information.

show router mpls static-lsp [*lsp-name* | **transit | terminate | count]**

Syntax Definitions

lsp-name	The name of an existing LSP.
transit	Displays transit information for static LSPs.
terminate	Displays endpoint information for static LSPs.
count	Displays the total number of static LSPs.

Defaults

By default, information for all static LSPs is displayed.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

Use the command parameters provided to display information for a specific static LSP or to provide a count of the number of static LSPs.

Examples

```
-> show router mpls static-lsp

MPLS Static LSPs (Originating)

LSP Name       To           Next Hop    Out Label    Up/Down Time   Adm   Opr
 ID                                       Out Port
------------+--------------+--------------+---------+--------------+----+----
lsp-1       10.1.1.4      20.20.20.1*     734       0d 05:56:45    Up    Up
 1                                        n/a
lsp-2       10.11.0.6     20.20.20.1*     750       0d 05:56:45    Up    Up
 2                                       n/a
lsp-3        5.5.5.5      20.20.20.1*     750       0d 05:56:45    Up    Up
 3                                       n/a

LSPs : 3
```

```
-> show router mpls static-lsp lsp-1

MPLS Static LSPs (Originating)

LSP Name      To          Next Hop     Out Label    Up/Down Time   Adm   Opr
 ID                                     Out Port
------------+--------------+--------------+---------+--------------+----+----
lsp-1       10.1.1.4      20.20.20.1*     734       0d 05:56:52     Up    Up
 1                                       n/a

LSPs: 1

-> show router mpls static-lsp transit

MPLS Static LSPs (Transit)

In Lable    In Port     Out Label    Next Hop     Adm   Opr
                        Out Port
------------+--------------+--------------+---------+--------
vlan-22     vlan-20      440         22.22.22.1    Up    Up
vlan-20     vlan-20      730         20.20.20.1    Up    Up
vlan-22     vlan-20      840         22.22.22.1    Up    Up
vlan-22     vlan-20      920         22.22.22.1    Up    Up
vlan-22     vlan-20      1020        22.22.22.1    Up    Up

LSPs : 5


-> show router mpls static-lsp terminate


In Lable    In Port     Out Label  Out Port    Next Hop     Adm   Opr

------------+--------------+--------------+---------+----------------
732         NA          NA         NA          NA           Up    Up
840         N/A         N/A        N/A         N/A          Down  Up

LSPs : 2



-> show router mpls static-lsp count

MPLS Static-LSP Count

Originate           Transit             Terminate
-------------------+-------------------+-------------
3                   5                   2
```

output definitions

LSP Name ID	The name of an existing LSP.
To	Ip address of the destination.
Out Label Out Port	Outgoing label number.
Up/Down Time	Time for Up or Down state.
Opr	The operational state of the LSP peer (**Up** or **Down**).

Release History

Release 6.4.2; command was introduced.

Related Commands

configure router mpls static-lsp	Configures a static LSP on an ingress Label Edge Router (LER).

MIB Objects

show router mpls status

Displays the MPLS status.

show router mpls status

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

This command administrative and operational information for the MPLS instance on the router.

Examples

```
-> show router mpls status

MPLS Status

  Admin Status:        Up,                 Oper Status:         Up,
  Oper Down Reason:    N/A

LSP Counts      Originate            Transit            Terminate
Static LSPs         0                   4                   0
Dynamic LSPs        0                   0                   0
Detour LSPs         0                   0                   0
```

output definitions

Admin Status	The administrative state of the LSP peer (**Up** or **Down**).
Oper Status	The operational state of the LSP peer (**Up** or **Down**).
Oper Down Reason	Reason for operational state - Down.
LSP Counts	Displays the total number of static LSPs.
Originate	Displays originate information for static LSPs.
Transit	Displays transit information for static LSPs.
Terminate	Displays endpoint information for static LSPs.

Release History

Release 6.4.2; command was introduced.

Related Commands

show router mpls static-lsp	Displays detailed static LSP information.

MIB Objects

56 Virtual Private LAN Service (VPLS) Commands

A Virtual Private LAN Service (VPLS) is a Virtual Private Network (VPN) technology that allows any-to-any (multipoint) connectivity. The provider network emulates a LAN by connecting all the remote customer sites at the edge of the provider network to a single bridged LAN. A full mesh of pseudo-wires (PW) needs to be established to form a VPLS.

A VPLS-capable network consists of Customer Edges (CE), Provider Edges (PE), and a core MPLS network. The CE device is a router or switch located at the customer's premises and is connected to the PE via an Attachment Circuit (AC). In the case of VPLS, it is assumed that Ethernet is the layer 2 protocol used between the CE and the PE.

The PE device is where the services originate and terminate and where all the necessary tunnels are set up to connect to all the other PEs. As VPLS is an Ethernet Layer 2 service, the PE must be capable of Media Access Control (MAC) learning, bridging, and replication on a per-VPLS basis.

The IP/MPLS core network interconnects the PEs but does not participate in the VPN functionality. Traffic is simply switched based on the MPLS labels.

This implementation of VPLS makes use of a service-based architecture that provides the following logical entities that are required to provision a service:

- **Customers (subscribers).** An account is created for each customer and assigned an ID. The customer ID is required and associated with the service at the time the service is created.
- **Service Access Points (SAPs).** Each subscriber service type is configured with at least one SAP. A SAP identifies the point at which customer traffic enters the service.
- **Service Distribution Points (SDPs)**. A SDP provides a logical point at which customer traffic is directed from one PE to another PE through a one-way service tunnel.

A distributed service consists of at least one SAP on a local node, one SAP on a remote node, and an SDP binding the service to the service tunnel.

This chapter provides information about the Command Line Interface (CLI) commands used to configure the above entities required to provision a service.

MIB information for the LDP commands is as follows:

Filename: AlcatelIND1ServiceMgr.MIB
Module: Alcatel-IND1-SERVICE-MGR-MIB

Filename: TIMETRA-SDP.MIB_mib
Module: TIMETRA-SDP-MIB

A summary of the available commands is listed here:

Customer Account Commands	**configure service customer create** **configure service customer contact** **configure service customer phone** **configure service customer description**
Service Distribution Point (SDP) Commands	**configure service sdp create** **configure service sdp description** **configure service sdp far-end** **configure service sdp shutdown** **configure service sdp ldp** **configure service sdp signaling** **configure service sdp lsp** **configure service sdp adv-mtu-override** **configure service sdp path-mtu**
VPLS Commands	**configure service vpls create** **configure service vpls description** **configure service vpls shutdown** **configure service vpls def-mesh-vc-id** **configure service vpls send-flush-on-failure** **configure service vpls service-mtu** **configure service vpls mesh-sdp** **configure service vpls mesh-sdp shutdown** **configure service vpls mesh-sdp egress vc-label** **configure service vpls mesh-sdp ingress vc-label** **configure service vpls mesh-sdp static-mac**
Service Access Point (SAP) Commands	**configure service l2profile** **configure service port mode access** **configure service port l2profile** **configure service port encap-type** **configure service vpls sap create** **configure service vpls sap description** **configure service vpls sap trusted** **configure service vpls sap shutdown** **configure service vpls sap static-mac**
Clear Commands	**clear service id fdb** **clear service id mesh-sdp ingress-vc-label**
Show Commands	**show service l2profile** **show service port** **show service customer** **show service sdp** **show service id all** **show service id base** **show service id labels** **show service id sap** **show service id sdp** **show service sap-using** **show service sdp-using** **show service egress-label** **show service ingress-label** **show service fdb-info** **show service fdb-mac**

configure service customer create

Creates a customer ID that is used to associate account information with a specific customer. The customer ID is associated with a Virtual Private LAN Service (VPLS) that is used to carry traffic between customer sites over a provider-managed MPLS network.

configure service customer *customer-id* **create**

configure service no customer *customer-id*

Syntax Definitions

customer-id	A unique numerical value to associate with a specific customer. The valid ID range is 2–2147483647.

Defaults

A default customer account ID (customer 1) exists on each router and is automatically assigned to new services.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Specify a customer ID that does not already exist in the router configuration.
- Use the **no** form of this command to remove a customer ID and all associated customer information. Note that deleting all service associations with a customer ID is required before the ID is removed from the router configuration.
- Editing or removing the default customer 1 account is not allowed.

Examples

```
-> configure service customer 10 create
-> configure service no customer 10
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure service customer contact	Configures contact information for a customer account.
configure service customer description	Configures a description for a customer account.
configure service customer phone	Configures phone number information for a customer account.
show service customer	Displays the customer account information configured for the router.

MIB Objects

```
custInfoTable
   custId
```

configure service customer contact

Configures contact information for the specified customer account. Use this command to provide information about the customer, such as a contact name or account contract name.

configure service customer *customer-id* **contact** *contact-info*

configure service customer *customer-id* **no contact**

Syntax Definitions

customer-id	An existing customer ID number.
contact-info	An ASCII text string up to 80 characters in length. Enclose special characters, such as #, $, or spaces, in double quotation marks (for example “Technical Support”).

Defaults

By default, no customer contact information is configured when a customer account ID is created.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to remove customer contact information from the specified customer account ID.
- Printable, 7-bit ASCII characters are allowed in the contact information string.

Examples

```
-> configure service customer 10 contact “Thomas Smith - Tech Support”
-> configure service no contact
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure service customer create	Creates a customer account and associates that account with a customer ID.
configure service customer description	Configures a description for a customer account.
configure service customer phone	Configures phone number information for a customer account.
show service customer	Displays the customer account information configured for the router.

MIB Objects

```
custInfoTable
   custId
   custContact
```

configure service customer phone

Configures telephone number information for the specified customer account.

configure service customer *customer-id* **phone** *phone-info*

configure service customer *customer-id* **no phone**

Syntax Definitions

customer-id	An existing customer ID number.
phone-info	An ASCII text string up to 80 characters in length. Enclose special characters, such as #, $, or spaces, in double quotation marks (for example “800-444-1234”).

Defaults

By default, telephone information is not added when a customer account is created.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to remove the telephone information from the specified customer account ID.
- Printable, 7-bit ASCII characters are allowed in the description text string.

Examples

```
-> configure service customer 10 phone “888-444-1234”
-> configure service customer 10 no phone
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure service customer create	Creates a customer account and associates that account with a customer ID.
configure service customer contact	Configures contact information for a customer account.
configure service customer description	Configures a description for a customer account.
show service customer	Displays the customer account information configured for the router.

MIB Objects

```
custInfoTable
   custId
   custPhone
```

configure service customer description

Configures an optional description for the specified customer account. Use this command to add more information about the customer or additional account details.

configure service customer *customer-id* **description** *desc-info*

configure service customer *customer-id* **no description**

Syntax Definitions

customer-id	An existing customer ID number.
desc-info	An ASCII text string up to 80 characters in length. Enclose special characters, such as #, $, or spaces, in double quotation marks (for example “Services Contract #4000”).

Defaults

By default, a description is not added when a customer account is created.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to remove the description from the specified customer account ID.
- Printable, 7-bit ASCII characters are also allowed in the description text string.

Examples

```
-> configure service customer 10 description “PT-Cal_Service_Manager”
-> configure service customer 10 no description
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure service customer create	Creates a customer account and associates that account with a customer ID.
configure service customer contact	Configures contact information for a customer account.
configure service customer phone	Configures phone number information for a customer account.
show service customer	Displays the customer account information configured for the router.

MIB Objects

```
custInfoTable
   custId
   custDescription
```

configure service sdp create

Configures a Service Distribution Point (SDP). An SDP is a logical entity that directs traffic to another router through MPLS-based service tunnels.

configure service sdp *sdp-id* **[mpls] create**

configure service no sdp *sdp-id*

Syntax Definitions

sdp-id	The identification number to associate with the specified SDP. The valid ID range is 1–17407.
mpls	The delivery mechanism for the SDP. No other mechanism is supported at this time.

Defaults

By default, MPLS is the delivery mechanism for the SDP and the SDP administrative state is disabled.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to remove the specified SDP. Disable the administrative status and remove any services associated with the SDP before attempting to remove the SDP.
- Administratively enabling the SDP is not allowed until a far-end router address is configured for the SDP. Specifying this address identifies the router on which the SDP will terminate. As a result, an SDP tunnel is configured that will provide a path from Point A to Point B.
- Configure an SDP on each participating provider edge (PE) router.
- Once created, an SDP is then bound to a specific customer Virtual Private LAN Service (VPLS). This binding process allows routers to participate in a service.
- Binding multiple services to one SDP is allowed; up to 32 SDP sessions are allowed at the same time.

Examples

```
-> configure service sdp 10 create
-> configure service sdp 20 mpls create
-> configure service no sdp 20
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure service sdp description	Configures a description for the specified SDP.
configure service sdp far-end	Configures the system IP address of the far-end destination router for the SDP.
configure service sdp shutdown	Configures the administrative status of the specified SDP.
configure service sdp ldp	Enables or disables an LDP-signaled Label Switch Path (LSP) for the specified SDP.
configure service sdp signaling	Enables or disables auto-label signaling for the specified SDP;
configure service sdp adv-mtu-override	Enables or disables VC-type MTU override for the specified SDP.
configure service sdp path-mtu	Configures the administrative MTU value for the SDP.
show service sdp-using	Displays the SDP usage for the local router or for a far-end router IP address.
show service id sdp	Displays the SDP configuration for the specified service.

MIB Objects

```
sdpInfoTable
   sdpId
   sdpDelivery
```

configure service sdp description

Configures a description for the specified SDP.

configure service sdp *sdp-id* **description** *desc-info*

configure service sdp *sdp-id* **no description**

Syntax Definitions

sdp-id	An existing SDP ID number.
desc-info	An ASCII text string up to 80 characters in length. Enclose special characters, such as #, $, or spaces, in double quotation marks (for example “PE1 to PE2”).

Defaults

By default, a description is not added when the SDP is created.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to remove the description from the specified SDP.
- Printable, 7-bit ASCII characters are also allowed in the description text string.

Examples

```
-> configure service sdp 10 description “SW-A to SW-B”
-> configure service sdp 10 no description
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure service sdp create	Configures an SDP, which is used to a direct traffic to another router through MPLS-based service tunnels.
configure service sdp far-end	Configures the system IP address of the far-end destination router for the SDP.
configure service sdp shutdown	Configures the administrative status of the specified SDP.
configure service sdp ldp	Enables or disables an LDP-signaled Label Switch Path (LSP) for the specified SDP.
configure service sdp signaling	Enables or disables auto-label signaling for the specified SDP;
configure service sdp adv-mtu-override	Enables or disables VC-type MTU override for the specified SDP.
configure service sdp path-mtu	Configures the administrative MTU value for the SDP.
show service sdp-using	Displays the SDP usage for the local router or for a far-end router IP address.
show service id sdp	Displays the SDP configuration for the specified service.

MIB Objects

```
sdpInfoTable
   sdpId
   sdpDescription
```

configure service sdp far-end

Configures the system IP address of the far-end destination router for the Service Distribution Point (SDP). This far-end address identifies the SDP endpoint, which is where the service associated with the SDP will terminate.

configure service sdp *sdp-id* **far-end** *ip-address*

configure service sdp *sdp-id* **no far-end**

Syntax Definitions

sdp-id	An existing SDP ID number.
ip-address	The system IP address for the far-end router. This is the user-configured Loopback0 address if the far-end router is an OmniSwitch.

Defaults

By default, a far-end address is not defined when the SDP is created.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to remove the far-end system IP address for the specified SDP. Administratively disable the SDP before attempting to remove the far-end address.
- Removing the far-end IP address from the SDP also removes all Label Switch Paths (LSPs) associated with the SDP.
- Administratively enabling an SDP is not allowed until a far-end router address is configured for the SDP. Specifying this address identifies the router on which the SDP will terminate. As a result, an SDP tunnel is configured that will provide a path from Point A to Point B.
- The SDP is operational when the SDP is administratively enabled and the protocol routing table contains the far-end IP address as a host route. OSPF ABRs should not summarize host routes between areas. This can cause SDPs to become operationally down. To avoid this potential problem, configure static host routes (direct and indirect) in the local router.
- If the SDP uses MPLS encapsulation (OmniSwitch supports MPLS only), the far-end IP address is used to check LSP names when added to the SDP. If the "**to** IP address" defined within the LSP configuration does not exactly match the SDP far-end IP address, the LSP is not added to the SDP and an error is generated.

Examples

```
-> configure service sdp 10 far-end 10.1.1.2
-> configure service sdp 10 no far-end
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure service sdp create	Configures an SDP, which is used to a direct traffic to another router through MPLS-based service tunnels.
configure service sdp description	Configures a description for the specified SDP.
configure service sdp shutdown	Configures the administrative status of the specified SDP.
configure service sdp ldp	Enables or disables an LDP-signaled Label Switch Path (LSP) for the specified SDP.
configure service sdp signaling	Enables or disables auto-label signaling for the specified SDP;
configure service sdp adv-mtu-override	Enables or disables VC-type MTU override for the specified SDP.
configure service sdp path-mtu	Configures the administrative MTU value for the SDP.
show service sdp-using	Displays the SDP usage for the local router or for a far-end router IP address.
show service id sdp	Displays the SDP configuration for the specified service.

MIB Objects

```
sdpInfoTable
   sdpId
   sdpFarEndIpAddress
```

configure service sdp shutdown

Configures the administrative status of the specified Service Distribution Point (SDP).

configure service sdp *sdp-id* **{no shutdown | shutdown}**

Syntax Definitions

sdp-id	An existing SDP ID number.
no shutdown	Administratively enables the SDP.
shutdown	Administratively disables the SDP.

Defaults

By default, the SDP administrative status is disabled.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Administratively enabling an SDP is not allowed until a system IP address for a far-end router is configured for the SDP.
- Disabling the SDP administrative status does not remove the SDP configuration from the router.
- The SDP is operational when the SDP is administratively enabled and the protocol routing table contains the far-end IP address as a host route. OSPF ABRs should not summarize host routes between areas. This can cause SDPs to become operationally down. To avoid this potential problem, configure static host routes (direct and indirect) in the local router.

Examples

```
-> configure service sdp 10 no shutdown
-> configure service sdp 20 shutdown
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure service sdp create	Configures an SDP, which is used to a direct traffic to another router through MPLS-based service tunnels.
configure service sdp description	Configures a description for the specified SDP.
configure service sdp far-end	Configures the system IP address of the far-end destination router for the SDP.
configure service sdp ldp	Enables or disables an LDP-signaled Label Switch Path (LSP) for the specified SDP.
configure service sdp signaling	Enables or disables auto-label signaling for the specified SDP;
configure service sdp adv-mtu-override	Enables or disables VC-type MTU override for the specified SDP.
configure service sdp path-mtu	Configures the administrative MTU value for the SDP.
show service sdp-using	Displays the SDP usage for the local router or for a far-end router IP address.
show service id sdp	Displays the SDP configuration for the specified service.

MIB Objects

```
sdpInfoTable
   sdpId
   sdpAdminStatus
```

configure service sdp ldp

Specifies LDP-signaled Label Switched Paths (LSPs) as the transport mechanism for the specified SDP tunnel.

configure service sdp *sdp-ip* **ldp**

configure service sdp *sdp-ip* **no ldp**

Syntax Definitions

sdp-id	An existing SDP ID number.

Defaults

By default, LDP-signaled LSPs are enabled for the SDP.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- There are two types of LSPs: LDP and static. Assigning static LSPs or enabling LDP is required when configuring a SDP. However, only one type of LSP per SDP is allowed.
- Changing the LSP type is only allowed when the SDP is administratively disabled.
- Use the **no** form of this command to specify the use of MPLS static LSPs instead of LDP-signaled LSPs. This will turn off LDP signaling for the SDP so that using static LSPs is allowed.
- Static LSPs are user-defined LSPs that require the manual configuration of MPLS label mappings and actions on each participating router within the static path. A static LSP is associated with a SDP using the **configure service sdp lsp** command.

Examples

```
-> configure service sdp 10 ldp
-> configure service sdp 10 no ldp
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure service sdp create	Configures an SDP, which is used to direct traffic to another router through MPLS-based service tunnels.
configure service sdp shutdown	Configures the administrative status of the specified SDP.
configure service sdp signaling	Enables or disables auto-label signaling for the specified SDP. Enable signaling if LDP-signaled LSPs are configured for the SDP.
configure service sdp adv-mtu-override	Enables or disables VC-type MTU override for the specified SDP.
configure service sdp path-mtu	Configures the administrative MTU value for the SDP.
show service sdp-using	Displays the SDP usage for the local router or for a far-end router IP address.
show service id sdp	Displays the SDP configuration for the specified service.

MIB Objects

```
sdpInfoTable
   sdpId
   sdpLdpEnabled
```

configure service sdp signaling

Enables or disables auto-label signaling for the specified SDP. Enable signaling if the specified SDP is using LDP-signaled LSPs for targeted LDP (TLDP) sessions. Disable signaling if the specified SDP is using static LSPs, which use manually configured label mappings and actions.

configure service sdp *sdp-ip* **signaling {off | tldp}**

Syntax Definitions

sdp-id	An existing SDP ID number.
off	Disables auto-label signaling for the specified SDP.
tldp	Enables auto-label signaling for the specified SDP.

Defaults

By default, auto-label signaling (TLDP) is enabled for the SDP.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- If signaling is disabled, then labels are manually configured when a service is bound to the SDP.
- Enabling or disabling auto-label signaling is only allowed when the SDP is administratively disabled.

Examples

```
-> configure service sdp 10 signaling off
-> configure service sdp 10 signaling tldp
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure service sdp create	Configures an SDP, which is used to a direct traffic to another router through MPLS-based service tunnels.
configure service sdp description	Configures a description for the specified SDP.
configure service sdp far-end	Configures the system IP address of the far-end destination router for the SDP.
configure service sdp shutdown	Configures the administrative status of the specified SDP.
configure service sdp ldp	Enables or disables an LDP-signaled Label Switch Path (LSP) for the specified SDP.
configure service sdp adv-mtu-override	Enables or disables VC-type MTU override for the specified SDP.
configure service sdp path-mtu	Configures the administrative MTU value for the SDP.
show service sdp-using	Displays the SDP usage for the local router or for a far-end router IP address.
show service id sdp	Displays the SDP configuration for the specified service.

MIB Objects

```
sdpInfoTable
   sdpId
   sdpLabelSignaling
```

configure service sdp lsp

Configures a static Label Switched Path (LSP) association with the specified Service Distribution Point (SDP). A static LSP is a user-configured path through Label Switching Routers (LSRs). Each participating LSR in the path requires manual configuration of MPLS actions and label mappings. However, assso-ciating a static LSP with an SDP is only done on the SDP router.

configure service sdp *sdp-ip* **lsp** *lsp-name*

configure service sdp *sdp-ip* **no lsp** *lsp-name*

Syntax Definitions

sdp-id	An existing SDP ID number.
lsp-name	The name of an existing static LSP to assign to the SDP ID.

Defaults

N/A.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to disable the static LSP association with the specified SDP.
- There are two types of LSPs: LDP and static. This command attaches a static LSP to a SDP. See Chapter 55, “MPLS Static LSP and FRR Commands,” for more information.
- LDP and static LSPs are mutually exclusive for the same SDP. If LDP is enabled for the SDP, disable LDP first before attempting to configure a static LSP for the SDP. The reverse is also true; disable any static LSPs associated with the SDP before attempting to enable LDP for the SDP.
- Configuring LSPs is only allowed when the SDP is administratively disabled.
- The specifed SDP must have LDP signaling enabled if the SDP is going to use LDP-signaled LSPs.
- The static LSPs associated with an SDP must terminate at the same far-end router IP address used by the SDP.

Examples

```
-> configure service sdp 10 lsp to-r4
-> configure service sdp 10 no lsp to-r4
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure service sdp create	Configures an SDP, which is used to a direct traffic to another router through MPLS-based service tunnels.
show service sdp-using	Displays the SDP usage for the local router or for a far-end router IP address.
show service id sdp	Displays the SDP configuration for the specified service.

MIB Objects

```
sdpInfoTable
   sdpId
   sdpLspList
```

configure service sdp adv-mtu-override

Enables or disables VC-type MTU override for the specified SDP. Use this command to override the advertised VC MTU with the service MTU.

configure service sdp *sdp-ip* **adv-mtu-override**

configure service sdp *sdp-ip* **no adv-mtu-override**

Syntax Definitions

sdp-id	An existing SDP ID number.

Defaults

By default, VC-type MTU override is disabled. The service MTU does not override the advertised VC MTU.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to disable VC-type MTU override for the specified SDP.
- When VC-type MTU override is enabled, the router signals a VC MTU equal to the service MTU (includes the Layer 2 header). When disabled, the service MTU minus the Layer 2 header is advertised. In the receive direction, either VC-type MTU is accepted.

Examples

```
-> configure service sdp 10 adv-mtu-override
-> configure service sdp 10 no adv-mtu-override
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure service sdp create	Configures an SDP, which is used to a direct traffic to another router through MPLS-based service tunnels.
configure service sdp description	Configures a description for the specified SDP.
configure service sdp far-end	Configures the system IP address of the far-end destination router for the SDP.
configure service sdp shutdown	Configures the administrative status of the specified SDP.
configure service sdp ldp	Enables or disables an LDP-signaled Label Switch Path (LSP) for the specified SDP.
configure service sdp signaling	Enables or disables auto-label signaling for the specified SDP;
configure service sdp path-mtu	Configures the administrative MTU value for the SDP.
show service sdp-using	Displays the SDP usage for the local router or for a far-end router IP address.
show service id sdp	Displays the SDP configuration for the specified service.

MIB Objects

```
sdpInfoTable
   sdpId
   sdpAdvertisedVllMtuOverride
```

configure service sdp path-mtu

Configures the administrative Maximum Transmission Unit (MTU) value for the SDP. This value specifies the largest service frame size that the SDP can transmit to the far-end router without dropping packets or requiring IP fragmentation.

configure service sdp *sdp-ip* **path-mtu** *bytes*

configure service sdp *sdp-ip* **no path-mtu**

Syntax Definitions

sdp-id	An existing SDP ID number.
bytes	The largest service frame size, in bytes, allowed through this SDP. The valid range is 576–9194.

Defaults

By default, the path MTU for the SDP is set to zero. This specifies that the MTU value is dynamically calculated from the corresponding tunnel.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to revert the path MTU to the default value of zero.
- If the physical MTU on an egress interface or channel indicates the next hop on an SDP path cannot support the current path MTU, the operational path MTU on that SDP is modified to a value that can be transmitted without fragmentation.
- If the service MTU is larger than the path MTU, the SDP binding for the service is placed in an inoperative state. If the service MTU is equal to or less than the path MTU, then the SDP binding is placed in an operational state.

Examples

```
-> configure service sdp 10 path-mtu 1514
-> configure service sdp 10 no path-mtu
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure service sdp create	Configures an SDP, which is used to a direct traffic to another router through MPLS-based service tunnels.
configure service sdp description	Configures a description for the specified SDP.
configure service sdp far-end	Configures the system IP address of the far-end destination router for the SDP.
configure service sdp shutdown	Configures the administrative status of the specified SDP.
configure service sdp ldp	Enables or disables an LDP-signaled Label Switch Path (LSP) for the specified SDP.
configure service sdp signaling	Enables or disables auto-label signaling for the specified SDP;
configure service sdp adv-mtu-override	Enables or disables VC-type MTU override for the specified SDP.
show service sdp-using	Displays the SDP usage for the local router or for a far-end router IP address.
show service id sdp	Displays the SDP configuration for the specified service.

MIB Objects

```
sdpInfoTable
   sdpId
   sdpAdvertisedVllMtuOverride
```

configure service vpls create

Configures a Virtual Private LAN Service (VPLS) and associates that service with a customer account. A VPLS connects multiple customer sites together across a provider-managed core network by creating a virtual zero-hop, Layer 2 switched domain.

configure service vpls *service-id* **customer** *customer-id* **create**

configure service no vpls *service-id*

Syntax Definitions

service-id	A unique numerical value to associate with a specific VPLS. The valid service ID range is 1–2147483647.
customer-id	An existing customer ID number to associate with the specified service ID number.

Defaults

N/A.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to remove the specified VPLS. Before attempting to remove the VPLS, shutdown the administrative status of the service and shutdown and delete any Service Access Points (SAPs) or Service Distribution Points (SDPs) associated with the service.
- Creating more than one VPLS for a single customer ID is allowed. However, once a customer ID is associated with a VPLS, changing the customer ID for that association is not allowed. If it is necessary to make such a change, delete the VPLS and create the service again with the new customer ID.
- Once a VPLS is created, it is then possible to bind the service to SAPs and SDPs.
- Up to 1024 VPLS services are supported.

Examples

```
-> configure service vpls 10 customer 10 create
-> configure service no vpls 10
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure service vpls description	Configures a description for the specified VPLS.
configure service vpls shutdown	Configures the administrative status of the specified VPLS.
configure service vpls def-mesh-vc-id	Configures a virtual circuit (VC) ID number used by each end of an MPLS tunnel to identify the VC.
configure service vpls send-flush-on-failure	Enables or disables the sending of a MAC flush message when a port or Service Access Point associated with the VPLS goes down
configure service vpls service-mtu	Configures the administrative MTU value for the specified VPLS
show service id all	Displays detailed configuration information about the specified service ID, including the SDP and SAP configuration that is associated with the service.

MIB Objects

```
svcBaseInfoTable
   svcId
   svcCustId
```

configure service vpls description

Configures a description for the specified Virtual Private LAN Service (VPLS).

configure service vpls *service-id* **[customer** *customer-id***] description** *desc-info*

configure service vpls *service-id* **[customer** *customer-id***] no description**

Syntax Definitions

service-id	An existing VPLS ID number.
customer-id	Optional**.** The customer ID number associated with the specified service ID number.
desc-info	An ASCII text string up to 80 characters in length. Enclose special characters, such as #, $, or spaces, in double quotation marks (for example “PE1 to PE2 Service1”).

Defaults

By default, a description is not added when the VPLS is created.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to remove the description from the specified VPLS.
- Specifying the customer ID associated with this VPLS is not required when using this command. However, if the customer ID specified is not the one associated with the VPLS, the command is not allowed.
- Printable, 7-bit ASCII characters are also allowed in the description text string.

Examples

```
-> configure service vpls 10 description “VPLS1-CustA”
-> configure service vpls 10 customer 10 description “VPLS1-CustA”
-> configure service vpls 10 no description
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure service vpls create	Configures a VPLS and associates the service with a customer account.
configure service vpls shutdown	Configures the administrative status of the specified VPLS.
configure service vpls def-mesh-vc-id	Configures a virtual circuit (VC) ID number used by each end of an MPLS tunnel to identify the VC.
configure service vpls send-flush-on-failure	Enables or disables the sending of a MAC flush message when a port or Service Access Point associated with the VPLS goes down
configure service vpls service-mtu	Configures the administrative MTU value for the specified VPLS
show service id all	Displays detailed configuration information about the specified service ID, including the SDP and SAP configuration that is associated with the service.

MIB Objects

```
svcBaseInfoTable
   svcId
   svcCustId
   svcDescription
```

configure service vpls shutdown

Configures the administrative status of the specified VPLS.

configure service vpls *service-id* **[customer** *customer-id***] {no shutdown | shutdown}**

Syntax Definitions

service-id	An existing VPLS ID number.
customer-id	Optional**.** The customer ID number associated with the specified service ID number.
no shutdown	Administratively enables the service.
shutdown	Administratively disables the service.

Defaults

By default, the administrative status for the service is disabled.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Disable the administrative status of the VPLS and any associated SAPs and SDPs before attempting to remove a VPLS.
- Disabling the VPLS administrative status does not remove the VPLS configuration from the router.
- Specifying the customer ID associated with this VPLS is not required when using this command. However, if the customer ID specified is not the one associated with the VPLS, the command is not allowed.

Examples

```
-> configure service vpls 10 no shutdown
-> configure service vpls 20 customer 20 no shutdown
-> configure service vpls 20 shutdown
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure service vpls create	Configures a VPLS and associates the service with a customer account.
configure service vpls description	Configures a description for the specified VPLS.
configure service vpls def-mesh-vc-id	Configures a virtual circuit (VC) ID number used by each end of an MPLS tunnel to identify the VC.
configure service vpls send-flush-on-failure	Enables or disables the sending of a MAC flush message when a port or Service Access Point associated with the VPLS goes down
configure service vpls service-mtu	Configures the administrative MTU value for the specified VPLS
show service id all	Displays detailed configuration information about the specified service ID, including the SDP and SAP configuration that is associated with the service.

MIB Objects

```
svcBaseInfoTable
   svcId
   svcCustId
   svcAdminStatus
```

configure service vpls def-mesh-vc-id

Configures a virtual circuit (VC) ID number used by each end of an MPLS tunnel to identify the VC. This value is used to identify the VC instead of getting this information from the label. Configuring the VC ID only applies to services bound to mesh SDPs.

configure service vpls *service-id* **[customer** *customer-id***] def-mesh-vc-id** *vc-id*

configure service no vpls *service-id* **[customer** *customer-id***] no def-mesh-vc-id**

Syntax Definitions

service-id	An existing VPLS ID number.
customer-id	Optional**.** The customer ID number associated with the specified service ID number.
vc-id	The VC ID number to assign. The valid range is 1–4294967295.

Defaults

By default, the VPLS ID number is used as the VC ID.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to remove the VC ID number.
- Specifying the customer ID associated with this VPLS is not required when using this command. However, if the customer ID specified is not the one associated with the VPLS, the command is not allowed.
- The VC ID number is significant between peer routers on the same hierarchical level.
- The value of a VC ID is conceptually independent from the value of the label or any other datalink specific information for the VC.

Examples

```
-> configure service vpls 10 def-mesh-vc-id 20
-> configure service vpls 10 customer 10 def-mesh-vc-id 20
-> configure service vpls 10 no def-mesh-vc-id 20
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure service vpls create	Configures a VPLS and associates the service with a customer account.
configure service vpls description	Configures a description for the specified VPLS.
configure service vpls shutdown	Configures the administrative status of the specified VPLS.
configure service vpls send-flush-on-failure	Enables or disables the sending of a MAC flush message when a port or Service Access Point associated with the VPLS goes down
configure service vpls service-mtu	Configures the administrative MTU value for the specified VPLS
show service id all	Displays detailed configuration information about the specified service ID, including the SDP and SAP configuration that is associated with the service.

MIB Objects

```
svcBaseInfoTable
   svcId
   svcCustId
   svcDefMeshVcId
```

configure service vpls send-flush-on-failure

Enables or disables the sending of a MAC flush message when a port or Service Access Point (SAP) associated with the VPLS goes down.

configure service vpls *service-id* **[customer** *customer-id***] send-flush-on-failure**

configure service no vpls *service-id* **[customer** *customer-id***] no send-flush-on-failure**

Syntax Definitions

service-id	An existing VPLS ID number.
customer-id	Optional**.** A customer ID number associated with the specified service ID number.

Defaults

By default, the sending of a MAC flush message on failure is disabled.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to disable sending of MAC flush messages.
- Specifying the customer ID associated with this VPLS is not required when using this command. However, if the customer ID specified is not the one associated with the VPLS, the command is not allowed.
- This functionality provides an LDP-based mechanism for recovering a physical link failure in a dual-homed connection to a VPLS service.

Examples

```
-> configure service vpls 10 send-flush-on-failure
-> configure service vpls 10 customer 10 send-flush-on-failure
-> configure service vpls 10 no send-flush-on-failure
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure service vpls create	Configures a VPLS and associates the service with a customer account.
configure service vpls description	Configures a description for the specified VPLS.
configure service vpls shutdown	Configures the administrative status of the specified VPLS.
configure service vpls def-mesh-vc-id	Configures a virtual circuit (VC) ID number used by each end of an MPLS tunnel to identify the VC.
configure service vpls service-mtu	Configures the administrative MTU value for the specified VPLS
show service id all	Displays detailed configuration information about the specified service ID, including the SDP and SAP configuration that is associated with the service.

MIB Objects

```
svcBaseInfoTable
   svcId
   svcCustId
svcTlsInfoTable
   svcTlsMacFlushOnFail
```

configure service vpls service-mtu

Configures the administrative Maximum Transmission Unit (MTU) value for the specified Virtual Private LAN Service (VPLS). This value specifies the largest frame size that the VPLS can transmit to the far-end router without dropping packets or requiring IP fragmentation.

configure service vpls *service-ip* **[customer** *customer-id***] service-mtu** *bytes*

configure service vpls *service-ip* **[customer** *customer-id***] no service-mtu**

Syntax Definitions

service-id	An existing VPLS ID number.
customer-id	Optional**.** A customer ID number associated with the specified service ID number.
bytes	The largest service frame size, in bytes, allowed through this service. The valid range is 1–9194.

Defaults

By default, the service MTU for VPLS is set to 1514.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to revert the service MTU to the default value.
- Specifying the customer ID associated with this VPLS is not required when using this command. However, if the customer ID specified is not the one associated with the VPLS, the command is not allowed.
- The service MTU and the service delineation encapsulation overhead (for example., 4 bytes for a 802.1Q tag) of the SAP is used to derive the required MTU of the physical port or channel on which the SAP was created. If the required payload is larger than the port or channel MTU, then the SAP is placed in an inoperative state. If the required MTU is equal to or less than the port or channel MTU, the SAP is able to transition to an operative state.
- When binding an SDP to a service, the service MTU is compared to the path MTU associated with the SDP. The path MTU is dynamically reduced due to the MTU capabilities discovered by the tunneling mechanism of the SDP or the egress interface MTU capabilities based on the next hop in the tunnel path.
- If the service MTU is larger than the path MTU, the SDP binding for the service is placed in an inoperative state. If the service MTU is equal to or less than the path MTU, then the SDP binding is placed in an operational state.

Examples

```
-> configure service vpls 10 service-mtu 3000
-> configure service vpls 10 customer 10 service-mtu 3000
-> configure service vpls 10 no service-mtu
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure service vpls create	Configures a VPLS and associates the service with a customer account.
configure service vpls description	Configures a description for the specified VPLS.
configure service vpls shutdown	Configures the administrative status of the specified VPLS.
configure service vpls def-mesh-vc-id	Configures a virtual circuit (VC) ID number used by each end of an MPLS tunnel to identify the VC.
configure service vpls send-flush-on-failure	Enables or disables the sending of a MAC flush message when a port or Service Access Point associated with the VPLS goes down
show service id all	Displays detailed configuration information about the specified service ID, including the SDP and SAP configuration that is associated with the service.

MIB Objects

```
svcBaseInfoTable
   svcId
   svcMtu
```

configure service vpls mesh-sdp

Configures a mesh binding between a Virtual Private LAN Service (VPLS) and a Service Distribution Point (SDP). Mesh SDPs bound to a service are logically treated as a single bridge port for flooded traffic, where flooded traffic received on any mesh SDP for the service is replicated to other ports and not transmitted on any mesh SDPs.

configure service vpls *service-id* **mesh-sdp** *sdp-id***[**:*vc-id***] [vc-type {ether | vlan} create**

configure service vpls *service-id* **no mesh-sdp** *sdp-id*

Syntax Definitions

service-id	An existing VPLS ID number.
sdp-id	An existing SDP ID number to bind to the specified service ID number.
vc-id	A VC ID number used to validate the VC ID portion of each mesh SDP binding defined for the service.
ether	Specifies Ethernet as the VC type for the mesh-SDP binding.
vlan	Specifies Ethernet VLAN as the VC type for the mesh-SDP binding.

Defaults

parameter	default
vc-id	*service-id* number
ether | **vlan**	**ether**

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to remove the SDP binding for the specified VPLS. Note that the SDP configuration is not removed, just the SDP binding with the service. Once the binding is removed, no packets are forwarded to the far-end router.
- Binding a service (VPLS instance) to an SDP is required to set up a Virtual Circuit (VC)/Pseudo Wire (PW) to the far end of the MPLS tunnel. If an SDP is not explicitly bound to a service, no far-end routers can participate in the service.
- When configuring services between OmniSwitch and SR Series routers, set the VC type to Ethernet if the null encapsulation type is used or to VLAN if the dot1q encapsulation type is used.
- The administrative and operational state of the SDP determines the state of that SDP for the service to which it is bound.

Examples

```
-> configure service vpls 10 mesh-sdp 100 create
-> configure service vpls 20 mesh-sdp 200 vc-type vlan create
-> configure service no mesh-sdp 100
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure service vpls mesh-sdp shutdown	Enables or disables the administrative status of the specified SDP mesh binding.
configure service vpls mesh-sdp egress vc-label	Configures the static MPLS VC label used by this router to send packets to the far-end router using the specified SDP mesh binding.
configure service vpls mesh-sdp ingress vc-label	Configures the static MPLS VC label used by the far-end router to send packets to this router using the specified mesh SDP binding.
configure service vpls mesh-sdp static-mac	Configures a static MAC address entry in the VPLS forwarding database that is associated with the specified mesh SDP binding.
show service sdp-using	Displays the SDP usage for the local router or for a far-end router IP address.
show service id sdp	Displays configuration information for the SDPs associated with the specified service.

MIB Objects

```
sdpBindTable
   sdpBindId
   sdpBindType
svcBaseInfoTable
   svcId
   svcDefMeshVcId
```

configure service vpls mesh-sdp shutdown

Enables or disables the administrative status of the specified mesh-SDP binding.

configure service vpls *service-id* **mesh-sdp** *sdp-id***[***:vc-id***] {no shutdown | shutdown}**

Syntax Definitions

service-id	An existing VPLS ID number.
sdp-id	An existing SDP ID number to bind to the specified service ID number.
vc-id	A VC ID number used to validate the VC ID portion of each mesh SDP binding defined for the service.
no shutdown	Enables the VPLS–SDP binding.
shutdown	Disables the VPLS–SDP binding.

Defaults

By default, the administrative status of the mesh–SDP binding is disabled.

parameter	default
vc-id	*service-id* value

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

Administratively disabling a VPLS–SDP binding does not remove the binding configuration from the router.

Examples

```
-> configure service vpls 10 mesh-sdp 100 no shutdown
-> configure service no mesh-sdp 100 shutdown
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure service vpls mesh-sdp	Configures a binding between a VPLS and a SDP.
configure service vpls mesh-sdp egress vc-label	Configures the static MPLS VC label used by this router to send packets to the far-end router using the specified SDP mesh binding.
configure service vpls mesh-sdp ingress vc-label	Configures the static MPLS VC label used by the far-end router to send packets to this router using the specified mesh SDP binding.
configure service vpls mesh-sdp static-mac	Configures a static MAC address entry in the VPLS forwarding database that is associated with the specified mesh SDP binding.
show service sdp-using	Displays the SDP usage for the local router or for a far-end router IP address.
show service id sdp	Displays configuration information for the SDPs associated with the specified service.

MIB Objects

```
sdpBindTable
   sdpBindId
   sdpBindType
   sdpBindAdminStatus
svcBaseInfoTable
   svcId
   svcDefMeshVcId
```

configure service vpls mesh-sdp egress vc-label

Configures the static MPLS VC label used by this router to send packets to the far-end router using the specified mesh SDP binding.

configure service vpls *service-id* **mesh-sdp** *sdp-id***[***:vc-id***] egress vc-label** *egress-vc-label*

configure service vpls *service-id* **no mesh-sdp** *sdp-id* **no egress vc-label**

Syntax Definitions

service-id	An existing VPLS ID number.
sdp-id	An existing SDP ID number that is bound to the specified service ID number.
vc-id	A VC ID number used to validate the VC ID portion of each mesh SDP binding defined for the service.
egress-vc-label	The egress VC value that identifies a specific connection. The valid range is 16–1048575.

Defaults

By default, the egress VC label value is set to zero (0).

parameter	default
vc-id	*service-id* value

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

Use the **no** form of this command to remove the egress VC label from the specified VPLS.

Examples

```
-> configure service vpls 100 mesh-sdp 20 egress vc-label 131070
-> configure service vpls 100 mesh-sdp 20 egress no vc-label
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure service vpls mesh-sdp	Configures a binding between a VPLS and a SDP.
configure service vpls mesh-sdp shutdown	Enables or disables the administrative status of the specified SDP mesh binding.
configure service vpls mesh-sdp ingress vc-label	Configures the static MPLS VC label used by the far-end router to send packets to this router using the specified mesh SDP binding.
configure service vpls mesh-sdp static-mac	Configures a static MAC address entry in the VPLS forwarding database that is associated with the specified mesh SDP binding.
show service sdp-using	Displays the SDP usage for the local router or for a far-end router IP address.
show service id sdp	Displays configuration information for the SDPs associated with the specified service.

MIB Objects

```
sdpBindTable
   sdpBindId
   sdpBindType
   sdpBindAdminEgressLabel
svcBaseInfoTable
   svcId
   svcDefMeshVcId
```

configure service vpls mesh-sdp ingress vc-label

Configures the static MPLS VC label used by the far-end router to send packets to this router using the specified mesh SDP binding.

configure service vpls *service-id* **mesh-sdp** *sdp-id***[***:vc-id***] ingress vc-label** *ingress-vc-label*

configure service vpls *service-id* **no mesh-sdp** *sdp-id* **no ingress vc-label**

Syntax Definitions

service-id	An existing VPLS ID number.
sdp-id	An existing SDP ID number that is bound to the specified service ID number.
vc-id	A VC ID number used to validate the VC ID portion of each mesh SDP binding defined for the service.
vc-label	The ingress VC value that identifies a specific connection. The valid range is 2048–18431.

Defaults

By default, the ingress VC label value is set to zero (0).

parameter	default
vc-id	*service-id* value

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

Use the **no** form of this command to remove the ingress VC label from the specified VPLS.

Examples

```
-> configure service vpls 100 mesh-sdp 20 ingress vc-label 131069
-> configure service vpls 100 mesh-sdp 20 ingress no vc-label
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure service vpls mesh-sdp	Configures a binding between a VPLS and a SDP.
configure service vpls mesh-sdp shutdown	Enables or disables the administrative status of the specified SDP mesh binding.
configure service vpls mesh-sdp egress vc-label	Configures the static MPLS VC label used by this router to send packets to the far-end router using the specified SDP mesh binding.
configure service vpls mesh-sdp static-mac	Configures a static MAC address entry in the VPLS forwarding database that is associated with the specified mesh SDP binding.
show service sdp-using	Displays the SDP usage for the local router or for a far-end router IP address.
show service id sdp	Displays configuration information for the SDPs associated with the specified service.

MIB Objects

```
sdpBindTable
   sdpBindId
   sdpBindType
   sdpBindAdminIngressLabel
svcBaseInfoTable
   svcId
   svcDefMeshVcId
```

configure service vpls mesh-sdp static-mac

Configures a static MAC address entry in the Virtual Private LAN Service (VPLS) forwarding database (FDB) that is associated with the specified mesh-Service Distribution Point (SDP) binding. Static MACs associated with SDPs are classified as remote MACs. A remote MAC is used by the associated VPLS so that MAC addresses are not learned on the edge device.

configure service vpls *service-id* **mesh-sdp** *sdp-id***[**:*vc-id***] static-mac** *mac-address*

configure service vpls *service-id* **mesh-sdp** *sdp-id* **no static-mac** *mac-address*

Syntax Definitions

service-id	An existing VPLS ID number.
sdp-id	An existing SDP ID number that is bound to the specified service ID number.
vc-id	A VC ID number used to validate the VC ID portion of each mesh SDP binding defined for the service.
mac-address	A 48-bit MAC address (*aa:bb:cc:dd:ee:ff*). Valid addresses are any non-broadcast, non-multicast MAC, and non-IEEE reserved addresses.

Defaults

parameter	default
vc-id	*service-id* value

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to remove the remote static MAC address entry from the VPLS forwarding database.
- Static MAC addresses configured on one edge device are not propagated to other edge devices associated with the same VPLS instance. Each edge device has an independent forwarding database for the associated VPLS.
- A MAC address can participate in only one static MAC address entry (local or remote) for a specific VPLS.

Examples

```
-> configure service vpls 100 mesh-sdp 20 static-mac 00:00:da:3e:44:01
-> configure service vpls 100 mesh-sdp 20 no static-mac 00:00:da:3e:44:01
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure service vpls mesh-sdp	Configures a binding between a VPLS and a SDP.
configure service vpls mesh-sdp shutdown	Enables or disables the administrative status of the specified SDP mesh binding.
configure service vpls mesh-sdp egress vc-label	Configures the static MPLS VC label used by this router to send packets to the far-end router using the specified SDP mesh binding.
configure service vpls mesh-sdp ingress vc-label	Configures the static MPLS VC label used by the far-end router to send packets to this router using the specified mesh SDP binding.
show service sdp-using	Displays the SDP usage for the local router or for a far-end router IP address.
show service id sdp	Displays configuration information for the SDPs associated with the specified service.

MIB Objects

```
tlsFdbInfoTable
   tlsFdbMacAddr
   tlsFdbType
   tlsFdbLocale
   tlsFdbSdpId
   tlsFdbVcId
svcBaseInfoTable
   svcId
   svcDefMeshVcId
```

configure service l2profile

Configures a Layer 2 profile that is applied to an access (customer facing) port. This profile is used to specify how to process Layer 2 control frames ingressing on the access port.

configure service l2profile *profile-name* **[create] {stp | 802.1x | 802.1ab | 802.3ad | gvrp | mvrp | amap} {peer | discard | tunnel}**

configure service no l2profile *profile-name*

Syntax Definitions

profile-name	Alphanumeric string of up to 32 characters. Use quotes around string if the profile name contains multiple words with spaces between them (e.g., “Alcatel-Lucent Engineering”).
create	Creates the Layer 2 profile if the *profile-name* specified does not exist in the switch configuration.
stp	Specifies how to process Spanning Tree BPDU.
802.1x	Specifies how to process 802.1x control frames.
802.1ab	Specifies how to process 802.1ab control frames.
802.3ad	Specifies how to process 802.3ad control frames.
gvrp	Specifies how to process GARP VLAN Registration Protocol packets.
mvrp	Specifies how to process Multiple VLAN Registration Protocol packets.
amap	Specifies how to process Alcatel-Lucent Management Adjacency Protocol packets.
peer	Allows the UNI port to participate in the specified protocol.
discard	Discards the specified PDU.
tunnel	Tunnels the specified PDU across the provider network.

Defaults

A default Layer 2 profile (**def-access-profile**) exists with the following default values:

parameter	default
stp	**tunnel**
802.1x	**discard**
802.1ab	**discard**
802.3ad	**peer**
gvrp	**tunnel**
mvrp	**tunnel**
amap	**discard**

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to delete a Layer 2 profile. Removing the **def-access-profile** is not allowed.
- Remove any profile associations with access ports before attempting to modify or delete the profile.
- Not all of the protocol parameters are currently supported with the **peer**, **tunnel**, and **discard** parameters. Use the following table to determine the parameter combinations that are supported:

	peer	discard	tunnel
stp	no	yes	yes
802.1x	no	yes	yes
802.1ab	no	yes	yes
802.3ad	yes	no	no
gvrp	no	yes	yes
mvrp	no	yes	yes
amap	no	yes	no

- If a user-configured Layer 2 profile is *not* associated with an access port, then the **def-access-profile** is used to process control packets ingressing on the port.

Examples

```
-> configure service l2profile “sap_1_profile” create stp discard
-> configure service l2profile “sap_1_profile” gvrp discard
-> configure service no l2profile “sap_1_profile”
```

Release History

Release 6.4.2; command was introduced.
Release 6.4.3; **mvrp** parameter added.

Related Commands

configure service port mode access	Configures a switch port or link aggregate as an access port.
configure service port l2profile	Assigns a Layer 2 profile to the specified service access port.
show service l2profile	Displays the Layer 2 profile configuration information for the router..

MIB Objects

```
alaServiceMgrPortProfileTable
   alaServiceMgrPortProfileID
   alaServiceMgrPortProfileStpBpduTreatment
   alaServiceMgrPortProfileGvrpTreatment
   alaServiceMgrPortProfileGvrpTreatment
   alaServiceMgrPortProfile8021xTreatment
   alaServiceMgrPortProfile8021ABTreatment
   alaEServiceUNIProfileGvrpTreatment
   alaServiceMgrPortProfileAmapTreatment
   alaServiceMgrPortProfile8023ADTreatment
```

configure service port mode access

Configures a switch port or link aggregate as an access port for customer traffic.

configure service port {*slot/port* | **linkagg** *agg_num***} mode access**

configure service port {*slot/port* | **linkagg** *agg_num***} no mode**

Syntax Definitions

slot/port1	The slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
agg_num	The link aggregate ID number (0–31).

Defaults

By default, switch ports and link aggregates are classified as network ports.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to revert the port mode back to the default mode (network).
- Access ports are required to configure a Service Access Point (SAP). A SAP is the point at which customer traffic enters and exits the provider service. SAPs are not configured on network ports

Examples

```
-> configure service port 1/3 mode access
-> configure service port linkagg 10 mode access
-> configure service port 1/3 no mode
-> configure service port linkagg 10 no mode
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure service port encap-type	Configures an encapsulation type for the specified service access port. The encapsulation type determines if an access port will support one or more services.
configure service l2profile	Configures a Layer 2 profile that is used to specify how to process Layer 2 control frames ingressing on the access port.
configure service port l2profile	Assigns a Layer 2 profile to the specified service access port.
show service port	Displays the access (customer-facing) port configuration for the router.

MIB Objects

```
alaServiceMgrAccessPortTable
   alaServiceMgrPortID
   alaServiceMgrPortMode
```

configure service port l2profile

Assigns an existing Layer 2 profile to the specified service access port. This profile determines how Layer 2 protocol frames ingressing on the access port are processed.

configure service port {*slot/port* | **linkagg** *agg_num***} l2profile {default |** *profile-name***}**

Syntax Definitions

slot/port1	The slot and port number of the service access port.
agg_num	The link aggregate ID number (0–31) of a service access link aggregate.
default	Assigns the default profile to the specified port.
profile-name	The name of an existing Layer 2 profile.

Defaults

By default, the default Layer 2 profile (**def-access-profile**) is assigned when a port is configured as a service access port.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to revert the associated profile back to the default profile.
- Specify only ports or link aggregates that are configured as service access ports. This command does not apply to network ports.
- Specify a profile name that already exists in the router configuration.

Examples

```
-> configure service port 1/3 l2profile sap_1_profile
-> configure service port linkagg 10 l2profile sap_1_profile
-> configure service port 1/3 l2profile default
-> configure service port linkagg 10 l2profile default
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure service port mode access	Configures a switch port or link aggregate as an access port.
configure service l2profile	Configures a Layer 2 profile that is used to specify how to process Layer 2 control frames ingressing on the access port.
configure service port encap-type	Configures an encapsulation type for the specified service access port. The encapsulation type determines if an access port will support one or more services.
show service port	Displays the access (customer-facing) port configuration for the router.

MIB Objects

```
alaServiceMgrAccessPortTable
   alaServiceMgrPortID
   alaServiceMgrPortMode
   alaServiceMgrPortProfileID
```

configure service port encap-type

Configures an encapsulation type for the specified service access port. The encapsulation type determines if the access port will support single or multiple Service Access Points (SAPs) for customer services.

configure service port {*slot/port* | **linkagg** *agg_num***} encap-type {null | dot1q}**

Syntax Definitions

slot/port1	The slot and port number of the service access port.
agg_num	The link aggregate ID number (0–31) of a service access link aggregate.
null	Allows only one SAP (one customer service) on the port. All customer traffic (tagged and untagged) is allowed.
dot1q	Allows multiple SAP associations (customer services) for the port. Only 802.1Q-tagged traffic on the port.

Defaults

By default, the **null** encapsulation type is selected when the port is configured as a service access port.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Specify only ports or link aggregates that are configured as service access ports. This command does not apply to network ports.
- The encapsulation type configured for the access port determines the encapsulation type for any SAPs associated with the port.

Examples

```
-> configure service port 1/3 encap-type null
-> configure service port linkagg 10 encap-type null
-> configure service port 1/17 encap-type dot1q
-> configure service port linkagg 20 encap-type dot1q
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure service port mode access	Configures a switch port or link aggregate as an access port.
configure service l2profile	Configures a Layer 2 profile that is used to specify how to process Layer 2 control frames ingressing on the access port.
configure service port l2profile	Assigns a Layer 2 profile to the specified service access port.
show service port	Displays the access (customer-facing) port configuration for the router.

MIB Objects

```
alaServiceMgrAccessPortTable
   alaServiceMgrPortId
   alaServiceMgrPortMode
   alaServiceMgrPortEncapType
```

configure service vpls sap create

Configures a Service Access Point (SAP) by associating a SAP ID with a Virtual Private LAN Service (VPLS). A SAP ID is comprised of a customer-facing port (referred to as an access port) and an encapsulation value that is used to identify the type of customer traffic to map to the associated service.

configure service vpls *service-id* **sap {***slot/port* **| linkagg** *agg_num***} [:0 | :all | :***qtag1***] create**

configure service vpls *service-id* **no sap {***slot/port* **| linkagg** *agg_num***} [:0 | :all | :***qtag1***]**

Syntax Definitions

service-id	An existing VPLS ID number.
slot/port1	The slot and port number of the service access port.
agg_num	The link aggregate ID number (0–31) of a service access link aggregate.
:0	Specifies a null encapsulation value for the SAP. Depending on the preconfigured encapsulation type for the access port, a SAP using a null encapsulation will direct tagged and untagged or only untagged traffic to the associated service.
:all	Specifies a wildcard SAP. All tagged or untagged traffic that is not classified into another SAP is mapped to the wildcard SAP. Not configurable on **null** encapsulation access ports.
:qtag1	Specifies a VLAN ID tag for traffic ingressing on the access port. Only traffic with this tag is mapped to this SAP. Not configurable on **null** encapsulation access ports.

Defaults

parameter	default
:0 | :all | :*qtag1*	**:0** (null)

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- To specify a SAP ID, use the *slot/port* and **linkagg** *agg-num* parameters combined with the **:0**, **:***qtag*, or **:all** parameters. For example, enter **1/2:all** to specify the SAP on access port 1/2 that maps all traffic to this service that is not already mapped to other SAPs.
- Use the **no** form of this command to remove a a SAP.
- Specify only ports or link aggregates that are configured as service access ports (see **configure service port mode access**). This command does not apply to network ports.
- The encapsulation mode for the access port determines how many SAPs are allowed on the access port. If the port is set to **null** encapsulation, only one default SAP is allowed on the port. If the port is set to

dot1q encapsulation, multiple SAPs (services) are allowed on the one port (see **configure service port encap-type**).

- If the SAP is configured to use the **null** encapsulation type, the access port encapsulation mode determines if both tagged and untagged traffic or only untagged traffic is allowed on the SAP. For example, if the access port is set to **null** encapsulation, both tagged and untagged traffic is mapped to the SAP. If the access port is set to **dot1q** encapsulation, then only tagged traffic is mapped to the SAP.

Examples

```
-> configure service vpls 10 sap 1/2
-> configure service vpls 11 sap 1/2:all
-> configure service vpls 12 sap 1/2:10
-> configure service vpls 13 linkagg 20
-> configure service vpls 14 linkagg 20:all
-> configure service vpla 15 linkagg 20:100
-> configure service vpls 10 no sap 1/2
-> configure service vpls 13 no linkagg 20
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure service vpls sap description	Configures a description for the specified SAP ID.
configure service vpls sap trusted	Configures the trust mode for the specified SAP ID.
configure service vpls sap shutdown	Configures the administrative status for the specified SAP ID.
configure service vpls sap static-mac	Configures a static MAC address entry in the forwarding database for the service that is associated with the specified SAP ID.
show service id sap	Displays configuration information about the SAPs associated with the specified service.
show service sap-using	Displays the SAP configuration for the local router.

MIB Objects

```
sapBaseInfoTable
   sapPortId
   sapEncapValue
svcBaseInfoTable
   svcId
```

configure service vpls sap description

Configures a description for the specified Service Access Point (SAP) ID. A SAP ID is comprised of a customer-facing port (referred to as an access port) and an encapsulation value that is used to identify the type of customer traffic to map to the associated service.

configure service vpls *service-id* **sap {***slot/port* **| linkagg** *agg_num***} [:0 | :all | :***qtag1***] description** *desc-info*

configure service vpls *service-id* **no sap {***slot/port* | **linkagg** *agg_num***} [:0 | :all | :***qtag1***] no description**

Syntax Definitions

service-id	An existing VPLS ID number.
slot/port1	The slot and port number of the service access port.
agg_num	The link aggregate ID number (0–31) of a service access link aggregate.
:0	Specifies a null encapsulation value for the SAP. Depending on the pre-configured encapsulation type for the access port, a SAP using a null encapsulation will direct tagged and untagged or only untagged traffic to the associated service.
:all	Specifies a wildcard SAP. All tagged or untagged traffic that is not classified into another SAP is mapped to the wildcard SAP. Not configurable on null encapsulation access ports.
:qtag1	Specifies a VLAN ID tag for traffic ingressing on the access port. Only traffic with this tag is mapped to this SAP. Not configurable on null encapsulation access ports.
desc-info	An ASCII text string up to 80 characters in length. Enclose special characters, such as #, $, or spaces, in double quotation marks (for example “CE1 to VPLS1 SAP”).

Defaults

By default, a description is not added when the SAP is created.

parameter	default
:0 | :all | :*qtag1*	**:0** (null)

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- To specify a SAP ID, use the *slot/port* and **linkagg** *agg-num* parameters combined with the **:0**, **:***qtag*, or **:all** parameters. For example, enter **1/2:all** to specify the SAP on access port 1/2 that maps all traffic to this service that is not already mapped to other SAPs.
- Use the **no** form of this command to remove the description from the specified SAP.

- Specify an existing VPLS service ID number and the associated access port for this SAP.
- Printable, 7-bit ASCII characters are also allowed in the description text string.

Examples

```
-> configure service vpls 10 sap 1/2:10 description “CE1 to VPLS1 SAP”
-> configure service vpls 13 linkagg 20 description “CE2 to VPLS2 SAP”
-> configure service vpls 10 sap 1/2:10 no description
-> configure service vpls 13 linkagg 20 no description
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure service vpls sap create	Configures a SAP by associating a SAP ID with a Virtual Private LAN Service (VPLS).
configure service vpls sap trusted	Configures the trust mode for the specified SAP ID.
configure service vpls sap shutdown	Configures the administrative status for the specified SAP ID.
configure service vpls sap static-mac	Configures a static MAC address entry in the forwarding database for the service that is associated with the specified SAP ID.
show service id sap	Displays configuration information about the Service Access Points (SAPs) associated with the specified service.
show service sap-using	Displays the SAP configuration for the local router.

MIB Objects

```
sapBaseInfoTable
   sapPortId
   sapEncapValue
   sapDescription
svcBaseInfoTable
   svcId
```

configure service vpls sap trusted

Configures the trust mode for the specified Service Access Port (SAP) ID. A SAP ID is comprised of a customer-facing port (referred to as an access port) and an encapsulation value that is used to identify the type of customer traffic to map to the associated service.

A trusted SAP can accept 802.1p values in incoming packets; an untrusted SAP will set any 802.1p values to zero in incoming packets, unless an 802.1p value is configured with this command.

configure service vpls *service-id* **sap {***slot/port* **| linkagg** *agg_num***} [:0 | :all | :***qtag1***] trusted**

configure service vpls *service-id* **sap {***slot/port* **| linkagg** *agg_num***} [:0 | :all | :***qtag1***] no trusted priority** *value*

Syntax Definitions

service-id	An existing VPLS ID number.
slot/port1	The slot and port number of the service access port.
agg_num	The link aggregate ID number (0–31) of a service access link aggregate.
:0	Specifies a null encapsulation value for the SAP. Depending on the pre-configured encapsulation type for the access port, a SAP using a null encapsulation will direct tagged and untagged or only untagged traffic to the associated service.
:all	Specifies a wildcard SAP. All tagged or untagged traffic that is not classified into another SAP is mapped to the wildcard SAP. Not configurable on null encapsulation access ports.
:qtag1	Specifies a VLAN ID tag for traffic ingressing on the access port. Only traffic with this tag is mapped to this SAP. Not configurable on null encapsulation access ports.
trusted	Allows the SAP to use the priority value obtained from tagged packets ingressing on the SAP port. Untagged packets use the default port priority value.
value	The priority value to set. Values range from 0 (lowest priority) to 7 (highest priority). This is the priority assigned to tagged and untagged packets ingressing on an untrusted SAP.

Defaults

By default, the SAP is trusted with the priority set to best effort (zero). These default values are set when a port is configured as an access port and then associated with the SAP.

parameter	default
:0 | :all | :*qtag1*	**:0** (null)

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- To specify a SAP ID, use the *slot/port* and **linkagg** *agg-num* parameters combined with the **:0**, **:***qtag*, or **:all** parameters. For example, enter **1/2:all** to specify the SAP on access port 1/2 that maps all traffic to this service that is not already mapped to other SAPs.
- Use the **no trusted** form of this command with the **priority** *value* parameter to configure a priority value to assign to packets ingressing on the SAP.
- Administratively disabling the SAP is not required to change the trust mode for the SAP.
- When the trust mode is changed from untrusted to trusted, the priority value is automatically set to the default best effort priority value (zero).
- Note that untagged Layer 2 control packets (for example, BPDU, GVRP, and AMAP) are always tunneled (if enabled) through the MPLS cloud with the default EXP bits set to 7, so that they can arrive at the destination router at the highest COS queue of 7. As a result, trusted and untrusted SAPs configured on the access ports will not affect the Layer 2 control packets ingressing on the access ports.
- Configuring the trust mode on an access port is not allowed. These settings are configured for the SAP to which the access port is associated.

Examples

```
-> configure service vpls 10 sap 1/2:10 trusted
-> configure service vpls 13 linkagg 20 trusted
-> configure service vpls 10 sap 1/2:10 no trusted priority 7
-> configure service vpls 13 linkagg 20 no trusted priority 3
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure service vpls sap create	Configures a SAP by associating a SAP ID with a Virtual Private LAN Service (VPLS).
configure service vpls sap description	Configures a description for the specified SAP ID.
configure service vpls sap shutdown	Configures the administrative status for the specified SAP ID.
configure service vpls sap static-mac	Configures a static MAC address entry in the forwarding database for the service that is associated with the specified SAP ID.
show service id sap	Displays configuration information about the Service Access Points (SAPs) associated with the specified service.
show service sap-using	Displays the SAP configuration for the local router.

MIB Objects

```
alaSapExtraInfoTable
   alaSapInfoTrusted
   alaSapInfoPriority
```

configure service vpls sap shutdown

Configures the administrative status for the specified Service Access Point (SAP) ID. A SAP ID is comprised of a customer-facing port (referred to as an access port) and an encapsulation value that is used to identify the type of customer traffic to map to the associated service.

configure service vpls *service-id* **sap {*slot/port* | linkagg** *agg_num*} **[:0 | :all | :*qtag1*] {no shutdown | shutdown}**

Syntax Definitions

service-id	An existing VPLS ID number.
slot/port1	The slot and port number of the service access port.
:0	Specifies a null encapsulation value for the SAP. Depending on the pre-configured encapsulation type for the access port, a SAP using a null encapsulation will direct tagged and untagged or only untagged traffic to the associated service.
:all	Specifies a wildcard SAP. All tagged or untagged traffic that is not classified into another SAP is mapped to the wildcard SAP. Not configurable on null encapsulation access ports.
:qtag1	Specifies a VLAN ID tag for traffic ingressing on the access port. Only traffic with this tag is mapped to this SAP. Not configurable on null encapsulation access ports.
agg_num	The link aggregate ID number (0–31) of a service access link aggregate.
no shutdown	Enables the administrative status of the SAP.
shutdown	Disables the administrative status of the SAP.

Defaults

By default, the administrative status of the SAP is disabled.

parameter	default
:0 | **:all** | **:***qtag1*	**:0** (null)

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- To specify a SAP ID, use the *slot/port* and **linkagg** *agg-num* parameters combined with the **:0**, **:***qtag*, or **:all** parameters. For example, enter **1/2:all** to specify the SAP on access port 1/2 that maps all traffic to this service that is not already mapped to other SAPs.
- Specify an existing VPLS service ID number and the associated access port for this SAP.

- Disabling the SAP administrative status does not remove the SAP configuration from the router.
- If an access port goes down, all SAPs associated with that port are operationally taken down as well.
- A SAP does not appear operationally down when a service is shutdown, even though traffic for that service is discarded.

Examples

```
-> configure service vpls 10 sap 1/2:10 no shutdown
-> configure service vpls 13 linkagg 20 no shutdown
-> configure service vpls 10 sap 1/2:10 shutdown
-> configure service vpls 13 linkagg 20 shutdown
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure service vpls sap create	Configures a SAP by associating a SAP ID with a Virtual Private LAN Service (VPLS).
configure service vpls sap description	Configures a description for the specified SAP ID.
configure service vpls sap trusted	Configures the trust mode for the specified SAP ID.
configure service vpls sap static-mac	Configures a static MAC address entry in the forwarding database for the service that is associated with the specified SAP ID.
show service id sap	Displays configuration information about the Service Access Points (SAPs) associated with the specified service.
show service sap-using	Displays the SAP configuration for the local router.

MIB Objects

```
sapBaseInfoTable
   sapPortId
   sapEncapValue
   sapAdminStatus
   sapOperStatus
svcBaseInfoTable
   svcId
```

configure service vpls sap static-mac

Configures a static MAC address entry in the Virtual Private LAN Service (VPLS) forwarding database (FDB) that is associated with the specified SAP ID. A SAP ID is comprised of a customer-facing port (referred to as an access port) and an encapsulation value that is used to identify the type of customer traffic to map to the associated service.

configure service vpls *service-id* **sap {***slot/port* **| linkagg** *agg_num***} [:0 | :all | :***qtag1***] static-mac** *mac-address*

configure service vpls *service-id* **sap {***slot/port* **| linkagg** *agg_num***} [:0 | :all | :***qtag1***] no static-mac** *mac-address*

Syntax Definitions

service-id	An existing VPLS ID number.
slot/port1	The slot and port number of the service access port.
:0	Specifies a null encapsulation value for the SAP. Depending on the pre-configured encapsulation type for the access port, a SAP using a null encapsulation will direct tagged and untagged or only untagged traffic to the associated service.
:all	Specifies a wildcard SAP. All tagged or untagged traffic that is not classified into another SAP is mapped to the wildcard SAP. Not configurable on null encapsulation access ports.
:qtag1	Specifies a VLAN ID tag for traffic ingressing on the access port. Only traffic with this tag is mapped to this SAP. Not configurable on null encapsulation access ports.
agg_num	The link aggregate ID number (0–31) of a service access link aggregate.
mac-address	A 48-bit MAC address (*aa:bb:cc:dd:ee:ff*). Valid addresses are any non-broadcast, non-multicast MAC, and non-IEEE reserved addresses.

Defaults

parameter	default
:0 | :all | :*qtag1*	**:0** (null)

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- To specify a SAP ID, use the *slot/port* and **linkagg** *agg-num* parameters combined with the **:0**, **:***qtag*, or **:all** parameters. For example, enter **1/2:all** to specify the SAP on access port 1/2 that maps all traffic to this service that is not already mapped to other SAPs.
- Use the **no** form of this command to remove the remote static MAC address entry from the VPLS forwarding database.

- Static MACs associated with a SAP are classified as local MACs. A local MAC is used by the associated VPLS so that MAC addresses are not learned on the edge device.
- A MAC address can participate in only one static MAC address entry (local or remote) for a specific VPLS.
- Static MAC addresses configured on one edge device are not propagated to other edge devices associated with the same VPLS instance. Each edge device has an independent forwarding database for the associated VPLS.

Examples

```
-> configure service vpls 100 sap 1/2:10 static-mac 00:00:da:3e:44:01
-> configure service vpls 101 sap linkagg 20:all static-mac 00:01:95:44:2a:10
-> configure service vpls 100 sap 1/2:10 no static-mac 00:00:da:3e:44:01
-> configure service vpls 101 sap linkagg 20:all no static-mac 00:01:95:44:2a:10
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure service vpls sap create	Configures a SAP by associating a SAP ID with a Virtual Private LAN Service (VPLS).
configure service vpls sap description	Configures a description for the specified SAP ID.
configure service vpls sap trusted	Configures the trust mode for the specified SAP ID.
configure service vpls sap shutdown	Configures the administrative status for the specified SAP ID.
show service id sap	Displays configuration information about the Service Access Points (SAPs) associated with the specified service.
show service sap-using	Displays the SAP configuration for the local router.

MIB Objects

```
tlsFdbInfoTable
   tlsFdbMacAddr
   tlsFdbType
   tlsFdbLocale
sapBaseInfoTable
   sapPortId
   sapEncapValue
svcBaseInfoTable
   svcId
```

clear service id fdb

Clears MAC addresses (including static) from the Source Learning MAC address Forwarding Database (FDB) for the specified VPLS service.

clear service id *service-id* **fdb {all | mac** *mac-address* **| sap {***slot/port* **| linkagg** *agg_num***} [:0 | :all | :***qtag1***] | mesh-sdp** *sdp-id***[**:*vc-id***]}**

Syntax Definitions

service-id	An existing VPLS ID number.
all	Clear all MAC addresses from the FDB for the specified service.
mac-address	A 48-bit MAC address (*aa:bb:cc:dd:ee:ff*) to clear from the FDB. Clears FDB entries related to this address.
slot/port1	The slot and port number of a service access port that identifies the specified SAP.
agg_num	The link aggregate ID number (0–31) of a service access link aggregate.that identifies an existing SAP.
:0	The encapsulation type portion of the SAP ID that specifies a null encapsulation value for the SAP. Depending on the pre-configured encapsulation type for the access port, a SAP using a null encapsulation will direct tagged and untagged or only untagged traffic to the associated service.
:all	The encapsulation type portion of the SAP ID that determines if untagged and tagged traffic is mapped to the SAP. Combine this parameter with the *slot/port* or **linkagg** parameters.
:qtag1	The encapsulation type portion of the SAP ID that identifies a VLAN ID tag for SAP traffic. Combine this parameter with the *slot/port* or **linkagg** parameters.
sdp-id	An existing SDP ID number.
vc-id	A VC ID number that identifies the VC ID portion of each mesh SDP binding defined for the service.

Defaults

parameter	default
:0 | :all | :*qtag*	null
vc-id	*service-id* value

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use this command to clear all MACs, a specific MAC, or all MACs associated with a specific SAP or mesh SDP from the FDB associated with the specified VPLS.
- A SAP ID is comprised of an access port or link aggregate number and an encapsulation type. To specify an existing SAP ID with this command, combine the **:all** or **:***qtag1* parameter with the *slot/port* or **linkagg** *agg_num* parameter. For example, if a SAP is mapped to access port 1/10 and customer traffic ingressing on this SAP is tagged with VLAN ID 200, enter 1/10:200 (*slot/port***:***qtag)* for the SAP ID.

Examples

```
-> clear service id 10 fdb all
-> clear service id 20 fdb mac 00:00:1a:22:33:10
-> clear service id 30 fdb 1/10:all
-> clear service id 40 fdb linkagg 10:all
-> clear service id 50 fdb mesh-sdp 10
```

Release History

Release 6.4.2; command was introduced.

Related Commands

show service fdb-info	Displays global forwarding database information for the router
show service fdb-mac	Displays the MAC address entry information found in the forwarding database.

MIB Objects

```
tlsFdbInfoTable
   tlsFdbMacAddr
   tlsFdbType
   tlsFdbLocale
sapBaseInfoTable
   sapPortId
   sapEncapValue
sdpBindTable
   sdpBindId
   sdpBindType
svcBaseInfoTable
   svcId
   svcDefMeshVcId
```

clear service id mesh-sdp ingress-vc-label

Clears the static MPLS VC label used by the far-end router to send packets to this router.

clear service id *service-id* **mesh-sdp** *sdp-id*[*:vc-id*]} **ingress-vc-label**

Syntax Definitions

service-id	An existing VPLS ID number.
sdp-id	An existing SDP ID number.
vc-id	A VC ID number that identifies the VC ID portion of each mesh SDP binding defined for the service.

Defaults

parameter	default
vc-id	*service-id* value

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

Use this command to clear ingress VC label information for the specified service-SDP association.

Examples

```
-> clear service id 10 mesh-sdp 20 ingress-vc-label
-> clear service id 20 mesh-sdp 30:10 ingress-vc-label
```

Release History

Release 6.4.2; command was introduced.

Related Commands

configure service vpls mesh-sdp ingress vc-label	Configures the static MPLS VC label used by the far-end router to send packets to this router using the specified service and SDP binding.
show service ingress-label	Displays the services that are using a specific ingress label or a range of ingress labels.

MIB Objects

```
sdpBindTable
   sdpBindId
   sdpBindType
   sdpBindAdminIngressLabel
```

```
svcBaseInfoTable
   svcId
   svcDefMeshVcId
```

show service l2profile

Displays the Layer 2 profile configuration information for the router. This type of profile is applied to access (customer-facing) ports and specifies how to process Layer 2 protocol frames ingressing on such ports.

show service l2profile [*profile-name***]**

Syntax Definitions

profile-name	An existing Layer 2 profile name. Use quotes around string if the profile name contains multiple words with spaces between them (e.g., “Alcatel-Lucent Engineering”).

Defaults

By default, all profiles are displayed if a profile name is not specified with this command.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the *profile-name* parameter to display information for a specific profile. Entering a profile name is case sensitive.
- If there are no profiles configured for the router, this command still displays the information for the default profile (def-access-profile). This profile is applied to access ports that were not associated with a specific profile.

Examples

```
->show service l2profile

Port Profile Table

Profile Name                   Stp    802.1x  802.3ad 802.1ab  GVRP   AMAP   MVRP
-----------------------------+-------+-------+-------+-------+-------+------+------
DropBPDU                     drop    drop    peer    drop    tunnel  drop   tunnel
Tunnel-Amap                  tunnel  drop    peer    drop    tunnel  tunnel tunnel
def-access-profile           tunnel  drop    peer    drop    tunnel  drop   tunnel

Number of Port Profiles: 3

->show service l2profile Tunnel-Amap

Port Profile Table

Profile Name                   Stp    802.1x  802.3ad 802.1ab  GVRP   AMAP   MVRP
-----------------------------+-------+-------+-------+-------+-------+------+------
Tunnel-Amap                  tunnel  drop    peer    drop    tunnel  tunnel tunnel

Number of Port Profiles: 1
```

output definitions

Profile Name	The name of the Layer 2 profile.
Stp	Indicates how Spanning Tree traffic control packets are processed.
802.1x	Indicates how IEEE 802.1x control packets are processed.
802.3ad	Indicates how IEEE 802.3ad control packets are processed.
802.1AB	Indicates how IEEE 802.1AB control packets are processed.
GVRP	Indicates how GARP VLAN Registration Protocol packets are processed.
AMAP	Indicates how Alcatel-Lucent Mapping Adjacency Protocol packets are processed.
MVRP	Inidicates how Multiple VLAN Registration Protocol packets are processed.

Release History

Release 6.4.2; command was introduced.
Release 6.4.3: **mvrp** field was added.

Related Commands

configure service l2profile	Configures a Layer 2 profile that is applied to a service access port.
configure service port l2profile	Assigns an existing Layer 2 profile to the specified service access port
show service port	Displays the access (customer-facing) port configuration for the router.

MIB Objects

```
alaServiceMgrPortProfileTable
   alaServiceMgrPortProfileID
   alaServiceMgrPortProfileStpBpduTreatment
   alaServiceMgrPortProfileGvrpTreatment
   alaServiceMgrPortProfile8021xTreatment
   alaServiceMgrPortProfile8021ABTreatment
   alaEServiceUNIProfileGvrpTreatment
   alaServiceMgrPortProfileAmapTreatment
   alaServiceMgrPortProfile8023ADTreatment
   alaServiceMgrPortProfileMvrpTreatment
```

show service port

Displays the access (customer-facing) port configuration for the router.

show service port [*slot/port* | **linkagg** *agg_num***]**

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).
agg-num	The link aggregate ID number (0–31).

Defaults

By default, all service access ports are displayed if a port or link aggregate number is not specified.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the *slot/port* and **linkagg** *agg-num* parameters to display the configuration for a specific port or link aggregate.
- Access ports are required to configure a Service Access Point (SAP). A SAP is the point at which customer traffic enters and exits the provider service. SAPs are not configured on network ports

Examples

```
-> show service port

Port Table

Port     Admin  Link   Cfg    Oper  Port  Port  L2Profile
Id      Status Status  MTU    MTU   Mode  Encp
-------+------+------+------+------+-----+-----+--------------------------------
8/7     Down   Down   1528   1528   accs  null  def-access-profile
8/8     Up     Up     9212   9212   accs  null  DropBPDU
8/9     Up     Down   9212   9212   accs  dotq  Tunnel-Amap
0/19    Up     Up     9212   9212   accs  null  def-access-profile

Number of Ports : 4

-> show service port 8/9

Port Table

Port     Admin  Link   Cfg    Oper  Port  Port  L2Profile
Id      Status Status  MTU    MTU   Mode  Encp
-------+------+------+------+------+-----+-----+--------------------------------
8/9     Up     Down   9212   9212   accs  dotq  Tunnel-Amap

Number of Ports : 1
```

```
-> show service port linkagg 19

Port Table

Port     Admin  Link   Cfg    Oper  Port  Port  L2Profile
Id      Status Status  MTU    MTU   Mode  Encp
-------+------+------+------+------+-----+-----+--------------------------------
0/19    Up     Up     9212   9212   accs  null  def-access-profile

Number of Ports : 1
```

output definitions

Port Id	The access port number or link aggregate ID number.
Admin Status	The administrative status (**Up** or **Down**) of the access port.
Link Status	The status of the link connection to the access port (**Up** or **Down**).
Cfg MTU	The configured MTU value for the access port.
Oper MTU	The operational MTU value for the access port.
Port Mode	The port mode (**accs**) indicates that the port is a service access port. Configured through the **configure service port mode access** command.
Port Encp	The encapsulation type associated with the access port. Configured through the **configure service port encap-type** command.
L2Profile	The name of the Layer 2 profile associated with the access port. Configured through the **configure service port l2profile** command.

Release History

Release 6.4.2; command was introduced.

Related Commands

show service l2profile	Displays the Layer 2 profile configuration for the router.
show service sap-using	Displays the Service Access Point (SAP) configuration for the local router.
show service id sap	Displays configuration information about the Service Access Points (SAPs) associated with the specified service.

MIB Objects

```
alaServiceMgrAccessPortTable
   alaServiceMgrPortID
   alaServiceMgrPortMode
   alaServiceMgrPortEncapType
   alaServiceMgrPortProfileId
```

show service customer

Displays the customer account information configured for the router.

configure service customer [*customer-id***]**

Syntax Definitions

customer-id	An existing customer ID number.

Defaults

By default, configuration information for all customer accounts is displayed.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the *customer-id* parameter to display information for a specific customer account.
- A default customer account (ID 1) exists on each router and is included in the general display of all customer accounts.This account is not user-configurable.

Examples

```
-> show service customer

Customer
    Customer-ID 1
      Description:       Default customer

    Customer-ID 129
      Contact:           VJ Pedapudi,
      Description:       Customer 129,
      Phone:             100-232-4407

    Customer-ID 1234
      Contact:           John Clark,
      Description:       Customer 1234,
      Phone:             100-434-1248

    Total Customers : 3

-> show service customer 129

Customer
   Customer-ID 129
     Contact:             VJ Pedapudi,
     Description:         Customer 129,
     Phone:               100-232-4407
```

output definitions

Customer-Id	The customer account ID number. Configured through the **configure service customer create** command.
Contact	Contact information for the customer account.Configured through the **configure service customer contact** command. This field does not display if a contact was not configured for this customer.
Description	Additional descriptive information for the customer account. Configured through the **configure service customer description** command. This field does not display if a description was not configured for this customer.
Phone	The contact phone number for the customer account. Configured through the **configure service customer phone** command. This field does not display if a phone number was not configured for this customer.

Release History

Release 6.4.2; command was introduced.

Related Commands

show service id all	Displays the detailed configuration for the specified service ID and associated service distribution and access points.

MIB Objects

```
custInfoTable
   custId
   custContact
   custDescription
   custPhone
```

show service sdp

Displays the Service Distribution Point (SDP) configuration for the switch.

show service sdp [*sdp-id***] [detail]**

Syntax Definitions

sdp-id	An existing SDP ID number.
detail	Displays detailed SDP information.

Defaults

By default, a list of all SDPs is displayed.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the *sdp-id* parameter to display information for a specific SDP.
- Use the **detail** parameter to display additional information about the SDPs.

Examples

```
-> show service sdp

Services: Service Destination Points

SdpId    Adm MTU   Opr MTU   IP address       Adm  Opr         Deliver Signal
--------+---------+---------+----------------+----+-----------+-------+--------
12       0         1514      1.1.1.3          Up   Up          LDP     TLDP
22       0         1514      1.1.1.4          Up   Up          LDP     TLDP
32       0         1514      1.1.1.5          Up   Up          LDP     TLDP
111      0         1514      1.1.1.1          Up   Up          LDP     TLDP

Number of SDPs : 4

-> show service sdp 32

Services: Service Destination Points

SdpId    Adm MTU   Opr MTU   IP address       Adm  Opr         Deliver Signal
--------+---------+---------+----------------+----+-----------+-------+--------
32       0         1514      1.1.1.5          Up   Up          LDP     TLDP
```

```
-> show service sdp detail

Services: Service Destination Points Details

Sdp Id 10  -(1.1.1.2)
  SDP Id:                10,                    SDP-Source:          N/A,
  Admin Path MTU:        0,                     Oper Path MTU:       0,
  Far End:               1.1.1.2,               Delivery:            MPLS,
  Admin State:           Down,                  Oper State:          Down,
  Signaling:             None,                  Metric:              0,
  Acct. Pol:             N/A,                   Collect Stats:       0,
  Last Status Change:    09/02/2009 17:59:54,   Adv. MTU Over.:      No,
  Last Mgmt Change:      09/02/2009 17:59:54,   VLAN VC Etype:       0x8100

  Flags:                 SdpAdminDown,
  Flags:                 TranspTunnDown TranspTunnUnstable

  KeepAlive Information:
  Admin State:           Ukwn,                  Oper State:          Ukwn,
  Hello Time:            0,                     Hello Msg Len:       0,
  Hello Timeout:         0,                     Unmatched Replies:   0,
  Max Drop Count:        0,                     Hold Down Time:      0,
  Tx Hello Msgs:         0,                     Rx Hello Msgs:       0

  Associated LSP LIST:
  Lsp Name:      path-to-R4,
  Admin State:         Down,                    Oper State:          Down,

  No Programmed LSPs

Sdp Id 11  -(2.2.2.1)
  SDP Id:                11,                    SDP-Source:          N/A,
  Admin Path MTU:        0,                     Oper Path MTU:       0,
  Far End:               2.2.2.1,               Delivery:            LDP,
  Admin State:           Down,                  Oper State:          Down,
  Signaling:             TLDP,                  Metric:              0,
  Acct. Pol:             N/A,                   Collect Stats:       0,
  Last Status Change:    09/02/2009 17:59:54,   Adv. MTU Over.:      No,
  Last Mgmt Change:      09/02/2009 17:59:54,   VLAN VC Etype:       0x8100

  Flags:                 SdpAdminDown,
  Flags:                 TldpSessDown TranspTunnDown

  KeepAlive Information:
  Admin State:           Ukwn,                  Oper State:          Ukwn,
  Hello Time:            0,                     Hello Msg Len:       0,
  Hello Timeout:         0,                     Unmatched Replies:   0,
  Max Drop Count:        0,                     Hold Down Time:      0,
  Tx Hello Msgs:         0,                     Rx Hello Msgs:       0

  Associated LSP LIST:
  No LSPs Associated

  No Programmed LSPs

Sdp Id 30  -(0.0.0.0)
  SDP Id:                30,                    SDP-Source:          N/A,
  Admin Path MTU:        0,                     Oper Path MTU:       0,
  Far End:               0.0.0.0,               Delivery:            LDP,
```

```
  Admin State:           Down,                  Oper State:          Down,
  Signaling:             TLDP,                  Metric:              0,
  Acct. Pol:             N/A,                   Collect Stats:       0,
  Last Status Change:    09/10/2009 18:35:35,   Adv. MTU Over.:      No,
  Last Mgmt Change:      09/10/2009 18:36:47,   VLAN VC Etype:       0x8100

  Flags:                 SdpAdminDown,
  Flags:                 TranspTunnDown TranspTunnUnstable

  KeepAlive Information:
  Admin State:           Ukwn,                  Oper State:          Ukwn,
  Hello Time:            0,                     Hello Msg Len:       0,
  Hello Timeout:         0,                     Unmatched Replies:   0,
  Max Drop Count:        0,                     Hold Down Time:      0,
  Tx Hello Msgs:         0,                     Rx Hello Msgs:       0

  Associated LSP LIST:
  No LSPs Associated

  No Programmed LSPs

Number of SDPs : 3

-> show service sdp 10 detail

Services: Service Destination Points Details

Sdp Id 10  -(1.1.1.2)
  SDP Id:                10,                    SDP-Source:          N/A,
  Admin Path MTU:        0,                     Oper Path MTU:       0,
  Far End:               1.1.1.2,               Delivery:            MPLS,
  Admin State:           Down,                  Oper State:          Down,
  Signaling:             None,                  Metric:              0,
  Acct. Pol:             N/A,                   Collect Stats:       0,
  Last Status Change:    09/02/2009 17:59:54,   Adv. MTU Over.:      No,
  Last Mgmt Change:      09/02/2009 17:59:54,   VLAN VC Etype:       0x8100

  Flags:                 SdpAdminDown,
  Flags:                 TranspTunnDown TranspTunnUnstable

  KeepAlive Information:
  Admin State:           Ukwn,                  Oper State:          Ukwn,
  Hello Time:            0,                     Hello Msg Len:       0,
  Hello Timeout:         0,                     Unmatched Replies:   0,
  Max Drop Count:        0,                     Hold Down Time:      0,
  Tx Hello Msgs:         0,                     Rx Hello Msgs:       0

  Associated LSP LIST:
  No LSPs Associated
```

```
No Programmed LSPs
```

output definitions

SDP Id	The SDP identifier comprised of the SDP ID number and the IP address of the far-end router for this SDP tunnel. For example, **10: -(1.1.1.2)** identifies SDP 10 with the tunnel endpoint at router 1.1.1.2.
Admin Path MTU	The desired largest frame size that can pass through this SDP to the far-end router without requiring fragmentation. Configured through the **configure service sdp path-mtu** command.
Oper Path MTU	The actual largest frame size that can pass through this SDP to the far-end router without requiring fragmentation.
Far End	The IP address of the remote end of the MPLS tunnel defined by this SDP. Configured through the **configure service sdp far-end** command.
Delivery	Specifies the type of delivery used by this SDP. In this case, LDP-based MPLS is the supported delivery method; GRE is not supported.
Admin State	The administrative state of this SDP (**Up** or **Down**). Configured through the **configure service sdp shutdown** command.
Oper State	The operational state of this SDP (**Up** or **Down**).
Signaling	Indicates whether or not Targeted LDP signaling is enabled (**none** or **TLDP**). Note that if TLDP is not enabled, only static LSPs are configurable for this SDP.
Collect Stats	Specifies whether or not LDP statistics are collected for this SDP.
Last Status Change	The date and time of the last operational status change to this SDP.
Last Mgmt Change	The date and time of the last management-initiated change to this SDP.
Flags	The conditions that affect the operational status of this SDP.
Associated LSP List	Displays static LSP information.
Programmed LSP List	Displays LDP-signaled LSP information.

Release History

Release 6.4.2; command was introduced.

Related Commands

show service sdp-using	Displays the Service Distribution Point (SDP) usage for the local router or for a far-end router IP address.
show service id sdp	Displays the detailed configuration for the specified service ID, including all SDPs and SAPs associated with the service.

MIB Objects

show service id all

Displays detailed configuration information about the specified service ID, including the SDP and SAP configuration associated with the service.

show service id *service-id* **all**

Syntax Definitions

service-id	An existing VPLS ID number.

Defaults

N/A.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

The service ID is a unique number that identifies a specific VPLS. All information associated with the service ID is displayed.

Examples

```
-> show service id 100 all

Service Detailed Information
  Service Id:         100,                Vpn Id:            N/A,
  Service Type:       VPLS,
  Customer Id:        1,
  Last Status Change:  01/19/2009 13:09:36,
  Last Mgmt Change:   01/19/2009 13:09:10,
  Admin State:        Up,                 Oper State:        Up,
  MTU:                1514,               Def. Mesh VC Id:   100,
  SAP Count:          5,                  SDP Bind Count:    1,
  Snd Flush on Fail:  Disabled,           Host Conn Verify:  N/A,
  Propagate MacFlush:  N/A

    Service Destination Points(SDPs)
        Sdp Id 10:100  -(10.11.0.6)
          SDP Id:             10:100,                 Type:               Mesh,
          VC Type:            Ether,                  VC Tag:             n/a,
          Admin Path MTU:     1514,                   Oper Path MTU:      1514,
          Far End:            10.11.0.6,              Delivery:           LDP,

          Admin State:        Up,                     Oper State:         Up,
          Acct. Pol:          N/A,                    Collect Stats:      LDP,
          Ingress Label:      131069,                 Egress Label:    131070,
          Ing mac Fltr:       n/a,                    Egr mac Fltr:       n/a,
          Ing ip Fltr:        n/a,                    Egr ip Fltr:        n/a,
          Admin ControlWord:  N/A,                    Oper ControlWord:   False,
          Last Status Change: 01/19/2009 13:10:48,    Signaling:          TLDP,
          Last Mgmt Change:   01/19/2009 13:09:10,    Force Vlan-Vc: Disabled,
```

```
        Class Fwding State:  N/A,
        Flags:               None

    Service Destination Points(SDPs)
        Sdp Id 50:200  -(10.11.0.7)
        SDP Id:              50:200,                 Type:               Mesh,
        VC Type:             Ether,                  VC Tag:             N/A,
        Admin Path MTU:      0,                      Oper Path MTU:      0,
        Far End:             10.11.0.7,              Delivery:           LDP,

        Admin State:         Up,                     Oper State:         Down,
        Acct. Pol:           N/A,                    Collect Stats:      LDP,
        Ingress Label:       0,                      Egress Label:       0,
        Admin ControlWord:   N/A,                   Oper ControlWord:   False,
        Last Status Change:  01/19/2009 22:28:16,    Signaling:          TLDP,
        Last Mgmt Change:    15/19/2009 11:18:50,    Force Vlan-Vc:   Disabled,
        Flags:               SdpOperDown,
        Flags:               NoIngVCLabel NoEgrVCLabel,
        Flags:               PathMTUTooSmall

    Service Access Points
        SAP 1/2:100
        Service Id:          100,
        SAP:                 1/2:100,                Encap:              q-tag,
        Admin State:         Up,                     Oper State:         Down,
        Flags:               PortOperDown PortMTUTooSmall,
        Multi Svc Site:      None,
        Last Status Change:  01/19/2009 13:09:10,
        Last Mgmt Change:    01/19/2009 13:09:10

       SAP 8/8:300
        Service Id:          100,
        SAP:                 8/8:300,                Encap:              q-tag,
        Admin State:         Up,                     Oper State:         Up,
        Flags:               None,
        Multi Svc Site:      None,
        Last Status Change:  01/19/2009 13:09:36,
        Last Mgmt Change:    01/19/2009 13:09:10
```

output definitions

SvcId	The unique service identification number used to identify the service. Configured through the **configure service vpls create** command.
Service Type	The type of service (only VPLS is supported).
Customer Id	The customer account ID number. Configured through the **configure service customer create** command.
Last Status Change	The date and time of the last operational status change to this service.
Last Mgmt Change	The date and time of the last management-initiated change to this service.
Admin State	The administrative state of the service (**Up** or **Down**). Configured through the **configure service vpls shutdown** command.
Oper State	The operational state of the service (**Up** or **Down**).

output definitions

MTU	The largest frame size that can pass through this service without requiring fragmentation. Configured through the **configure service vpls service-mtu** command.
Def. Mesh VC Id	The default VC ID for the mesh SDP binding for this service. Configured through the **configure service vpls def-mesh-vc-id** command.
SAP Count	The number of SAPs associated with this service.
SDP Bind Count	The number of SDPs bound to this service.
Send Flush on Fail	Whether or not (**Enabled** or **Disabled**) a MAC flush message is sent when an access port or SAP failure occurs. Configured through the **configure service vpls send-flush-on-failure** command.
Service Destination Points (SDPs)	The following fields display configuration information for each SDP associated with this service.
SDP Id	The SDP identifier comprised of the SDP ID number, the service ID number, and the IP address of the far-end router for this SDP tunnel. For example, **10:100 -(10.11.0.6)** identifies SDP 10 bound to VPLS 100 with the tunnel endpoint at router 10.11.0.6.
Type	The SDP binding type (**mesh** or **spoke**) for this service. The spoke binding type is not supported. Configured through the **configure service vpls mesh-sdp** command.
VC Type	The type of VC (**Ether**, **Vlan**, or **Vpls**). Configured through the **configure service vpls mesh-sdp** command.
Admin Path MTU	The desired largest frame size that can pass through this SDP to the far-end router without requiring fragmentation. Configured through the **configure service sdp path-mtu** command.
Oper Path MTU	The actual largest frame size that can pass through this SDP to the far-end router without requiring fragmentation.
Far End	The IP address of the remote end of the MPLS tunnel defined by this SDP. Configured through the **configure service sdp far-end** command.
Delivery	Specifies the type of delivery used by this SDP. In this case, LDP-based MPLS is the supported delivery method; GRE is not supported.
Admin State	The administrative state of this SDP (**Up** or **Down**). Configured through the **configure service sdp shutdown** command.
Oper State	The operational state of this SDP (**Up** or **Down**).
Collect Stats	Specifies whether or not LDP statistics are collected for this SDP.
Ingress Label	The VC label used by the far-end device to send packets to the local device for this SDP binding.
Egress Label	The VC label used by the local device to send packets to the far-end device for SDP binding.
Last Status Change	The date and time of the last operational status change to this SDP.
Signaling	The signaling protocol used to obtain the ingress and egress labels from frames transmitted and received on this SDP.
Last Mgmt Change	The date and time of the last management-initiated change to this SDP.
Flags	The conditions that affect the operational status of this SDP.

output definitions

Service Access Points (SAPs)	The following fields display configuration information for each SDP associated with this service.
Service Id	The service ID associated with the SAP. Configured through the **configure service vpls create** command and bound to the SAP using the **configure service vpls sap create** command.
SAP	The access port number for the SAP. Configured through the **configure service port mode access** command and bound to the SAP using the **configure service vpls sap create** command.
Encap	The encapsulation type (**null** or **dot1q**) configured for the access port. This indicates the value of the label used to identify the SAP on the access port. Configured through the **configure service port encap-type** command.
Admin State	The administrative state of this SAP (**Up** or **Down**). Configured through the **configure service vpls sap shutdown** command.
Oper State	The operational state of this SAP (**Up** or **Down**).
Flags	The conditions that affect the operational status of this SAP.
Multi Svc Site	The multi-service site of which the SAP is a member.
Last Status Change	The date and time of the last operational status change to this SAP.
Last Mgmt Change	The date and time of the last management-initiated change to this SAP.

Release History

Release 6.4.2; command was introduced.

Related Commands

show service id base	Displays the basic configuration for the specified service ID and a list of service distribution and access points associated with the service.
show service id labels	Displays a list of all labels that the specified service is using.

MIB Objects

show service id base

Displays basic information about the specified service, including a list of SDPs and SAPs associated with the service.

show service id *service-id* **base**

Syntax Definitions

service-id	An existing VPLS ID number.

Defaults

N/A.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

The service ID is a unique number that identifies a specific VPLS. All information associated with the service ID is displayed.

Examples

```
-> show service id 9999 base

Service Basic Information
  Service Id:         100,                 Vpn Id:             N/A,
  Service Type:       VPLS,
  Customer Id:        1,
  Last Status Change: 01/19/2009 13:09:36,
  Last Mgmt Change:   01/19/2009 13:09:10,
  Admin State:        Up,                  Oper State:         Up,
  MTU:                1514,                Def. Mesh VC Id:    100,
  SAP Count:          5,                   SDP Bind Count:     1,
  Snd Flush on Fail:  Disabled,            Host Conn Verify:   N/A,
  Propagate MacFlush:  N/A

Service Access & Destination Points

Identifier                                 Type         AdmMTU  OprMTU  Adm  Opr
-------------------------------------------+------------+-------+-------+----+-----
sap:1/2:100                                q-tag        1518    1518    Up   Down
sap:1/2:110                                q-tag        1518    1518    Up   Down
sap:1/2:all                                q-tag        1518    1518    Up   Down
sap:1/11:200                               q-tag        1518    1518    Up   Up
sap:8/8:300                                q-tag        1518    1518    Up   Up
sdp:10:100 M(10.11.0.6)                    n/a          1514    1514    Up   Up
```

output definitions

SvcId	The unique service identification number used to identify the service. Configured through the **configure service vpls create** command.
Service Type	The type of service (only VPLS is supported).
Customer Id	The customer account ID number. Configured through the **configure service customer create** command.
Last Status Change	The date and time of the last operational status change to this service.
Last Mgmt Change	The date and time of the last management-initiated change to this service.
Admin State	The administrative state of the service (**Up** or **Down**). Configured through the **configure service vpls shutdown** command.
Oper State	The operational state of the service (**Up** or **Down**).
MTU	The largest frame size that can pass through this service without requiring fragmentation. Configured through the **configure service vpls service-mtu** command.
Def. Mesh VC Id	The default VC ID for the mesh SDP binding for this service. Configured through the **configure service vpls def-mesh-vc-id** command.
SAP Count	The number of SAPs associated with this service.
SDP Bind Count	The number of SDPs bound to this service.
Send Flush on Fail	Whether or not (**Enabled** or **Disabled**) a MAC flush message is sent when an access port or SAP failure occurs. Configured through the **configure service vpls send-flush-on-failure** command.
Service Access and Destination Points	The following fields display basic information for each SAP and SDP associated with this service.
Identifier	The SAP or SDP identifier: • The SAP ID is comprised of the access port number and encapsulation value (0, VLAN ID, or all). For example, **sap:1/2:100** identifies a SAP on access port 1/2 using a VLAN ID 100 to map customer traffic tagged with VLAN 100 to the service associated with the SAP. • The SDP identifier is comprised of the SDP ID number, the service ID number, and the IP address of the far-end router for this SDP tunnel. For example, **10:100 -M(10.11.0.6)** identifies SDP 10 bound to VPLS 100 with the tunnel endpoint at router 10.11.0.6.
Type	The encapsulation type (**null** or **dot1q**) configured for the access port. This indicates the value of the label used to identify the SAP on the access port. Configured through the **configure service port encap-type** command. Note that the encapsulation type does not apply to SDPs;
AdmMTU	The desired largest frame size that can pass through the service or SDP to the far-end router without requiring fragmentation. Configured through the **configure service vpls service-mtu** or **configure service sdp path-mtu** commands.
OprMTU	The actual largest frame size that can pass through the service or SDP to the far-end router without requiring fragmentation.

output definitions

Adm	The administrative state of the SAP or SDP (**Up** or **Down**). Configured through the **configure service vpls sap shutdown** or **configure service sdp shutdown** commands.
Opr	The operational state of the SAP or SDP (**Up** or **Down**).

Release History

Release 6.4.2; command was introduced.

Related Commands

show service id all	Displays the detailed configuration for the specified service ID and associated service distribution and access points.
show service id labels	Displays a list of all labels that the specified service is using.

MIB Objects

show service id labels

Displays a list of all labels that the specified service is using.

show service id *service-id* **labels**

Syntax Definitions

service-id	An existing VPLS ID number.

Defaults

N/A.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

The service ID is a unique number that identifies a specific VPLS. All ingress and egress labels that this service is using are displayed.

Examples

```
-> show service id 100 labels
Martini Service Labels

Svc Id     Sdp Binding        Type  I.Lbl                E.Lbl
----------+------------------+-----+--------------------+--------------------
100        10:100             Mesh  131069               131070

Number of Bindings Found : 1
```

output definitions

Svc Id	The unique service identification number used to identify the service.
SDP Binding	The SDP ID number associated with the service.
Type	The SDP binding type (**mesh** or **spoke**) for the service. The spoke SDP binding type is not supported.
I.Lbl	The VC label used by the far-end device to send packets to the local device for the SDP binding.
E.Lbl	The VC label used by the local device to send packets to the far-end device for the SDP binding.

Release History

Release 6.4.2; command was introduced.

Related Commands

show service id all	Displays the detailed configuration for the specified service ID and associated service distribution and access points.
show service egress-label	Displays a list of services that are using the specified egress labels.
show service ingress-label	Displays a list of service that are using the specified ingress labels.

MIB Objects

show service id sap

Displays configuration information about the Service Access Points (SAPs) associated with the specified service.

show service id *service-id* **sap [***slot/port* **| linkagg** *agg_num***] [:0 | :all | :***qtag1***]**

Syntax Definitions

service-id	An existing VPLS ID number.
slot/port1	The slot and port number of the service access port.
agg_num	The link aggregate ID number (0–31) of a service access link aggregate.
:0	Specifies no (null) encapsulation value for the SAP. Depending on the pre-configured encapsulation type for the access port, a SAP using a null encapsulation will direct tagged and untagged or only untagged traffic to the associated service.
:all	Specifies a wildcard SAP. All 802.1q-tagged or untagged traffic that is not classified into another SAP is mapped to the wildcard SAP. Not configurable on null encapsulation access ports.
:qtag1	Specifies a VLAN ID tag for traffic ingressing on the access port. Only traffic with this tag is mapped to this SAP. Not configurable on null encapsulation access ports.

Defaults

By default, a list of all SAPs associated with the specified service ID is displayed.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

To display detailed information for an individual SAP, specify a SAP ID using the *slot/port* and **linkagg** *agg-num* parameters combined with the **:0**, **:***qtag*, or **:all** parameters. For example, enter **1/2:all** to display information for the SAP on access port 1/2 that maps all traffic that is not classified into other SAPs to this service.

Examples

```
-> show service id 100 sap

PortId     SvcId        Adm    Oper   Trusted Pri
----------+------------+------+------+-------+-----
1/11:200    100         Up     Up     Yes     0
1/11:all    100         Up     Up     Yes     0
1/11:0      100         Down   Down   Yes     0

Number of SAPs : 3
```

output definitions

PortId	The access port number and encapsulation type for the SAP. Configured through the **configure service port mode access** command.
Service Id	The service ID associated with the SAP. Configured through the **configure service vpls create** command and bound to the SAP using the **configure service vpls sap create** command.
Adm	The administrative state of this SAP (**Up** or **Down**). Configured through the **configure service vpls sap shutdown** command.
Oper	The operational state of this SAP (**Up** or **Down**).
Trusted	The trusted status (**Yes** or **No**) for traffic mapped to this SAP. If **Yes** is displayed, the internal priority value for ingress traffic is used. If **No** is displayed, the value displayed in the **Pri** field is used.
Pri	The priority value assigned to the traffic mapped to this SAP. This value is only applied if the **Trusted** status for the SAP is set to **Yes**.

```
-> show service id 100 sap 1/11:200

Service Access Points(SAP)
  Service Id:          100,
  SAP:                 1/11:200,                 Encap:              q-tag,
  Admin State:         Up,                       Oper State:         Up,
  Flags:               None,
  Multi Svc Site:      None,
  Last Status Change:  01/19/2009 13:09:36,
  Last Mgmt Change:    01/19/2009 13:09:10
```

output definitions

Service Id	The service ID associated with the SAP. Configured through the **configure service vpls create** command and bound to the SAP using the **configure service vpls sap create** command.
SAP	The access port number for the SAP. Configured through the **configure service port mode access** command and bound to the SAP using the **configure service vpls sap create** command.
Encap	The encapsulation type (**null** or **dot1q**) configured for the access port. This indicates the value of the label used to identify the SAP on the access port. Configured through the **configure service port encap-type** command.
Admin State	The administrative state of this SAP (**Up** or **Down**). Configured through the **configure service vpls sap shutdown** command.
Oper State	The operational state of this SAP (**Up** or **Down**).
Flags	The conditions that affect the operational status of this SAP.
Multi Svc Site	The multi-service site of which the SAP is a member.
Last Status Change	The date and time of the last operational status change to this SAP.
Last Mgmt Change	The date and time of the last management-initiated change to this SAP.

Release History

Release 6.4.2; command was introduced.

Related Commands

show service id all	Displays the detailed configuration for the specified service ID, including all SDPs and SAPs associated with the service.
show service sap-using	Displays the Service Access Point (SAP) configuration for the local router.
show service port	Displays the access (customer-facing) port configuration for the router.

MIB Objects

show service id sdp

Displays configuration information for the Service Distribution Points (SDPs) associated with the specified service.

show service id *service-id* **sdp [***sdp-id***[:***vc-id***] | far-end** *ip-address***] [detail]**

Syntax Definitions

service-id	An existing VPLS ID number.
sdp-id	An existing SDP ID number.
vc-id	A VC ID number used to validate the VC ID portion of each mesh SDP binding defined for the service.
ip-address	The system IP address for the far-end router. This is the user-configured Loopback0 address if the far-end router is an OmniSwitch.
detail	Displays detailed SDP information.

Defaults

By default, a list of all SDPs associated with the specified service ID is displayed.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the *sdp-id* parameter to display information for a specific SDP.
- Use the **far-end** *ip-addr* parameter to display information about an SDP with a specific far-end address.
- Use the **detail** parameter to display additional information about the SDPs.

Examples

```
-> show service id 100 sdp

Services: Service Destination Points

SdpId            Type IP address      Adm     Opr       I.Lbl       E.Lbl
-----------------+----+--------------+-------+---------+-----------+-----------
10:100           Mesh 10.11.0.6       Up      Up        131069      131070

Number of SDPs : 1

-> show service id 100 sdp detail

Services: Service Destination Points Details
    Sdp Id 10:100  -(10.11.0.6)
      SDP Id:              10:100,                  Type:              Mesh,
```

```
      VC Type:             Ether,                    VC Tag:             n/a,
      Admin Path MTU:      1514,                     Oper Path MTU:      1514,
      Far End:             10.11.0.6,                Delivery:           LDP,

      Admin State:         Up,                       Oper State:         Up,
      Acct. Pol:           N/A,                      Collect Stats:      LDP,
      Ingress Label:       131069,                   Egress Label:       131070,
      Ing mac Fltr:        n/a,                      Egr mac Fltr:       n/a,
      Ing ip Fltr:         n/a,                      Egr ip Fltr:        n/a,
      Admin ControlWord:   N/A,                      Oper ControlWord:   False,
      Last Status Change:  01/19/2009 13:10:48,      Signaling:          TLDP,
      Last Mgmt Change:    01/19/2009 13:09:10,      Force Vlan-Vc:      Disabled,
      Class Fwding State:  N/A,
      Flags:               None

    Number of SDPs : 1

-> show service id 100 sdp far-end 10.11.0.6

Service Destination Point(Far-End : 10.11.0.6)

SdpId            Type IP address      Adm     Opr       I.Lbl       E.Lbl
-----------------+----+--------------+-------+---------+-----------+-----------
10:100           Mesh 10.11.0.6       Up      Up        131069      131070

Number of SDPs : 1

-> show service id 100 sdp far-end 10.11.0.6 detail

Service Destination Point(Far-End : 10.11.0.6) Details

    Sdp Id 10:100  -(10.11.0.6)
      SDP Id:              10:100,                   Type:               Mesh,
      VC Type:             Ether,                    VC Tag:             n/a,
      Admin Path MTU:      1514,                     Oper Path MTU:      1514,
      Far End:             10.11.0.6,                Delivery:           LDP,

      Admin State:         Up,                       Oper State:         Up,
      Acct. Pol:           N/A,                      Collect Stats:      LDP,
      Ingress Label:       131069,                   Egress Label:       131070,
      Ing mac Fltr:        n/a,                      Egr mac Fltr:       n/a,
      Ing ip Fltr:         n/a,                      Egr ip Fltr:        n/a,
      Admin ControlWord:   N/A,                      Oper ControlWord:   False,
      Last Status Change:  01/19/2009 13:10:48,      Signaling:          TLDP,
      Last Mgmt Change:    01/19/2009 13:09:10,      Force Vlan-Vc:      Disabled,
      Class Fwding State:  N/A,
      Flags:               None

    Number of SDPs : 1
```

output definitions

SDP Id	The SDP identifier comprised of the SDP ID number, the service ID number, and the IP address of the far-end router for this SDP tunnel. For example, **10:100 -(10.11.0.6)** identifies SDP 10 bound to VPLS 100 with the tunnel endpoint at router 10.11.0.6.
Type	The SDP binding type (**mesh** or **spoke**) for this service. The spoke binding type is not supported. Configured through the **configure service vpls mesh-sdp** command.
VC Type	The type of VC (**Ether**, **Vlan**, or **Vpls**). Configured through the **configure service vpls mesh-sdp** command.
Admin Path MTU	The desired largest frame size that can pass through this SDP to the far-end router without requiring fragmentation. Configured through the **configure service sdp path-mtu** command.
Oper Path MTU	The actual largest frame size that can pass through this SDP to the far-end router without requiring fragmentation.
Far End	The IP address of the remote end of the MPLS tunnel defined by this SDP. Configured through the **configure service sdp far-end** command.
Delivery	Specifies the type of delivery used by this SDP. In this case, LDP-based MPLS is the supported delivery method; GRE is not supported.
Admin State	The administrative state of this SDP (**Up** or **Down**). Configured through the **configure service sdp shutdown** command.
Oper State	The operational state of this SDP (**Up** or **Down**).
Collect Stats	Specifies whether or not LDP statistics are collected for this SDP.
Ingress Label	The VC label used by the far-end device to send packets to the local device for this SDP binding.
Egress Label	The VC label used by the local device to send packets to the far-end device for SDP binding.
Last Status Change	The date and time of the last operational status change to this SDP.
Signaling	The signaling protocol used to obtain the ingress and egress labels from frames transmitted and received on this SDP.
Last Mgmt Change	The date and time of the last management-initiated change to this SDP.
Flags	The conditions that affect the operational status of this SDP.

Release History

Release 6.4.2; command was introduced.

Related Commands

show service id all	Displays the detailed configuration for the specified service ID, including all SDPs and SAPs associated with the service.
show service id labels	Displays a list of all labels that the specified service is using.
show service sdp-using	Displays the SDP usage for the local router or for a far-end router IP address.
show service sdp	Displays the SDP configuration for the switch.

MIB Objects

show service sap-using

Displays the Service Access Point (SAP) configuration for the local router.

show service sap-using [sap {*slot/port* **| linkagg** *agg_num***}] [:0 | :all | :***qtag1***]**

Syntax Definitions

slot/port1	The slot and port number of the service access port.
agg_num	The link aggregate ID number (0–31) of a service access link aggregate.
:0	Specifies no (null) encapsulation value for the SAP. Depending on the pre-configured encapsulation type for the access port, a SAP using a null encapsulation will direct tagged and untagged or only untagged traffic to the associated service.
:all	Specifies a wildcard SAP. All 802.1q-tagged or untagged traffic that is not classified into another SAP is mapped to the wildcard SAP. Not configurable on null encapsulation access ports.
:qtag1	Specifies a VLAN ID tag for traffic ingressing on the access port. Only traffic with this tag is mapped to this SAP. Not configurable on null encapsulation access ports.

Defaults

By default, a list of all SAPs configured for the router is displayed.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

To display detailed information for an individual SAP, specify a SAP ID using the *slot/port* and **linkagg** *agg-num* parameters combined with the **:0**, **:***qtag*, or **:all** parameters. For example, enter **1/2:all** to display information for the SAP on access port 1/2 that maps all traffic that is not classified into other SAPs to this service.

Examples

```
-> show service sap-using

Service Access Points

PortId              SvcId      Adm  Opr  Trusted Pri
--------------------+----------+----+----+-------+---
1/2:100             100        Up   Down Yes     0
1/2:110             100        Up   Down Yes     0
1/2:all             100        Up   Down Yes     0
1/11:200            100        Up   Up   Yes     0
8/8:300             100        Up   Up   Yes     0
1/3                 200        Up   Up   Yes     0
0/5:400             200        Up   Up   Yes     0
```

```
-> show service sap-using sap linkagg 5:400

Service Access Points Using Port 0/5:400

PortId              SvcId      Adm  Opr  Trusted Pri
--------------------+----------+----+----+-------+---
0/5:400             200        Up   Up Yes     0

Number of SAPs : 1
```

output definitions

PortId	The access port number and encapsulation type for the SAP. Configured through the **configure service port mode access** command.
Service Id	The service ID associated with the SAP. Configured through the **configure service vpls create** command and bound to the SAP using the **configure service vpls sap create** command.
Adm	The administrative state of this SAP (**Up** or **Down**). Configured through the **configure service vpls sap shutdown** command.
Oper	The operational state of this SAP (**Up** or **Down**).
Trusted	The trusted status (**Yes** or **No**) for traffic mapped to this SAP. If **Yes** is displayed, the internal priority value for ingress traffic is used. If **No** is displayed, the value displayed in the **Pri** field is used.
Pri	The priority value assigned to the traffic mapped to this SAP. This value is only applied if the **Trusted** status for the SAP is set to **Yes**.

Release History

Release 6.4.2; command was introduced.

Related Commands

show service id sap	Displays the detailed configuration for the specified service ID, including all SDPs and SAPs associated with the service.
show service port	Displays the access (customer-facing) port configuration for the router.

MIB Objects

show service sdp-using

Displays the Service Distribution Point (SDP) usage for the local router or for a far-end router IP address.

show service sdp-using [*sdp-id***[:***vc-id***] | far-end** *ip-address***]**

Syntax Definitions

sdp-id	An existing SDP ID number.
vc-id	A VC ID number used to validate the VC ID portion of each mesh SDP binding defined for the service.
ip-address	The system IP address for the far-end router. This is the user-configured Loopback0 address if the far-end router is an OmniSwitch.

Defaults

By default, a list of all associated SDPs configured for the switch is displayed.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the *sdp-id* parameter to display information for a specific SDP.
- Use the **far-end** *ip-addr* parameter to display information about an SDP with a specific far-end address.

Examples

```
-> show service sdp-using

SDP Using

SvcId       SdpId               Type    Far End        Opr    I.Label  E.Label
-----------+-------------------+-------+--------------+------+--------+--------
100         10:100              Mesh    10.11.0.6      Up     131069   131070
200         30:200              Mesh    30.1.2.3       Down   0        0

Number of SDPs : 2

-> show service sdp-using 10

Service Destination Point (Sdp Id : 10:0)

SvcId       SdpId               Type    Far End        Opr    I.Label  E.Label
-----------+-------------------+-------+--------------+------+--------+--------
100         10:100              Mesh    10.11.0.6      Up     131069   131070

Number of SDPs : 1
```

```
-> show service sdp-using far-end 10.11.0.5

Service Destination Point(Far-End : 10.11.0.6)

SvcId       SdpId               Type    Far End        Opr    I.Label  E.Label
-----------+-------------------+-------+--------------+------+--------+--------
100         10:100              Mesh    10.11.0.6      Up     131069   131070

Number of SDPs : 1
```

output definitions

SvcId	The service ID associated with the SDP. Configured through the **configure service vpls create** command and bound to the SAP using the **configure service vpls mesh-sdp** command.
SDP Id	The SDP identifier comprised of the SDP ID number, the service ID number, and the IP address of the far-end router for this SDP tunnel. For example, **10:100** identifies SDP 10 bound to VPLS 100 with the tunnel endpoint at router 10.11.0.6.
Type	The SDP binding type (**mesh** or **spoke**) for this service. The spoke binding type is not supported. Configured through the **configure service vpls mesh-sdp** command.
Far End	The IP address of the remote end of the MPLS tunnel defined by this SDP. Configured through the **configure service sdp far-end** command.
Oper S	The operational state of this SDP (**Up** or **Down**).
I. Label	The VC label used by the far-end device to send packets to the local device for this SDP binding.
E. Label	The VC label used by the local device to send packets to the far-end device for SDP binding.

Release History

Release 6.4.2; command was introduced.

Related Commands

show service id all	Displays the detailed configuration for the specified service ID, including all SDPs and SAPs associated with the service.
show service id labels	Displays a list of all labels that the specified service is using.
show service id sdp	Displays configuration information for the Service Distribution Points (SDPs) associated with the specified service.
show service sdp	Displays the SDP configuration for the switch.

MIB Objects

show service egress-label

Displays the services that are using a specific egress label or a range of egress labels.

show service egress-label *start-label* **[***end-label***]**

Syntax Definitions

start-label	An egress label number. The valid range is 0 or 16–131071.
end-label	The last egress label number in a range of labels. The valid range is 2049–131071.

Defaults

By default, all services associated with the starting label number are displayed.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the optional *end-label* parameter along with the *start-label* parameter to specify a range of egress labels.
- If an ending label number is not specified, then all services using the starting label number are displayed. No range is specified.

Examples

```
-> show service egress-label 131070
Martini Service Labels

Svc Id     Sdp Binding        Type  I.Lbl                E.Lbl
----------+------------------+-----+--------------------+--------------------
100        10:100             Mesh  131069               131070

Number of Bindings Found : 1
```

output definitions

Svc Id	The unique service identification number used to identify the service.
SDP Binding	The SDP ID number associated with the service.
Type	The SDP binding type (**mesh** or **spoke**) for the service. The spoke SDP binding type is not supported.
I.Lbl	The VC label used by the far-end device to send packets to the local device for this SDP binding.
E.Lbl	The VC label used by the local device to send packets to the far-end device for this SDP binding.

Release History

Release 6.4.2; command was introduced.

Related Commands

show service ingress-label	Displays the services that are using a specific ingress label or a range of ingress labels.
show service id labels	Displays a list of all labels that the specified service is using.

MIB Objects

show service ingress-label

Displays the services that are using a specific ingress label or a range of ingress labels.

show service ingress-label *start-label* **[***end-label***]**

Syntax Definitions

start-label	An ingress label number. The valid range is 0 or 2048–131071.
end-label	The last ingress label number in a range of labels. The valid range is 2049–131071.

Defaults

By default, all services associated with the starting label number are displayed.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the optional *end-label* parameter along with the *start-label* parameter to specify a range of ingress labels.
- If an ending label number is not specified, then all services using the starting label number are displayed. No range is specified.

Examples

```
-> show service ingress-label 2048 131071
Martini Service Labels

Svc Id     Sdp Binding       Type  I.Lbl               E.Lbl
----------+-----------------+-----+-------------------+--------------------
100         10:100             Mesh  131069               131070
200         30:200             Mesh  0                    0

Number of Bindings Found : 2
```

output definitions

Svc Id	The unique service identification number used to identify the service.
SDP Binding	The SDP ID number associated with the service.
Type	Indicates the SDP binding type (**mesh** or **spoke**) for the service. The spoke SDP binding type is not supported.
I.Lbl	The VC label used by the far-end device to send packets to the local device for this SDP binding.
E.Lbl	The VC label used by the local device to send packets to the far-end device for this SDP binding.

Release History

Release 6.4.2; command was introduced.

Related Commands

show service egress-label	Displays the services that are using a specific egress label or a range of egress labels.
show service id labels	Displays a list of all labels that the specified service is using.
clear service id mesh-sdp ingress-vc-label	Clears the static MPLS VC label used by the far-end router to send packets to this router.

MIB Objects

show service fdb-info

Displays global forwarding database (FDB) information for the router.

show service fdb-info

Syntax Definitions

N/A.

Defaults

N/A.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

This command displays the FDB information that exists for all services. Fields that display “N/A” are currently not supported.

Examples

```
-> show service fdb-info
Forwarding Database (FDB) Information

    Service 100
      Service Id:         100,              Mac Move:             N/A,
      Mac Move Rate:      N/A,              Mac Move Timeout:     N/A,
      Table Size:         N/A,              Total Count:          5,
      Learned Count:      5,                Static Count:         0,
      OAM-learned Count:  N/A,              DHCP-learned Count:   N/A,
      Host-learned Count: N/A,
      Remote Age:         N/A,              Local Age:            N/A,
      Mac Learning:       N/A,              Discard Unknown:      N/A,
      Mac Aging:          N/A,              Relearn Only:         N/A

    Service 200
      Service Id:         200,              Mac Move:             N/A,
      Mac Move Rate:      N/A,              Mac Move Timeout:     N/A,
      Table Size:         N/A,              Total Count:          1,
      Learned Count:      0,                Static Count:         1,
      OAM-learned Count:  N/A,              DHCP-learned Count:   N/A,
      Host-learned Count: N/A,
      Remote Age:         N/A,              Local Age:            N/A,
      Mac Learning:       N/A,              Discard Unknown:      N/A,
      Mac Aging:          N/A,              Relearn Only:         N/A


    Total Service FDBs        : 2
    Total FDB Configured Size : N/A
    Total FDB Entries In Use  : 6
```

output definitions

Service Id	The unique service identification number used to identify the service.
Total Count	The number of MAC address entries (both learned and static) in the FDB for this service.
Learned Count	The number of dynamically learned MAC address entries in the FDB for this service.
Static Count	The number of static MAC address entries in the FDB for this service.
Total Service FDBs	The total number of service FDBs.
Total FDB Entries In Use	The total number of entries (both learned and static) in use.

Release History

Release 6.4.2; command was introduced.

Related Commands

show service fdb-mac	Displays the MAC address entry information found in the forwarding database (FDB).
clear service id fdb	Clears MAC addresses (including static) from the Source Learning MAC address forwarding database for the specified service.

MIB Objects

show service fdb-mac

Displays the MAC address entry information found in the forwarding database (FDB).

show service fdb-mac [*mac-address***]**

Syntax Definitions

mac-address	A 48-bit MAC address for the static ARP (*aa:bb:cc:dd:ee:ff*). Valid addresses are any non-broadcast, non-multicast MAC, and non-IEEE reserved addresses.

Defaults

By default, all MAC address entries are displayed.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the optional *mac-address* parameter with this command to display information for a specific MAC address.
- Fields that display “N/A” are currently not supported.

Examples

```
-> show service fdb-mac 00:02:da:16:02:0c

Service Forwarding Database for 00:02:da:16:02:0c

ServId      MAC Address        Source-Identifier      Type     Last-Change
---------+------------------+---------------------+----------+--------------------
 2000       00:02:da:16:02:0c   sap:16/6:2            Learn      N/A

 No. of Entries: 1
```

output definitions

Service Id	The unique service identification number used to identify the service.
MAC Address	The MAC address entry associated with this service.
Source-Identifier	The Service Access Point (SAP) on which the address was learned or configured.
Type	The type of MAC address (**Learned**=dynamically learned address or **Static**=management configured permanent address).

Release History

Release 6.4.2; command was introduced.

Related Commands

show service fdb-info	Displays global forwarding database (FDB) information for the router.
clear service id fdb	Clears MAC addresses (including static) from the Source Learning MAC address forwarding database for the specified service.

MIB Objects

57 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 syslog-facility-id
swlog console level
swlog appid interface level
swlog remote command-log
swlog remote command-log
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 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> swlog
-> no swlog
```

Release History

Release 6.1; command introduced.

Related Commands

swlog appid interface level	Defines the level at which switch logging information will be filtered for the specified application.
swlog remote command-log	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 syslog-facility-id

Specifies a facility ID that switch logging will include in the priority (PRI) section of the event message.

swlog syslog-facility-id {*facility_id* **|** *integer***}**

Syntax Definitions

facility_id	A facility identification keyword. Current facility IDs are listed in the table below.
integer	A numerical equivalent value for the facility ID, in the range of 0–23. Current numeric equivalent values are listed in the table below.

Supported Facility IDs and their Numeric Equivalents

kernel - 0	**NTP - 12**
user - 1	**log-audit - 13**
mail - 2	**log-alert - 14**
system - 3	**clock2 - 15**
sec-auth1-4	**local0 - 16**
syslog - 5	**local1 - 17**
lptr - 6	**local2 - 18**
net-news - 7	**local3 - 19**
UUCP - 8	**local4 - 20**
clock1- 9	**local5 - 21**
sec-auth2 - 10	**local6 - 22**
FTP - 11	**local7 - 23**

Defaults

parameter	default
facility_id	**local0**
integer	**16**

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

Use the ID name (i.e., **system**) or the numeric equivalent to specify the facility ID.

Examples

```
-> swlog syslog-facility-id system
-> swlog syslog-facility-id 3
```

Release History

Release 6.3.1.R02; command introduced.

Related Commands

swlog	Enables or disables switch logging.
swlog remote command-log	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.

swlog console level

Configures the debug level for the console.

swlog console level { warning | off | info | error | debug3 | debug2 | debug1 | alert | alarm | *num* **}**

Syntax Definitions

warning	Only warning messages are logged to the console.
off	Debug messages are not logged to the console.
info	Only information level messages are logged to the console.
error	Activate only error messages logging to the console.
debug3	Activate only debug level 3 message logging to the console.
debug2	Activate debug level 2 message logging to the console.
debug1	Activate debug level 1 message logging to the console.
alert	Activate only alerts. Alerts vary based on the type and severity of the switch logging message.
alarm	Activate alarm level. Alarms vary based on the type and severity of the switch logging message.
num	A numerical equivalent value for the severity level *(see table on the following page)*. All switch logging messages of the specified level and lower are logged to the console. 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 to 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**	An 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 6400, 6850E, 6855, 9000E

Usage Guidelines

Note. When trap generation is disabled using the **trap port link** command, the event is logged in the console only when the debug level for the application is set to **debug1** or other lower severity level (**debug2** or **debug3**). When trap generation is enabled, the link up/down event is logged with a level of **info** even though debug level for application is set to **info** or other lower severity level (**debug1**, **debug2** or **debug3**).

- This command can also be used on the secondary CMM.
- Use the **show swlog** command to verify the **swlog console level** settings on the switch.

Examples

```
-> swlog console level alarm
-> swlog console level info
-> swlog console level alert
```

Release History

Release 6.4.5; command introduced.

Related Commands

trap port link	Enables or disables trap link messages for a specific slot or port. If enabled, a message is displayed on the Network Management Station (NMS) whenever the specified port changes state.
show swlog	Displays switch logging information.

MIB Objects

```
systemSwitchLoggingGroup
   systemSwitchLoggingLevel
```

swlog appid interface 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 (subsystem) or by their numeric equivalent.

swlog appid {*app_id* **|** *integer***} interface level { warning | off | info | error | debug3 | debug2 | debug1 | alert | alarm |** *num* **}**

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**

warning	Only warning messages are logged to the switch log file .**swlog** for the specified application.
off	Debug messages are not logged to the switch log file .**swlog** for the specified application.
info	Only information level messages are logged to the switch log file .**swlog** for the specified application.
error	Activate only error messages logging for the specified application.
debug3	Activate only debug level 3 logging for the specified application..
debug2	Activate debug level 2 logging for the specified application.
debug1	Activate debug level 1 logging for the specified application.

alert	Activate only alerts. Alerts vary based on the type and severity of the switch logging message.
alarm	Activate alarm level. Alarms vary based on the type and severity of the switch logging message.
num	A numerical equivalent value for the severity level *(see table on the following page)*. All switch logging messages of the specified level and lower are 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 to 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**	An 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 6400, 6850E, 6855, 9000E

Usage Guidelines

Note. When trap generation is disabled using the **trap port link** command, the event is logged in the switch log only when the debug level for the application is set to **debug1** or other lower severity level (**debug2** or **debug3**). When trap generation is enabled, the link up/down event is logged with a level of **info** even though debug level for application is set to **info** or other lower severity level (**debug1**, **debug2** or **debug3**).

- You can enter multiple application IDs in the command line. Separate each application ID with a space and no comma.
- Application IDs may be entered in any order.
- This command can also be used on the secondary CMM.
- Use the **show swlog** command to verify the **swlog appid interface level** settings on the switch.

- Use the **show log swlog** command to view the contents of the **.swlog** file with swlog messages according to the debug level settings.

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 6.1; command introduced.

Related Commands

trap port link	Enables or disables trap link messages for a specific slot or port. If enabled, a message is displayed on the Network Management Station (NMS) whenever the specified port changes state.
swlog	Enables or disables switch logging.
swlog remote command-log	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 remote command-log

Enables or disables remote command logging.

swlog remote command-log {enable | disable}

Syntax Definitions

N/A

Defaults

By default, switch logging is disabled.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> swlog remote command-log enable
-> swlog remote command-log disable
```

Release History

Release 6.3.4; command 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
   systemSwitchLoggingEnable
```

swlog output

Enables or disables switch logging output to the console, file, or data socket (remote session).

swlog output {console | flash | socket *[ip_address* **[remote command-log]***]}*

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 IPv4 or IPv6 address for the remote session host.
remote command-log	Specifies command-log output to be sent to a remote session.

Defaults

parameter	default
console | **flash** | **socket**	**flash** and **console**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to disable one or more configured output IP addresses.
- This command can also be used on the secondary CMM.
- You can send files to multiple hosts (maximum of four) using the **socket** keyword, followed by the IP address of the remote host.
- When sending the output to a syslog server, the Loopback0 address is used if configured, otherwise the VLAN's IP address is used.

Examples

```
-> swlog output console
-> no swlog output flash
-> swlog output socket 14.1.1.1
-> swlog output socket 15.1.1.1 remote command-log
```

Release History

Release 6.1; command introduced.

Related Commands

swlog	Enables or disables switch logging.
swlog appid interface 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
   systemSwitchLoggingHostUserCommandHost
   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 6400, 6850E, 6855, 9000E

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 6.1; command 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use this command when the switch logging display is too long due to some of the data being old or out of date.
- This command can also be used on the secondary CMM.

Examples

```
-> swlog clear
```

Release History

Release 6.1; command introduced.

Related Commands

swlog remote command-log	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 6400, 6850E, 6855, 9000E

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

```
-> show log swlog
Displaying file contents for '/flash/swlog2.log'
FILEID: fileName[/flash/swlog1.log], endPtr[350],
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 2012  SYSTEM       info     Switch Logging files cleared by
                                                command
MON NOV 11 13:07:26 2012  WEB          info     The HTTP session login
                                                successful!
MON NOV 11 13:18:24 2012  WEB          info     The HTTP session login
                                                succesful!
MON NOV 11 13:24:03 2012  TELNET       info     New telnet connection, Address
```

```
                                                    128.251.30.88
MON NOV 11 13:24:03 2012  TELNET       info     Session 4, Created
MON NOV 11 13:59:04 2012   WEB         info      The HTTP session user logout
                                                 successful!

-> show log swlog

Displaying file contents for '/flash/swlog2.log'
FILEID: fileName[/flash/swlog2.log], endPtr[60],  configSize[64000], mode[2]
Displaying file contents for '/flash/swlog1.log'
FILEID: fileName[/flash/swlog1.log], endPtr[350],  configSize[64000], mode[1]

Time Stamp               Application Level   Log Message

-------------------------+-----------+------+------------------------------

WED SEP 21 14:52:09 2011 SYSTEM       info Switch Logging cleared by command.
                                           File Size=128000 bytes

WED SEP 21 14:53:23 2011 STP          info Topology changed on VLAN/STP id 1

WED SEP 21 14:53:43 2011 INTERFACE   debug1  2/3: link DOWN

WED SEP 21 14:54:10 2011 INTERFACE   debug1  2/3: link UP

WED SEP 21 14:54:13 2011 STP          info Topology changed on VLAN/STP id 1
```

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 6.1; command introduced.

Related Commands

swlog	Enables or disables switch logging.
swlog appid interface level	Adds or removes a filter level for a specified subsystem.
swlog remote command-log	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 6400, 6850E, 6855, 9000E

Usage Guidelines

This command can also be used on the secondary CMM.

Examples

```
-> show swlog
Operational Status                    : On,
Log Device 1                          : flash,
Log Device 2                          : ipaddr 192.21.161.105,
Log Device 3                          : console,
Syslog FacilityID                     : local0(16),
Remote command-log                    : Disabled,
Console Display Level                 : debug3 (9),
All Applications Not Shown Level          : info (6)

Application ID       Level
--------------------+----------------
INTERFACE      (  6)     debug1 (7)
```

output definitions

Operational Status	The operational status of switch logging.
Log Device	The device where the output is being logged.
Syslog FacilityID	The facility ID that switch logging will include in the priority (PRI) section of the event message.
Remote command-log	The status of the remote command-log feature.

output definitions

Console Display Level	The Consol Display Level. Levels include alarm (2), error (3), alert (4), warning (5), info (6), debug1 (7), debug2 (8), and debug3 (9).
All Applications Not Shown Level	The Severity Level of the Application ID. Levels include alarm (2), error (3), alert (4), warning (5), info (6), debug1 (7), debug2 (8), and debug3 (9).

Release History

Release 6.1; command introduced.

Related Commands

swlog	Enables or disables switch logging.
swlog appid interface level	Defines the level at which switch logging information will be filtered for the specified application.
swlog remote command-log	Enables or disables switch logging output to the console, file, or data socket.
show log swlog	Displays stored switch logging information from flash.

58 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
show health fabric

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, and 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- When a resource falls back below the configured threshold, an additional 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 58-6, or refer to the “Diagnosing Switch Problems” chapter in the *OmniSwitch AOS Release 6 Network Configuration Guide*.
- To view the current health threshold values, use the **show health threshold** command. Do not use the **show temperature** command as it does not display health threshold statistics. These two **show** commands are unrelated.

Examples

```
-> health threshold rx 85
-> health threshold txrx 55
-> health threshold memory 95
-> health threshold cpu 85
-> health threshold temperature 40
```

Release History

Release 6.1; command was introduced.

Related Commands

show health threshold	Displays the 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 6400, 6850E, 6855, 9000E

Usage Guidelines

Decreasing the polling interval may impact switch performance.

Examples

```
-> health interval 6
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 the 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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; command was introduced.

Related Commands

health interval	Configures the interval between health statistics checks.

MIB Objects

```
HealthThreshInfo
   healthSamplingInterval
```

show health

Displays the 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 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- If no slot/port information is specified, the 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

-> 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.
Limit	Currently configured device threshold levels (percentage of total available bandwidth).
Curr	Current device bandwidth usage.
1 Min Avg	Average device bandwidth usage over a 1-minute period.
1 Hr Avg	Average device bandwidth usage over a 1-hour period.
1 Hr Max	Maximum device bandwidth usage over a 1-hour period (i.e., the maximum of the 1 minute averages).

Release History

Release 6.1; 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 the RAM memory health statistics for all active NI modules in the switch.
cpu	Displays the CPU health statistics for all active NI modules.
rx	Displays the health statistics for traffic *received* on all active NI modules.
txrx	Displays the health statistics for traffic both *transmitted and received* on all active NI modules.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 6.1; command was introduced.

Related Commands

show health	Displays the 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 the 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 6400, 6850E, 6855, 9000E

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 6.1; command was introduced.

Related Commands

N/A

MIB Objects

```
healthSliceTable
   healthSliceSlot
   healthSliceSlice
   healthSliceMemoryLatest
   healthSliceCpuLatest
```

show health fabric

Displays the health statistics of a fabric for a particular slot or a range of slots.

show health fabric *slot 1[-slot2]*

Syntax Definitions

slot	A specific physical slot number for which fabric statistics are to be displayed (e.g., 3).
slot2	Last fabric slot number in a range of slots you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 9000E

Usage Guidelines

N/A

Examples

```
-> show health fabric 3
* - current value exceeds threshold

Slot  03                          1 Min  1 Hr  1 Hr
Fabric              Limit   Curr   Avg    Avg   Max
-----------------+-------+------+------+-----+----
Receive
    Primary          80     00     00    00    00
    Secondary        80     00     00    00    00
Transmit/Receive
    Primary          80     00     00    00    00
    Secondary        80     00     00    00    00
```

output definitions

Slot	The physical slot number for the corresponding fabric.
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.

output definitions (continued)

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 6.1; command was introduced.

Related Commands

N/A

MIB Objects

```
healthFabricTable
   healthFabricSlot
   healthFabricPrimaryRxLatest
   healthFabricPrimaryRx1MinAvg
   healthFabricPrimaryRx1HrAvg
   healthFabricPrimaryRx1HrMax
   healthFabricPrimaryRxTxLatest
   healthFabricPrimaryRxTx1MinAvg
   healthFabricPrimaryRxTx1HrAvg
   healthFabricPrimaryRxTx1HrMax
   healthFabricSecondaryRxLatest
   healthFabricSecondaryRx1MinAvg
   healthFabricSecondaryRx1HrAvg
   healthFabricSecondaryRx1HrMax
   healthFabricSecondaryRxTxLatest
   healthFabricSecondaryRxTx1MinAvg
   healthFabricSecondaryRxTx1HrAvg
   healthFabricSecondaryRxTx1HrMax
```

59 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

Filename: AlcatelIND1ConfigMgr.mib
Module: ALCATEL-IND1-CONFIG-MGR-MIB DEFINITIONS

Filename: AlcatelIND1System_mib
Module: ALCATEL-IND1-SYSTEM-MIB

A summary of available commands is listed here:

reload
reload working
reload issu
write memory
write memory flash-synchro
copy working certified
copy flash-synchro
takeover
show running-directory
show reload
show microcode
show microcode history
show microcode issu
usb
usb auto-copy
usb disaster-recovery
mount
umount
show usb statistics

reload

Reboots the CMM to its startup software configuration.

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

reload [primary | secondary] [with-fabric] 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.
with-fabric	Performs a complete CMM reload. This parameter is available only on OmniSwitch chassis-based series switches.
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 issued. 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- This command causes the specified CMM to reboot. If no CMM is specified, the primary CMM reboots.
- The CPM, CFM and CPU of CMM can be reset independently.
- If a reload command is issued and the local/remote fabric module is in up state, only the CPM will be reset.
- If a reload command is issued and the local/remote fabric module is in a down state, then the complete CMM will be reloaded.

- 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 AOS Release 6 Switch Management Guide*.
- If the switch is part of a 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 the appropriate *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 with-fabric
-> reload primary in 15:25
-> reload primary at 15:25 august 10
-> reload primary at 15:25 10 august
```

Release History

Release 6.1; 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. The switch immediately reboots from the working directory and then at the end of this time period, automatically reboots again 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 issued. 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 6400, 6850E, 6855, 9000E

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 overridden.
- 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 a 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 6.1; command was introduced.

Related Commands

reload	Reboots the CMM to its startup software configuration.

MIB Objects

```
chasControlModuleTable
   csEntPhysicalIndex
   chasControlActivateTimeout
```

reload issu

Upgrades the system with the images stored in the /flash/issu directory with minimal disruption to the data traffic.

reload issu [in [*hours:***] *minutes* | **at** *hour:minute***]**

Syntax Definitions

in [*hours:***] *minutes*	Optional syntax. Schedules a reload of the primary CMM 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 primary CMM to take place at the specified time using a 24-hour clock.

Defaults

By default, the switch starts copying the image files to the working directory of the primary CMM immediately after issuing the command if no time delay is specified.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- The switch must be running an In-Service Software Upgrade (ISSU) capable build, which is only those builds that are part of the 'S##' branch (for example, 6.4.1.###.S01).
- The primary and secondary CMMs should be fully synchronized, certified, redundant, and running an ISSU capable 'S##' build, such as 6.4.1.123.S01, to invoke the ISSU feature.
- Before using this command, create an ISSU directory on the switch flash (for example, /flash/issu), then download the "S###" image files into this directory.
- Image files used for the upgrade must be within the same 'S##' branch to pefrom an ISSU upgrade. For example, 6.4.1.###.**S02** image files cannot be used to upgrade a switch running 6.4.1.###/.**S01**.
- There are four image files that are ISSU capable: **Jbase.img**, **Jsecu.img**, **Jadvrout.img** and **Jos.img**.
- Admin user privileges are required to invoke the ISSU feature.
- A minimum of 25MB flash space is required on the switch to accomodate all the image files needed for the upgrade.
- Once the images are upgraded, use the **copy working certified flash-synchro** command to restore redundancy between the Primary and Secondary CMM.

Examples

```
-> reload issu
-> reload issu in 45
-> reload issu at 09:25
```

Release History

Release 6.4.1; command was introduced

Related Commands

reload	Reboots the CMM to its startup software configuration
reload working	Immediate primary CMM reboot to the working software configuration without secondary CMM takeover.
show microcode issu	Displays the microcode version information of the images in the ISSU directory.

MIB Objects

```
chasControlModuleTable
   chasControlVersionMngt
   chasGlobalcontrolDelayedActivatetimer
```

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 6400, 6850E, 6855, 9000E

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 **write memory** commands, in an OmniSwitch set up with redundant CMMs.

Examples

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

Release History

Release 6.1; command was introduced.

Related Commands

write memory	Copies the running primary RAM version of the CMM software to the working primary flash.
copy flash-synchro	Copies 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 6400, 6850E, 6855, 9000E

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.

Note. On an OmniSwitch set up with redundant CMMs, the saved **boot.cfg** file will be overwritten if the **takeover** command is executed after the **write memory** command.

Examples

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

Release History

Release 6.1; command was introduced.

Related Commands

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

MIB Objects

```
configManager
   configWriteMemory
```

write memory flash-synchro

Copies the running configuration (RAM) to the working directory, certifies the primary CMM and synchronizes the primary and secondary CMM.

[configure] write memory flash-synchro

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- This command is a combination of the ‘write memory’ and ‘copy working certified flash-synchro’ commands and does the following:

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

2 Overwrites the contents of the certified directory on the primary CMM with the contents of the working directory on the primary CMM.

3 Synchronizes the primary and secondary CMMs.

- 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.

Examples

```
-> write memory flash-synchro
```

Release History

Release 6.3.4; command was introduced.

Related Commands

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

MIB Objects

```
configManager
   configWriteMemory
```

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 6400, 6850E, 6855, 9000E

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 a 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 6.1; command was introduced.

Related Commands

copy working certified	Copies 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	Copies 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 6400, 6850E, 6855, 9000E

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 a stack, all switches in the stack are updated with the primary CMM files.

Examples

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

Release History

Release 6.1; command was introduced.

Related Commands

copy working certified	Copies the working primary flash version of the CMM software to certified primary flash. Or copies 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 [with-fabric]

Syntax Definitions

with-fabric	Performs a complete CMM reload.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 is 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.
- The CPM, CFM and CPU of CMM can be reset independently.
- If a takeover command is issued and the local/remote fabric module is in up state, only the CPM will be reset.
- If a takeover command is issued and the local/remote fabric module is in a down state, then the complete CMM will be reloaded.
- This command can also be used on the secondary CMM.
- If the switch is part of a 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 *Hardware Users Guide*.

Note. The saved **boot.cfg** file will be overwritten if the **takeover** command is executed after the **write memory** command on an OmniSwitch set up with redundant CMMs. Refer to the “NIs Reload On Take-over” description on page 59-19 for more information on the **takeover** command and redundant management modules.

Examples

```
-> takeover
-> takeover with-fabric
```

Release History

Release 6.1; command was introduced.

Related Command

reload	Reboots the CMM to its startup software configuration.

MIB Objects

```
chasEntPhysicalTable
   csEntPhysicalIndex
   chasEntPhysAdminStatus
```

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 6400, 6850E, 6855, 9000E

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 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.

output definitions (continued)

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).
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 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- It is possible to preset a reboot on a CMM by 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, and 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 6.1; 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.

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 6400, 6850E, 6855, 9000E

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
-----------------+--------------+--------+---------------------------------
Jbase.img         6.1.1.403.R01   10520989 Alcatel-Lucent Base Software
Jos.img           6.1.1.403.R01    1828255 Alcatel-Lucent OS
Jadvrout.img      6.1.1.403.R01    1359435 Alcatel-Lucent Advanced Routing
```

output definitions

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

Release History

Release 6.1; command was introduced.

Related Commands

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

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 6400, 6850E, 6855, 9000E

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 8/27/05 23:45:00
```

Release History

Release 6.1; command was introduced.

Related Commands

show microcode	Displays microcode versions installed on the switch.

show microcode issu

Displays the microcode version information of the images in the ISSU directory of the flash memory.

show microcode issu

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

N/A

Examples

```
-> show microcode issu
   Package           Release       Size     Description
-----------------+---------------+--------+----------------------------------
jos.img           6.4.1.733.S01    1854193 Alcatel-Lucent OS
jsecu.img         6.4.1.733.S01     472002 Alcatel-Lucent Security
jadvrout.img      6.4.1.733.S01    2649893 Alcatel-Lucent Advanced Routing
jbase.img         6.4.1.733.S01   14195061 Alcatel-Lucent Base Software
```

output definitions

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

Release History

Release 6.4.1; command was introduced.

Related Commands

reload issu	Upgrades the working directory of the primary CMM with minimal disruption to the data traffic.
show microcode	Displays microcode versions installed on the switch.
show microcode history	Displays the archive history for microcode versions installed on the switch.

MIB Objects

```
systemMicrocodeTable
   systemMicrocodeEntry
```

usb

Enables access to the device connected to the USB port.

usb {enable | disable}

Syntax Definitions

N/A

Defaults

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

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Must use an Alcatel-Lucent certified USB device.
- If a Alcatel-Lucent certified USB device is connected after enabling the USB interface, the device will be automatically mounted as **/uflash**.
- Once mounted, common file and directory commands can be used for file managment.

Examples

```
-> usb enable
-> cp /flash/working/boot.cfg /uflash/boot.cfg
-> ls /uflash
```

Release History

Release 6.4.3; command was introduced.

Related Commands

MIB Objects

usb auto-copy	Allows backup image files from the USB device to be automatically copied to the /flash/working directory on the switch immediately after the USB device is connected

```
systemServices
   systemServicesUsbEnable
```

usb auto-copy

Upgrades the image files from the USB device to the */flash/working* directory on the switch immediately after the USB device is connected.

usb auto-copy {enable | disable}

Syntax Definitions

N/A

Defaults

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

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The USB device must contain the proper file structure and image files mentioned below and the USB root directory must contain a signature file named *aossignature*. The *aossignature* file can be a blank text file transferred to the switch.
- This operation will enable all of the image files from the */uflash/6850/working, /uflash/6855/working, /uflash/6400/working* or */uflash/9000E/working* directory, based upon the platform performing the operation, to be copied to the */flash/working* directory and then reboot the switch.
- If the auto-copy is successful, the auto-copy feature will be disabled before rebooting the switch and must be re-enabled by the administrator for the next auto-copy process to execute. This will prevent running the same auto-copy multiple times.

Examples

```
-> usb auto-copy enable
-> usb auto-copy disable
```

Release History

Release 6.4.3; command was introduced.

Related Commands

usb	Enables access to the device connected to the USB interface.

MIB Objects

```
systemServices
   systemServicesUsbAutoCopyEnable
```

usb disaster-recovery

Enables the disaster-recovery access to the USB device connected to the USB port when the switch is unable to boot properly.

usb disaster-recovery {enable | disable}

Syntax Definitions

N/A

Defaults

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

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The USB device must contain the proper file structure and image files mentioned below.
- If miniboot is unable to load AOS from the os.img file then the disaster-recovery operation will begin. The disaster recovery operation will format the switch flash, copy all of the files from the */uflash/6850/certified*, */uflash/6855/certified*, */uflash/6400/certified*, or */uflash/9000E/certified* directory, based upon the platform performing the operation, to the */flash/certified* directory and reboot the switch.
- Disaster recovery should be run on a standalone unit so that it does not affect any other units in a stack.
- A minimum 6.4.3 version of uboot/miniboot is required.

Examples

```
-> usb disaster-recovery enable
-> usb disaster-recovery disable
```

Release History

Release 6.4.3; command was introduced.

Related Commands

usb	Enables access to the device connected to the USB interface.

MIB Objects

```
systemServices
   systemServicesUsbDisasterRecoveryEnable
```

mount

Mounts a USB device on /uflash.

mount [/uflash]

Syntax Definitions

/uflash	The name of the file-system to mount.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Once the USB device is mounted most file and directory commands associated with the /flash file system can be used with **/uflash** such as: **mkdir**, **rmdir**, **cd**, **rm**, **cp**, **ls**.

Examples

```
-> mount /uflash
-> ls /uflash
```

Release History

Release 6.4.3; command was introduced.

Related Commands

umount	Unmounts the /uflash file system from AOS.

MIB Objects

```
systemServicesAction
   systemServicesArg1
```

umount

Unmounts the /uflash file system from AOS.

umount /uflash

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

This command unmounts the USB drive and should be used prior to unplugging the USB drive to prevent possible data corruption.

Examples

```
-> umount /uflash
```

Release History

Release 6.4.3; command was introduced.

Related Commands

mount	Mounts the /uflash file system from AOS.

MIB Objects

```
systemServicesAction
   systemServicesArg1
```

show usb statistics

Displays the status USB setting and features.

show usb statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show usb statistics
USB:                   Disabled
USB auto-copy:         Enabled
USB disaster-recovery: Disabled
/uflash is not mounted
```

output definitions

USB	Status of USB device interface.
USB auto-copy	Status of USB auto-copy feature.
USB disaster-recovery	Status of USB auto-copy feature.
/uflash	Whether the USB device is mounted or unmounted.

Release History

Release 6.4.3; command was introduced.

Related Commands

usb	Enables access to the device connected to the USB interface.
usb auto-copy	Allows backup files from the USB device to be automatically copied to the /flash/working directory on the switch immediately after the USB device is connected.
usb disaster-recovery	Enables the disaster-recovery access to the USB device connected to the interface.

MIB Objects

```
systemServices
   systemServicesUsbEnable
   systemServicesUsbAutoCopyEnable
   systemServicesUsbDisasterRecoveryEnable
```

show issu status

This command will display the status of ISSU, the slot number of units that have been upgraded by ISSU, the unit for which upgrade is in progress and the failure reason if ISSU fails.

show usb statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

N/A

Examples

```
cli> show issu status
ISSU STATUS
  Status                       : None,
  Slots Upgraded               : None,
  Slot Upgradation In Progress : None,
  Slots to be Upgraded         : 1 2 3 4 5 6 7,
  Failure Reason               : None

cli> show issu status
ISSU STATUS
  Status                       : In Progress,
  Slots Upgraded               : None,
  Slot Upgradation In Progress : 1,
  Slots to be Upgraded         : 2 3 4,
  Failure Reason               : None

cli> show issu status
ISSU STATUS
  Status                       : Aborted,
  Slots Upgraded               : None,
  Slot Upgradation In Progress : 1,
  Slots to be Upgraded         : 2 3 4,
  Failure Reason               : NI Up Not Received for slot 5

cli> show issu status
ISSU STATUS
  Status                       : Successful,
  Slots Upgraded               : 1 2 3 4 5 6 7,
  Slot Upgradation In Progress : None,
```

```
Slots to be Upgraded          : None,
Failure Reason                : None
```

output definitions

Status	Status of the ISSU upgrade
Slot Upgraded	Which slots have already been upgraded.
Slot Upgradation In Progress	Which slot is currently being upgraded.
Slots to be Upgraded	Which slots still need to be upgraded for ISSU to complete.
Failure Reason	Why the ISSU upgrade failed.

Release History

Release 6.4.5; command was introduced.

Related Commands

reload issu	Performs an ISSU upgrade.
show issu signature	Displays the signature value of the images.

MIB Objects

```
alcatelIND1ChassisMIBObjects
     alaChasIssuForStackablesStatus
     alaChasIssuForStackablesSlotsUpgraded
     alaChasIssuForStackablesSlotInProgress
     alaChasIssuForStackablesSlotsLeft
```

show issu signature

This command will display the signature value for the working, certified and issu directories.

show usb statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

This command should be run before performing an ISSU upgrade to confirm the compatibility between the ISSU images and the current images. The values should be the same.

Examples

```
cli> show microcode signature
SIGNATURE
  Certified : 37b4ec326781e85fddb90faf337ece1c,
  Working   : 37b4ec326781e85fddb90faf337ece1c,
  Issu      : 37b4ec326781e85fddb90faf337ece1c

cli> show microcode signature
SIGNATURE
  Certified : 37b4ec326781e85fddb90faf337ece1a,
  Working   : 37b4ec326781e85fddb90faf337ece1a,
  Issu      : 37b4ec326781e85fddb90faf337ece1c
```

output definitions

Certified	The signature value of the images in the Certified directory.
Working	The signature value of the images in the Certified directory.
Issu	The signature value of the images in the Certified directory.

Release History

Release 6.4.5; command was introduced.

Related Commands

reload issu	Performs an ISSU upgrade.
show issu status	Displays the status of an ISSU upgrade.

MIB Objects

```
systemSignature
  systemSignatureCertified
  systemSignatureWorking
  systemSignatureIssu
```

60 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 Users 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

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** **update** **update lanpower** **reload ni** **reload all** **reload pass-through** **power ni** **temp-threshold** **stack set slot** **stack clear slot** **hash-control**
Monitoring Commands	**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 stack status** **show hash-control**
Licensing Commands	**license apply** **show license info** **show license file**
OS-BPS Commands	**power slot bps connector-priority** **power bps mode** **update bps firmware** **show power bps connector-priority** **show power supply bps**

system contact

Specifies the switch 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 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

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

Release History

Release 6.1; command was introduced.

Related Commands

system name	Modifies the switch current system name.
system location	Specifies the switch current physical location.
show system	Displays the basic system information for the switch.

MIB Objects

```
system
   systemContact
```

system name

Modifies the switch 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 6250"**.

Defaults

By default, the system name is set to 'VxTarget'.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

The OmniSwitch can be configured with a DHCP Client interface that allows the switch to obtain the system name (DHCP Option-12) from a DHCP server dynamically. The user-defined system name configuration (through CLI, WebView, SNMP) always gets priority over the DHCP server values.

For more information on DHCP client options, refer to the "Configuring DHCP" chapter of the *OmniSwitch AOS Release 6 Network Configuration Guide*

Examples

```
-> system name OmniSwitch6855
-> system name OS-6855
```

Release History

Release 6.1; command was introduced.

Related Commands

system contact	Specifies the switch administrative contact (for example, an individual or a department).
system location	Specifies the switch current physical location.
show system	Displays the basic system information for the switch.

MIB Objects

```
system
   systemName
```

system location

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

system location *text_string*

Syntax Definitions

text_string	The switch 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 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

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

Release History

Release 6.1; command was introduced.

Related Commands

system contact	Specifies the switch administrative contact (for example, an individual or a department).
system name	Modifies the switch current system name.
show system	Displays the basic system information for the switch.

MIB Objects

```
system
   systemLocation
```

system date

Displays or modifies the switch 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, **08/08/2005**.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 (for example, Daylight Savings Time), refer to the **system timezone** command on page 60-9.

Examples

```
-> system date 08/08/2005
-> system date
08/08/2005
```

Release History

Release 6.1; command was introduced.

Related Commands

system time	Displays or modifies the switch 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 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 6400, 6850E, 6855, 9000E

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 6.1; command was introduced.

Related Commands

system date	Displays or modifies the switch 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 6400, 6850E, 6855, 9000E

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 OmniSwitch chassis-based switches refer to the “Chassis Management Module (CMM)” chapter in the *Hardware Users Guide* and “Managing CMM Directory Content” in the *OmniSwitch AOS Release 6 Switch Management Guide*. For stackable switches, refer to “Managing Stacks” in addition to “Managing CMM Directory Content”.

Examples

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

Release History

Release 6.1; 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 (for example, 05:30).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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	2nd Sunday in Mar. at 2:00 a.m.	1st Sunday in Nov. 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 6.1; command was introduced.

Related Commands

system date	Displays or modifies the switch current system date.
system time	Displays or modifies the switch 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- If your timezone shows a default value in the DST Start and DST End columns of the “Time Zone and DST Information Table” found in Chapter 2, “Managing System Files,” of the *OmniSwitch AOS Release 6 Switch Management Guide*, 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.
- Setting the start and end date and time for DST is only supported when a custom timezone is configured.

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 6.1; command was introduced.

Related Commands

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

MIB Objects

```
systemServices
   systemServicesTimezone
   systemServicesEnableDST
```

update

Updates the versions of Uboot, FPGA, BootROM, or Miniboot. Refer to the Release Notes and/or any available Upgrade Instructions for the new release before performing this type of update on the switch.

update {uboot {cmm | ni {all | *slot*}} uboot-miniboot | fpga cmm | bootrom {all | *slot*} | [default | backup] miniboot [all | *slot*] }

Syntax Definitions

uboot	Updates the uboot version.
cmm	Specifies that the update is performed for the Chassis Management Module (CMM)**.**
ni	Specifies that the update is performed for the Network Interface (NI) Module**.**
all	Specifies that the update is performed for all slots within a chassis or all switches within a stack.
slot	Specifies the number of the NI module within a chassis or the switch number within a stack for which the update is performed.
uboot-miniboot	Updates the uboot *and* the miniboot version on all available slots within a chassis or on all available switches within a stack.
fpga	Updates the FPGA version.
miniboot	Updates the miniboot version.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- On OmniSwitch chassis-based switches, the *slot* parameter is not allowed with the **cmm** parameter.
- Note that when performing an update, it is important that the correct update file is used and that the file is located in the **/flash** directory on the switch. Specifying the wrong file may impact the operation of the switch.
- A different update file is required depending on the type of switch and the type of update. The following table provides a list of the required update files:

OmniSwitch	Update Type	Update File
6400	Uboot	kuboot.bin
	Miniboot	gminiboot.uboot

OmniSwitch	Update Type	Update File
	Uboot and Miniboot	kuboot.bin gminiboot.uboot
	FPGA	Gfpga.upgrade_kit
6855	Uboot	kuboot.bin
	Miniboot	k2Iminiboot.uboot
	Uboot and Miniboot	kuboot.bin k2Iminiboot.uboot
	FPGA	K2Ifpga.upgrade_kit
9000E	Uboot	uboot.bin
	Uboot and Miniboot	uboot.bin miniboot.uboot
	FPGA	Jfpga.upgrade_kit
	Miniboot	miniboot.uboot

Examples

```
OS6855-> update uboot 1
OS6855-> update uboot-miniboot
OS6855-> update miniboot all

OS6400-> update uboot 2
OS6400-> update uboot-miniboot
OS6400-> update fpga cmm
OS6400-> update miniboot 3
```

Release History

Release 6.1.1; command was introduced.
Release 6.1.2; *slot* and **bootrom** parameters were added.
Release 6.1.3; **uboot-miniboot** parameter added.

Related Commands

reload all	Reloads all the NIs and CMMs in a chassis.

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesAction
```

update lanpower

Uploads new firmware to the POE controller. Please contact your Alcatel-Lucent support representative before using this command.

update lanpower {*lanpower_num* **| all}**

Syntax Definitions

lanpower_num	The POE unit number to update.
all	Updates all POE units in the switch.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

N/A

Examples

```
-> update lanpower 3
-> update lanpower all
```

Release History

Release 6.1.3; command was introduced.

Related Commands

update	Updates the versions of Uboot, FPGA, BootROM, or Miniboot.

reload ni

Reloads (that is, reboots) a specified Network Interface (NI) module.

reload ni [slot] *number*

Syntax Definitions

slot	Optional command syntax.
number	Slot (that is, switch) number within a stack that represents the NI module to be reloaded.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- On OmniSwitch chassis based switches, 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 stackable series 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 a stack consisting of three or more switches.

Examples

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

Release History

Release 6.1; command was introduced.

Related Commands

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

MIB Objects

```
chasEntPhysicalTable
   chasEntPhysAdminStatus
   reset
```

reload all

Reloads (that is, reboots) all the Network Interfaces (NIs) and Chassis Management Module (CMMs) in an OmniSwitch chassis, a standalone switch, or all the switches in an OmniSwitch 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 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> reload all
```

Release History

Release 6.1; 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 the hardware information and current status for Network Interface (NI) modules currently running in the chassis.

MIB Objects

```
chasEntPhysicalTable
   chasEntPhysAdminStatus
   reset
```

reload pass-through

Reloads (that is, reboots) a switch in a stackable configuration which has been forced into the pass-through mode. The pass-through mode is a state in which a switch has been assigned a slot number that is not available in the current stacked configuration. When a switch is in the pass-through mode, its Ethernet ports are brought down (that is, they cannot pass traffic). However, its stacking ports are fully functional and can pass traffic through to other switches in the stack; in this way, pass-through mode provides a mechanism to prevent the stack ring from being broken.

Note. If a switch is forced into the pass-through mode, the rest of the virtual chassis (that is, stack) will not be disrupted. Any elements in the stack *not* operating in pass-through mode continue to operate normally.

reload pass-through *slot-number*

Syntax Definitions

slot-number	The virtual chassis slot number of the switch currently in the pass-through mode (1001–1008). For more information on pass-through slot numbering, refer to the "Usage Guidelines" section below.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- Switches in the pass-through mode are given distinct slot numbers. These slot numbers are *not* related to their position in the stack. Instead, they are assigned the prefix "100," followed by the numerical order in which they were forced into pass-through. In other words, if only one switch in a stack is forced into the pass-through mode, it is given the slot number 1001. If multiple switches in a stack are forced into pass-through, the first switch in pass-through is given the slot number 1001, the second switch is given the slot number 1002, the third switch is given the slot number 1003, etc.
- Before issuing the **reload pass-through** command, be sure that the corresponding switch has been given a unique *saved slot* number. The saved slot number is the slot number the switch will assume after it has been rebooted. If the saved slot number is not unique, the switch will simply return to pass-through mode. To view the current and saved slot numbers for all switches in a stack, use the **show stack topology** command. To assign a unique saved slot number to a switch before rebooting, use the **stack set slot** command.

Examples

```
-> reload pass-through 1001
```

Release History

Release 6.1; command was introduced.

Related Commands

show stack topology	Displays the current operating topology of switches within a stack.
stack set slot	Assigns a new saved slot number to a switch in a stacked configuration.

MIB Objects

```
alaStackMgrChassisTable
   alaStackMgrSlotNINumber
   alaStackMgrCommandAction
   reloadPassThru
```

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.

Defaults

N/A

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use the **no** form of this command to power off an NI module.
- This command is not supported on OmniSwitch stackable switches.

Examples

```
-> no power ni 1
-> power ni 1
```

Release History

Release 6.1; command was introduced.

Related Commands

reload ni	Reloads (that is, reboots) a specified Network Interface (NI) module.
show ni	Shows the 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 warning temperature threshold for the switch.

temp-threshold *temp* **slot** *slot-number*

Syntax Definitions

temp	The new temperature threshold value, in Celsius.
slot-number	The chassis slot number for which the warning temperature threshold is set. *This parameter is supported only on stackable switches.*

Defaults

Refer to the appropriate *Hardware Users Guide* for platform specific temperature values.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **show temperature** command to display the current value for the temerpature warning threshold.
- Do not use the **show health threshold** command as it does not display temperature threshold information.

Examples

```
-> temp-threshold 45
-> temp-threshold 55 slot 2
```

Release History

Release 6.1; command was introduced.
Release 6.1.5; **slot** parameter added.

Related Commands

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

MIB Objects

```
chasChassisTable
   chasTempThreshold
```

stack set slot

Sets the *saved slot* number or mode for stackable configuration switches. The saved slot number is the slot position the switch will assume following a reboot. The **stack set slot** command also provides syntax for immediately rebooting the corresponding switch.

stack set slot *slot-number* **{saved-mode {OS6850E|OS6850} | saved-slot** *slot-number* **[reload]}**

Syntax Definitions

slot-number	The current slot position used by the switch (1–8; 1001–1008). Note that the valid slot number range also includes slot positions 1001 through 1008, reserved for switches in pass-through mode.
OS6850E | **OS6850**	The stacking mode of the OS6850E.
saved-slot-number	The new (that is, saved) slot number (1–8). The saved slot number is the slot position the switch will assume following a reboot.
reload	Optional command syntax. When **reload** is entered in the command line, a confirmation prompt is issued. If the user approves the reload, the corresponding switch will be rebooted immediately and the new (that is, saved) slot number will take effect when the switch comes back up—barring any pass-though mode conditions, such as duplicate slot numbers. This parameter is not supported when changing the mode.

Defaults

parameter	default
saved-mode (Only supported on OS6850E Models)	6850

Platforms Supported

OmniSwitch 6850E, 6855

Usage Guidelines

- When the **stack set slot** command is issued, the new saved slot value is written to the **boot.slot.cfg** file. This file is located in the switch /flash directory and is used when assigning a slot number for the switch during the boot process.
- In order to avoid duplicate slot numbers within the virtual chassis—which can force one or more switches into pass-though mode—be sure that the saved slot number being configured is not already being used by another switch in the stack. To view the saved slot numbers currently assigned, use the **show stack topology** command. For detailed information on assigning saved slot numbers, as well as information on pass-through mode, refer to the *Hardware Users Guide*.
- Changing the mode is only supported on OS6850E models. OS6850 mode is applicable only for 6.4.4.

Examples

```
-> stack set slot 2 saved-slot 3
```

```
-> stack set slot 1001 saved-slot 4 reload
-> stack set slot 1 saved-mode 6850E
```

Release History

Release 6.1; command was introduced.
Release 6.4.4; **saved-mode** parameter was added.

Related Commands

stack clear slot	Clears the current saved slot information for a switch within a stackable switch configuration.
show stack topology	Displays the current operating topology of switches within a stack.

MIB Objects

```
alaStackMgrChassisTable
   alaStackMgrSlotNINumber
   alaStackMgrSavedSlotNINumber
   alaStackMgrCommandAction
   alaStackMgrCommandStatus
```

stack clear slot

Clears the current saved slot information for a switch within a stacked configuration. When the saved slot information has been cleared via the **stack clear slot** command, the corresponding switch will automatically be assigned a unique slot number following a reboot.

stack clear slot *slot-number*

Syntax Definitions

slot-number	The current slot position used by the switch (1–8; 1001–1008). Note that the valid slot number range also includes slot positions 1001 through 1008, reserved for switches in pass-through mode.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

- When the **stack clear slot** command is issued, the **boot.slot.cfg** file is immediately removed from the switch /flash directory. As a result, no slot assignment information will be found the next time the switch is booted. Because the switch slot will be considered *undefined* during the boot process, the switch is automatically assigned a unique slot number.
- Primary and secondary management modules *cannot* be forced into pass-through mode using the **stack clear slot** command. If the user attempts to force the secondary management module into pass-through, the secondary switch will reboot and assume idle status when it comes back up. Meanwhile, an idle switch within the stack is selected and rebooted; when it comes up it assumes the secondary role.

Examples

```
-> stack clear slot 1002
-> stack clear slot 3
```

Release History

Release 6.1; command was introduced.

Related Commands

stack set slot	Sets the saved slot number for switches in a stacked configuration.
show stack topology	Displays the current operating topology of switches within a stack.

MIB Objects

```
alaStackMgrChassisTable
   alaStackMgrSlotNINumber
   alaStackMgrSavedSlotNINumber
   alaStackMgrCommandAction
   alaStackMgrCommandStatus
```

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 6400, 6850E, 6855, 9000E

Usage Guidelines

This command may be used when logged into the switch that performs either the primary or secondary CMM role in a stack.

Examples

```
-> show system
System:
  Description: Alcatel-Lucent OS6400-CMM 6.4.5.63.R02 Oct 21, 2012.,
  Object ID:    1.3.6.1.4.1.6486.800.1.1.2.1.6.1.2,
  Up Time:      0 days 5 hours 20 minutes and 49 seconds,
  Contact:      Alcatel-Lucent, www.alcatel-lucent.com/enterprise/en,
  Name:         OmniSwitch 6400E,
  Location:     NMS_LABORATORY,
  Services:     72,
  Date & Time:  THU JUN 2 2010 16:21:30 (PST)

Flash Space:
    Primary CMM:
      Available (bytes):  31266816,
      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.

output definitions (continued)

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 *primary* management module.
Flash Space: Primary CMM: Comments	Comments regarding the available flash memory space available on the switch primary management module, if applicable.

Release History

Release 6.1; command was introduced.

Related Commands

system contact	Specifies the switch administrative contact (for example, an individual or a department).
system name	Modifies the switch current system name.
system location	Specifies the switch current physical location.

MIB Objects

```
system
   systemContact
   systemName
   systemLocation
```

show hardware info

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

show hardware info

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

This command may be used when logged into the switch that performs either as the primary or secondary CMM role in a stack.

Examples

```
-> show hardware info
CPU Type                          : PowerPC 8245,
Flash Manufacturer                : TOSHIBA,
Flash size                        : 67108864 bytes (64 MB),
RAM Manufacturer                  : (null),
RAM size                          : 268435456 bytes (256 MB),
NVRAM Battery OK ?                : YES,
BootROM Version                   : 6.1.2.20.R02 ,
Backup Miniboot Version           : 6.1.2.20.R02,
Default Miniboot Version          : 6.1.2.20.R02,
Product ID Register               : 54
Hardware Revision Register        : 00
CPLD Revision Register            : 06
XFP Module ID                     : 02
```

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 (that is, 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.

output definitions (continued)

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.
BootROM Version	The current BootROM version.
Backup Miniboot Version	The current backup miniboot version.
Default Miniboot Version	The current default miniboot version.
Product ID Register	The register number of the product ID.
Hardware Revision Register	The register number of the hardware revision.
CPLD Revision Register	The register number of the CPLD revision.
XFP Module ID	The ID number of the XFP module.

Release History

Release 6.1; command was introduced.

Related Commands

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

show chassis [*number***]**

Syntax Definitions

number	Specifies the slot (that is, switch) number within a stack of switches. The valid range of slot numbers is 1–8, depending on the size of the stack.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- This command may be used when logged into either the primary or secondary CMM.
- The *number* parameter is not an option when using this command on a standalone switch or chassis.

Examples

```
-> show chassis

Chassis 1
  Model Name:                   OS6850E-24X,
  Description:                  24 G  2 10G,
  Part Number:                  902937-90,
  Hardware Revision:            07,
  Serial Number:                L408029P,
  Manufacture Date:             MAR 15 2011,
  Admin Status:                 POWER ON,
  Operational Status:           UP,
  Number Of Resets:             2104
  MAC Address:                  00:e0:b1:d3:08:ff,


Chassis 2
  Model Name:                   OS6850-48E,
  Description:                  10/100/1000,
  Part Number:                  902274-10,
  Hardware Revision:            004,
  Serial Number:                432L0008,
  Manufacture Date:             SEP 08 2004,
  Admin Status:                 POWER ON,
  Operational Status:           UP,
  Number Of Resets:             115
  MAC Address:                  00:e0:b2:d3:08:ff,
```

```
Chassis 3
  Model Name:                     OS6850-48E,
  Description:                    10/100/1000,
  Part Number:                    902274-10,
  Hardware Revision:              002,
  Serial Number:                  E23L9037,
  Manufacture Date:               JUN 09 2004,
  Admin Status:                   POWER ON,
  Operational Status:             UP,
  Number Of Resets:               115
```

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-Lucent part number for the chassis.
Hardware Revision	The hardware revision level for the chassis.
Serial Number	The Alcatel-Lucent 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.
Number of Resets	The number of times the CMM has been reset (that is, reloaded or rebooted) since the last cold boot of the switch.

Release History

Release 6.1; command was introduced.

Related Commands

show hardware info	Displays the current system hardware information.
show power	Displays the 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 the CMM modules in a standalone switch or the switches that perform the CMM role running in a stack.

show cmm [*number***]**

Syntax Definitions

number	Specifies the CMM slot number within a standalone switch or the CMM switch number within a stack switches.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- On OmniSwitch chassis-based 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 chassis-based 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 chassis-based switches, CMM information is displayed separately for each subcomponent. For example, on OmniSwitch 9000E switches, CMM-A-1 refers to the fabric board of a CMM installed in the left position; on OmniSwitch 9000E switches CMM-A-2 refers to the processor board of the same CMM.
- If a switch, which performs a secondary CMM role is installed and runs in a stack, the hardware and status information for both the switches that perform the primary and secondary CMM role will be displayed.
- This command may be used when logged into the switch that performs either the primary or secondary CMM role in a stack.

Examples

```
-> show cmm
CMM in slot 1
  Model Name:                     OS6850E-U24,
  Description:                    10/100/1000,
  Part Number:                    902271-10,
  Hardware Revision:              002,
  Serial Number:                  E23L9059,
  Manufacture Date:               JUN 08 2004,
  Firmware Version:               N/A,
  Admin Status:                   POWER ON,
  Operational Status:             UP,
  Power Consumption:              0,
  Power Control Checksum:         0x0,
  MAC Address:                    00:d0:95:a3:e5:09,
```

output definitions

Model Name	The model name of the switch. Note that on OmniSwitch chassis-based switches, CMM modules are made up of two major subcomponents: the fabric board and the processor board. Fabric boards are denoted as OS9*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 (for example, BBUS Bridge or PROCESSOR).
Part Number	The Alcatel-Lucent part number for the board.
Hardware Revision	The hardware revision level for the board.
Serial Number	The Alcatel-Lucent serial number for the board.
Manufacture Date	The date the board was manufactured.
Firmware Version	The firmware version for the board 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 Consumption	The current power consumption for the CMM.
Power Control Checksum	The current power control checksum for the corresponding CMM.
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 Addre sses and Ranges” chapter of the *OmniSwitch AOS Release 6 Switch Management Guide* for more information.

Release History

Release 6.1; command was introduced.

Related Commands

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

show ni

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

show ni [*number***]**

Syntax Definitions

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

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

This command may be used when logged into the switch that performs either the primary or secondary CMM role in a stack.

Examples

```
-> show ni 1
Module in slot 1
  Model Name:                   OS9-GNI-C20L,
  Description:                  RJ45(Upgd)SFP,
  Current mode of 10G ports:    uplink,
  Mode of 10G ports at next boot:stacking,
  Part Number:                  902434-90,
  Hardware Revision:            A07,
  Serial Number:                H03Q0008,
  Manufacture Date:             JAN 31 2007,
  Firmware Version:
  Admin Status:                 POWER ON,
  Operational Status:           UP,
  Power Consumption:            49,
  Power Control Checksum:       0x0,
  MAC Address:                  00:e0:b1:6a:43:10,
  ASIC - Physical 1:            BCM56504_B2
  CPLD - Physical 1:            0010/00
  UBOOT Version :               6.1.5.354.R01
  UBOOT-miniboot Version :      No Miniboot
  POE SW Version :              n/a
  C20L Upgd FailCount :         0

(OS6850E-XNI-U2)-> show ni
Module in slot 7
  Model Name:                   OS6850E-U24X,
```

```
Description:                    24 G SFP  2 10G,
Current Switch mode :           OS6850E,
Saved Switch mode :             OS6850E,
Current mode of 10G ports:      uplink,
Mode of 10G ports at next boot:uplink,
Part Number:                    902940-90,
Hardware Revision:              08,
Serial Number:                  L508017P,
Manufacture Date:               MAR 15 2011,
Firmware Version:               ,
Admin Status:                   POWER ON,
Operational Status:             UP,
Power Consumption:              0,
Power Control Checksum:         0xb183,
CPU Model Type   :              Motorola MPC8248,
MAC Address:                    00:e0:b1:f5:02:3b,
ASIC - Physical 1:              BCM56514_A0,
FPGA - Physical 1:              0007/00,
UBOOT Version :                 6.4.4.213.R01,
UBOOT-miniboot Version :        6.4.4.213.R01,
POE SW Version :                n/a

  10G Daughter Board  1
    Model Name:                     OS6-XNI-U2,
    Description:                    2 10G SFP+,
    Part Number:                    902953-90,
    Hardware Revision:              03,
    Serial Number:                  L468188P,
    Manufacture Date:               DEC 10 2010,
    Firmware Version:               ,
    Admin Status:                   POWER ON,
    Operational Status:             UP
    MAC Address:                    00:e0:b1:93:a5:7c,
    ASIC - Physical 1:              ,
```

output definitions

Model Name	The NI module name. For example, OS9-GNI-C24 indicates a twenty four-port 10/100/1000BaseT Ethernet module.
Description	A general description of the NI. For example, 24pt 10/100/1000BaseT Mod indicates a twenty four-port 10/100/1000BaseT Ethernet module.
Part Number	The Alcatel-Lucent part number for the NI.
Hardware Revision	The hardware revision level for the NI.
Serial Number	The Alcatel-Lucent serial number for the NI printed circuit board (PCB).
Manufacture Date	The date the NI was manufactured.
Firmware Version	The firmware version for the NI ASICs.
Admin Status	The current power status of the NI. Options include POWER ON or POWER OFF.

output definitions (continued)

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 Consumption	The current power consumption for the CMM.
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 ASICs.
CPLD - Physical	General information regarding the CPLD.
UBOOT Version	UBOOT version of the NI.
UBOOT-miniboot Version	UBOOT-miniboot version of the NI.
POE SW Version	POE software version of the NI (POE modules only).
C20L Upgd FailCount	The number of failed upgrade attempts (C20L modules that have attempted to be upgraded only).

Release History

Release 6.1; command was introduced.
Release 6.1.5; fields added.

Related Commands

reload ni	Reloads (that is, 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 the basic information for either a specified module or all modules installed in the chassis.
show module long	Displays the detailed information for either a specified module or all modules installed in the chassis.
show module status	Displays the basic status information for either a specified module or all modules installed in the chassis.

MIB Objects

```
chasEntPhysOperStatus
```

show module

Displays the basic information for either a specified module or all modules installed in a standalone switch chassis or a stack. Modules include switches performing the primary and secondary CMM roles and Network Interface (NI) in a stack.

show module [*number***]**

Syntax Definitions

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

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

This command may be used when logged into the switch that performs either the primary or secondary CMM role in a stack.

Examples

```
-> show module
                                    HW    Mfg
Slot     Part-Number     Serial #   Rev   Date       Model Name
-------+--------------+------------+---+----------+----------------------------
CMM-1    902271-10      E23L9059     002 JUN 08 2004  OS6850E
NI-1     902271-10      E23L9059     002 JUN 08 2004  OS6850E
```

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 60-35 for additional information on CMM location callouts.
Part-Number	The Alcatel-Lucent part number for the module.
Serial #	The Alcatel-Lucent 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, OS9-GNI-U24 indicates a twenty four-port Gigabit Ethernet module.

Release History

Release 6.1; command was introduced.

Related Commands

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

show module long

Displays the detailed information for either a specified module or all the modules installed in a standalone switch chassis or a stack. Modules include switches performing the primary and secondary CMM roles and Network Interface (NI) in a stack.

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

Syntax Definitions

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

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- When a module with a daughter board is viewed using the show module long command (for example, an OS9-GNI-C24 module provides 24 10/100/1000 BaseT auto-sensing twisted-pair ports), 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 the switch that performs either the primary or secondary CMM role in a stack.

Examples

```
-> show module long
CMM in slot 1
  Model Name:                   OS6850E-U24X,
  Description:                  10/100/1000,
  Part Number:                  902271-10,
  Hardware Revision:            002,
  Serial Number:                E23L9059,
  Manufacture Date:             JUN 08 2004,
  Firmware Version:             N/A,
  Admin Status:                 POWER ON,
  Operational Status:           UP,
  Power Consumption:            0,
  Power Control Checksum:       0x0,
  MAC Address:                  00:d0:95:a3:e5:09,

Module in slot 1
  Model Name:                   OS6850-U24,
  Description:                  10/100/1000,
```

```
Part Number:                    902271-10,
Hardware Revision:              002,
Serial Number:                  E23L9059,
Manufacture Date:               JUN 08 2004,
Firmware Version:               N/A,
Admin Status:                   POWER ON,
Operational Status:             UP,
Power Consumption:              200,
Power Control Checksum:         0x0,
MAC Address:                    00:d0:95:a3:e5:0b,
ASIC - Physical 1 (hex):        BCM5695_A1,
ASIC - Physical 2 (hex):        BCM5695_A1,
ASIC - Physical 3 (hex):        BCM5670_A1
CPLD - Physical 1 (hex):        0006/00
```

output definitions

Model Name	The NI module name. For example, OS9-GNI-C24 indicates a twenty four-port 10/100/1000BaseT Ethernet module.
Description	A general description of the NI. For example, 24pt 10/100/1000BaseT Mod indicates a twenty four-port 10/100/1000BaseT Ethernet module.
Part Number	The Alcatel-Lucent part number for the NI.
Hardware Revision	The hardware revision level for the NI.
Serial Number	The Alcatel-Lucent serial number for the NI printed circuit board (PCB).
Manufacture Date	The date the NI was manufactured.
Firmware Version	The firmware version for NI 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 ASICs.
CPLD - Physical	General information regarding the CPLD.

Release History

Release 6.1; command was introduced.

Related Commands

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

show module status

Displays the basic status information for either a specified module or all modules installed in a standalone switch chassis or a stack. Modules include switches performing the primary and secondary CMM roles and Network Interface (NI) in a stack.

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

Syntax Definitions

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

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

This command may be used when logged into the switch that performs either as the primary or secondary CMM role in a stack.

Examples

```
-> show module status
       Operational                Firmware
Slot     Status      Admin-Status   Rev           MAC
------+------------+------------+---------+-----------------
CMM-1    UP           POWER ON      N/A     00:d0:95:a3:e5:09
NI-1     UP           POWER ON      N/A     00:d0:95:a3:e5:0b
```

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 60-35 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 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 *OmniSwitch AOS Release 6 Switch Management Guide*. For NI modules, the MAC address for the corresponding NI is displayed.

Release History

Release 6.1; command was introduced.

Related Commands

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

show power

Displays the 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- When the **show power** command is entered on stackable 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 chassis-based 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 chassis-based 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

```
-> show power
Slot  PS   Wattage   Type   Status     Location
----+----+---------+------+-----------+----------
      1     600      AC    UP           Internal
      2     600      AC    UP           Internal
      3     --       --    --           --
      4     600      IP    UP           External
      5     600      IP    UP           External
      6     600      IP    UP           External
      7     600      IP    UP           External

-> show power 5
Module in slot PS-5
(Power Shelf slot 5)
  Model Name:                   OS-IPS-600A,
  Description:                  ILPS AC,
  Part Number:                  902252-10,
```

```
Hardware Revision:              A01,
Serial Number:                  E51P4078,
Manufacture Date:               JAN 07 2005,
Operational Status:             UP,
Power Provision:                600
```

output definitions

Model Name	The power supply model number.
Description	A description of the associated power supply. This field will reflect the model name in most cases.
Part Number	The Alcatel-Lucent part number for the power supply.
Hardware Revision	The hardware revision level for the power supply.
Serial Number	The Alcatel-Lucent serial number for the power supply.
Manufacture Date	The date the power supply was manufactured.
Type	The type of power supply. Options include AC or IP.
Location	The location of the power supply. Options include Internal or External.
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.

Release History

Release 6.1; command was introduced.

Related Commands

show chassis	Displays the 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	Specifies the switch (slot) number of the chassis for stackable switches or a fan number for chassis-based switches.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 9000E

Usage Guidelines

- On chassis-based switches if no fan number is specified the status of all fans is displayed.
- On stackable switches if no switch number is specified the status of all fans for all switches is displayed.

Examples

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

output definitions

Chassis	The number of the switch in a stack.
Fan	The fan number describing the fan position.
Status	The current operational status of the corresponding fan.

Release History

Release 6.1; 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	Specifies the slot (that is, switch) number within the stack. The valid range of slot numbers is 1–8, depending on the size of the stack.

Defaults

If a slot number is not specified with this command on an OmniSwitch stackable switch, temperature information for all switches operating in the stack is displayed by default.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

The *number* parameter is not an option when using this command on a single-chassis, standalone switch, such as the OmniSwitch 9000E.

Examples

```
-> show temperature

Temperature for chassis 1
  Hardware Board Temperature (deg C)              = 41,
  Temperature Upper Threshold Range (deg C)       = 15 to 80,
  Temperature Upper Threshold (deg C)             = 57,
  Temperature Status                              = UNDER THRESHOLD,
  Temperature Danger Threshold (deg C)            = 80

Temperature for chassis 2
  Hardware Board Temperature (deg C)              = 40,
  Temperature Upper Threshold Range (deg C)       = 15 to 80,
  Temperature Upper Threshold (deg C)             = 57,
  Temperature Status                              = UNDER THRESHOLD,
  Temperature Danger Threshold (deg C)            = 80

Temperature for chassis 3
  Hardware Board Temperature (deg C)              = 40,
  Temperature Upper Threshold Range (deg C)       = 15 to 80,
  Temperature Upper Threshold (deg C)             = 57,
  Temperature Status                              = UNDER THRESHOLD,
  Temperature Danger Threshold (deg C)            = 80
```

output definitions

Hardware Board Temperature	The current chassis temperature as determined by the built-in temperature sensor. The temperature is displayed in degrees Celsius. This temperature is checked against the upper threshold value. If the threshold is exceeded, a warning is sent to the user.
Temperature Upper Threshold Range	The supported threshold range when specifying a threshold for the switch via the **temp-threshold** command.
Temperature Upper Threshold	The warning temperature threshold, in degrees Celsius. If the switch reaches or exceeds this temperature, the primary switch or CMM TEMP LED displays amber and a warning is sent to the user. For information on changing the upper threshold value, refer to the **temp-threshold** command on page 60-24.
Temperature Status	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 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 reaches this value the switch will power off all Network Interface (NI) modules until the temperature conditions (for example, chassis air flow obstruction or ambient room temperature) have been addressed.

Release History

Release 6.1; command was introduced.

Related Commands

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

MIB Objects

```
chasChassisTable
   chasHardwareBoardTemp
   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 6400, 6850E, 6855

Usage Guidelines

- The OS6850E must be in the correct mode depending on which model it is being stacked with.

Examples

```
-> show stack topology
                                          Link A  Link A          Link B  Link B
NI      Role      State   Saved  Link A  Remote  Remote  Link B  Remote  Remote
                          Slot   State   NI      Port    State   NI      Port
----+-----------+--------+------+-------+-------+-------+-------+-------+-------
   1 PRIMARY     RUNNING    1    UP          3   StackB  UP          2   StackA
   2 IDLE        RUNNING    2    UP          1   StackB  UP          3   StackA
   3 SECONDARY   RUNNING    3    UP          2   StackB  UP          1   StackA
```

output definitions

NI	The current slot position for each switch in the virtual chassis (that is., stacked configuration). Note that the order of the slot numbers does not necessarily correspond with the physical positions of switches within the stack. In other words, slot position 1 may not be the uppermost (top) switch in the stack. To manually assign these slot numbers via the CLI, use the **stack set slot** command.
Role	The current management role of the corresponding switch within the stack. Options include PRIMARY (the switch is the primary management module in the stack; standalone switches also display this role), SECONDARY (the switch is the secondary—or backup—management module in the stack), IDLE (the switch does not have a management role but is operating normally as a network interface module within the stack), PASS-THRU (the switch is operating in pass-through mode), UNDEFINED (the switch current role is not known).

output definitions (continued)

State	The current operational state of the corresponding switch. Options include RUNNING (the switch is up and operating normally), DUP-SLOT (the switch has a duplicate saved slot number or incorrect mode and has automatically entered pass-through mode), INC-SLOT (the switch is in the incorrect mode and has automatically entered pass-through mode),CLR-SLOT (the switch has been manually "cleared" via the **stack clear slot** command and is now in pass-through mode), OUT-SLOT (the current stacked configuration already has eight switches and therefore cannot accommodate this switch), OUT-TOK (there are not enough unused tokens remaining in the current stacked configuration to accommodate this switch), UNKNOWN (the switch current state is not known).
Saved Slot	The designated saved slot number for the corresponding switch. The saved slot number is the slot position the switch will assume following a reboot. A value of zero (0) indicates that the switch has been "cleared" and, as a result, is designated for pass-through mode. To assign saved slot numbers, use the **stack set slot** command. To clear a switch and designate it for pass-though mode, use the **stack clear slot** command.
Link A State	The current status of the stacking cable link at the switch stacking port A. Options include UP, DOWN, or UNKNOWN.
Link A Remote NI	The slot number of the switch to which stacking cable A *remote end* is connected. In other words, if a switch in slot position 1 displays a Link A Remote NI value of 3, this indicates that the stacking cable plugged into slot 1 stacking port A is connected to the *slot 3* switch. If no stacking cable link exists, the value 0 displays.
Link A Remote Port	The specific stacking port to which stacking cable A *remote end* is connected. Options include StackA, StackB, and 0. If stacking cable A remote end is connected to stacking port B on the other switch, the value displays StackB. If no stacking cable link exists, the value 0 displays.
Link B State	The current status of the stacking cable link at the switch stacking port B. Options include UP, DOWN, or UNKNOWN.
Link B Remote NI	The slot number of the switch to which stacking cable B *remote end* is connected. In other words, if a switch in slot position 6 displays a Link A Remote NI value of 7, this indicates that the stacking cable plugged into slot 6 stacking port B is connected to the *slot 7* switch.
Link B Remote Port	The specific stacking port to which stacking cable B *remote end* is connected. Options include StackA, StackB, and 0. If stacking cable B remote end is connected to stacking port B on the other switch, the value displays StackB. If no stacking cable link exists, the value 0 displays.

Release History

Release 6.1; command was introduced.
Release 6.4.4; INC-SLOT output parameter was added.

Related Commands

show stack status	Displays the current redundant stacking cable status and token availability for a stacked configuration.
stack clear slot	Sets the *saved slot* number or mode for stackable configuration switches.

MIB Objects

```
alaStackMgrChassisTable
   alaStackMgrSlotNINumber
   alaStackMgrSlotCMMNumber
   alaStackMgrChasRole
   alaStackMgrLocalLinkStateA
   alaStackMgrRemoteNISlotA
   alaStackMgrRemoteLinkA
   alaStackMgrLocalLinkStateB
   alaStackMgrRemoteNISlotB
   alaStackMgrRemoteLinkB
   alaStackMgrChasState
   alaStackMgrSavedSlotNINumber
   alaStackMgrCommandAction
   alaStackMgrCommandStatus
```

show stack status

Displays the current redundant stacking cable status and token availability for a stacked configuration.

show stack status

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855

Usage Guidelines

N/A

Examples

```
-> show stack status

Redundant cable status  : present
Tokens used             : 8
Tokens available        : 24
```

output definitions

Redundant cable status	Indicates whether a redundant stacking cable is currently installed. Options include **present** and **not present**. To provide added resiliency and redundancy, it is strongly recommended that a redundant stacking cable is connected from the top switch in the stack to the bottom switch in the stack at all times. For more information on stack redundancy, refer to the *Hardware Users Guide*.
Tokens used	The number of tokens used in the current stacked configuration. Each virtual chassis (also referred to as a stacked configuration) is allocated a number of tokens per stack. If a switch is added to a stack in which there are not enough tokens available, the incoming switch is automatically placed in pass-though mode. For detailed information on stack-related topics, including tokens and pass-through mode, refer to the *Hardware Users Guide*.
Tokens available	The number of remaining tokens for any incoming switches in a stack.

Release History

Release 6.1; command was introduced.

Related Commands

show stack topology	Displays the current operating topology of switches within a stack.

MIB Objects

```
alaStackMgrStackStatus
alaStackMgrTokensUsed
alaStackMgrTokensAvailable
```

hash-control

Configures the hash control method on the switch. Depending upon this configuration, hashing algorithm used by various applications for packet forwarding will be affected.

hash-control {brief | extended [udp-tcp-port] | load-balance non-ucast {enable | disable}}

hash-control extended no udp-tcp-port

Syntax Definitions

brief	Sets hashing to brief mode.
extended	Sets hashing to extended mode.
udp-tcp-port	Sets extending hashing to use UDP/TCP ports.
enable | disable	Enables or disables the the load balancing of non-unicast traffic on a link aggregate.

Defaults

parameter	default
hash-control (6400/6850E/ 6855)	brief
hash-control (9000E)	extended
udp-tcp-port	disabled
non-ucast	disabled

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Disabling TCP-UDP port hashing is recommended when Server Load Balancing (SLB) is configured, because SLB dynamically assigns ports.
- The hash control setting also impacts the fabric load balancing for Chassis based products. It is recommended not to set brief hashing mode on Chassis based products.
- Changing the hash control mode affects the hashing algorithm for Link Aggregation, Server Load Balancing and EMCP.
- The hashing mode must be set to extended to enable UDP/TCP port hashing.
- Enabling or disabling the **load-balance non-ucast** option applies to all link aggregates. When this option is disabled (the default), link aggregation will only load balance unicast packets; all non-unicast packets are sent through the primary port of the link aggregate.
- When the **load-balance non-ucast** option is enabled, all non-unicast traffic (broadcast, L2 multicast, L3 multicast, and unknown unicast) is load balanced over the link aggregate.

Examples

```
-> hash-control brief
-> hash-control extended
-> hash-control extended udp-tcp-port
-> hash-control extended no udp-tcp-port
-> hash-control load-balance non-ucast enable
-> hash-control load-balance non-ucast disable
```

Release History

Release 6.4.2; command was introduced.
Release 6.4.3; **load-balance non-ucast** parameter was added.

Related Commands

show hash-control	Displays the current hash control setting for the switch.

MIB Objects

```
alaChasHashMode
alaChasUdpTcpPortMode
alachasNonUCHashControl
```

show hash-control

Displays the current hash control settings for the switch.

show hash-control [non-ucast]

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show hash-control
Hash Mode    = brief,
Udp-Tcp-Port = disabled
-> show hash-control non-ucast
Non-ucast Hash Status = Enabled,
```

output definitions

Hash Mode	The current hash mode.
Udp-Tcp-Port	Status of UDP/TCP hashing.
Non-ucast Hash Status	Status of Non-ucast hash status.

Release History

Release 6.4.2; command was introduced.
Release 6.4.3; **non-ucast** parameter was added.

Related Commands

hash-control	Configures the hash mode of the switch..

MIB Objects

```
alaChasHashMode
alaChasUdpTcpPortMode
alachasNonUCHashControl
```

license apply

Activates the license for licensed protocols on the switch.

license apply

Syntax Definitions

NA

Defaults

By default licensed protocols are not activated on the switch.

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Currently, MPLS is the only licensed feature on an OmniSwitch.
- Ensure the license file *lmLicense.dat* is placed in the **/flash** directory of the primary CMM.
- When the **license apply** command is issued, the switch displays a message to ensure the installation. Enter 'Y' to apply the license and reboot the switch.
- Use **show license file** command to verify the installed license.

Examples

```
-> license apply
The switch will reboot after the license is applied.
Are you sure you want to proceed(Y/N)?
Y
```

Release History

Release 6.4.2; command was introduced.

Related Commands

show license info	Displays all the licensed applications installed on the switch.
show license file	Displays the license file information of the switch.

MIB Objects

```
aluLicenseManagerApplyLicense
```

show license info

Displays all the licensed applications installed on the switch.

show license info

Syntax Definitions

NA

Defaults

NA

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use this command to verify which licenses are installed on the switch.
- The number of days remaining is determined only by the switch up time. If a switch is turned off the Time Remaining is not decremented.

Examples

```
->show license info
  Application    License Type
  -------------+--------------
  MPLS            Permanent
```

output definitions

Application	Displays the name of the licensed applications installed on the switch.
Type	The type of license.

Release History

Release 6.4.2; command was introduced.

Related Commands

show license file	Displays the license file information of the switch.

MIB Objects

```
aluLicenseManagerInfoTable
   aluLicenseedApplication
   aluLicenseType
```

show license file

Displays the information contained in the license file.

show license file

Syntax Definitions

NA

Defaults

NA

Platforms Supported

OmniSwitch 9000E

Usage Guidelines

- Use this command to display the contents of the *lmLicense.dat* license file.
- The *lmLicense*.dat file can contain licenses for other switches.

Examples

```
-> show license file
MAC Address         Application
------------------+-------------
00:d0:95:d5:e6:01      MPLS
00:d0:95:d5:e6:0a      MPLS
00:d0:95:d5:e6:0b      MPLS
00:d0:95:d5:e6:0c*     MPLS

* - indicates entry applicable for local switch
```

output definitions

MAC Address	Displays the base MAC address of the switch. An asterisk indicates the MAC address of the local switch.
Application	Displays the name of the licensed application.

Release History

Release 6.4.2; command was introduced.

Related Commands

show license info	Displays all the licensed applications installed on the switch.

MIB Objects

```
aluLicenseManagerFileInfoTable
   aluSwitchMacAddress
   aluLicensedFileApplication
```

power slot bps connector-priority

This command is used to specify the priority of a connector on the OS-BPS.

power slot *slot-number* **bps connector-priority** *priority*

Syntax Definitions

slot-number	The slot number whose priority will be changed.
priority	Specifies the OS-BPS connector priority. (1-8)

Defaults

Connector Index	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Default Priority Value	8	7	6	5	4	3	2	1

Platforms Supported

OmniSwitch 6850E

Usage Guidelines

- When the OS-BPS needs to reduce power due to a power supply removal or failure it will start with the lowest priority (1) connector (8) and continue in order until it has sufficient power.
- Using the default values listed above, the switch attached to connector 8 would be the first to lose power, then the switch attached to connector 7, etc.
- The higher the priority value the higher the priority. For example, priority 8 is the highest priority and priority 1 is the lowest priority.
- This command only has an effect when the OS-BPS is running in full (N+N) mode.

Examples

```
-> power slot 2 bps connector-priority 8
-> power slot 1 bps connector-priority 7
```

Release History

Release 6.4.5; command was introduced.

Related Commands

show power bps connector-priority	This command is used to display the current OS-BPS connector priority.

MIB Objects

```
chasNiNumber
   chasOSBpsConnectorPriority
```

power bps mode

This command is used to change the mode of the OS-BPS.

power bps mode {single | full}

Syntax Definitions

single | full	Specifies either single mode (N+1) or full mode (N+N).

Defaults

parameter	default
Mode	single (N+1)

Platforms Supported

OmniSwitch 6850E

Usage Guidelines

- Any unit in a stack can be used to change the mode but the OS-BPS will only operate in the last mode that was configured.
- Single mode is an unmanaged power mode and the OS-BPS will continue to provide redundant power until the requested power is more than the OS-BPS can provide.
- Full mode is a managed power mode and the OS-BPS will intelligently provide redundant power based on its available power and the connector priority.

Examples

```
-> power bps mode full
```

Release History

Release 6.4.5; command was introduced.

Related Commands

show power supply bps	This command is used to display the inventory and status of the OS-BPS.

MIB Objects

```
alaChasOSBpsMode
```

update bps firmware

This command is used to update the firmware of the OS-BPS.

update bps firmware

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E

Usage Guidelines

Contact Service & Support for appropriate firmware file.

Examples

```
-> update bps firmware
```

Release History

Release 6.4.5; command was introduced.

Related Commands

show power supply bps	This command is used to display the inventory and status of the OS-BPS.

MIB Objects

N/A

show power bps connector-priority

This command is used to display the current OS-BPS connector priority.

show power bps connector-priority

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E

Usage Guidelines

N/A

Examples

```
-> show power bps connector-priority
Slot                priority
------------       -------------
 1                   1
 2                   8
 3                   3
 4                   4
 5                   6
 6                   5
 7                   7
 8                   2
```

output definitions

Slot	The slot number of the stack.
Priority	The priority level of the slot.

Release History

Release 6.4.5; command was introduced.

Related Commands

power slot bps connector-priority	This command is used to specify the priority of a connector on the OS-BPS.

MIB Objects

```
alaChasOSBpsMode
```

show power supply bps

This command is used to display the inventory and status of the OS-BPS.

show power supply bps

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6850E

Usage Guidelines

N/A

Examples

```
-> show power supply bps
Shelf
  Model Name:                   OS-BPS,
  Module Type:                  Backup Advanced Power Shelf
  Description:                  OS-PS-shelf,
  Part Number:                  90200-00,
  Hardware Revision:            B02,
  Serial Number:                1030000831,
  Manufacture Date:             Jul 23 2010,
  Operational Status:           UP,
  PoE Power Provision           4500W
  PoE Allocated:                4000W
  System Power Allocated:       900W
  Mode:                         N+N
  CPLD revision:   0x12
  C_MCU revision:   0xE
  M_MCU revision:   0X9
System power supply 1
  Description:                  OS-PS-450W-A,
  Module Type:   0x150000001
  Part Number:                  902916-90,
  Hardware Revision:            B02,
  Serial Number:                1030000831,
  Manufacture Date:             Jul 23 2010,
  Operational Status:           UP,
  Power Provision:              450W
System power supply 2
  Description:                  OS-PS-450W-A,
  Module Type:                  0x150000001
  Part Number:                  902916-90,
  Hardware Revision:            B02,
```

```
    Serial Number:                1030000831,
    Manufacture Date:             Jul 23 2010,
    Operational Status:           UP,
    Power Provision:              2000W
  POE power supply 1
   Description:                   OS-PS-2000W,
   Module Type:                   0x06040101
    Part Number:                  902916-90,
    Hardware Revision:            B02,
    Serial Number:                1030000831,
    Manufacture Date:             Jul 23 2010,
    Operational Status:           UP,
    Power Provision:              2000W
  POE power supply 2
    Description:                  OS-PS-2000W,
    Module Type:                  0x06040101
    Part Number:                  902916-90,
    Hardware Revision:            B02,
    Serial Number:                1030000831,
    Manufacture Date:             Jul 23 2010,
    Operational Status:           UP,
    Power Provision:              2000W
  POE power supply 3
    Description:                  OS-PS-2000W,
    Module Type:                  0x06040101
    Part Number:                  902916-90,
    Hardware Revision:            B02,
    Serial Number:                1030000831,
    Manufacture Date:             Jul 23 2010,
    Operational Status:           UP,
    Power Provision:              2000W
```

output definitions

Model Name	The model name for the chassis or power supply.
Module type	The module type of the chassis or power supply.
Description	The description for the chassis or power supply.
Part Number	The Alcatel-Lucent part number for the chassis or power supply.
Hardware Revision	The hardware revision level of the chassis or power supply.
Serial Number	The serial number of the chassis or power supply.
Manufacture Date	The manufacture date of the chassis or power supply.
Operational Status	The operational status of the chassis or power supply.
PoE Total Available Power	The total amount of PoE power available in the OS-BPS.
System Total Available Power	The total amount of system power available in the OS-BPS.
PoE Total Allocation	The total amount of PoE power being used in the OS-BPS.
System Total Allocation	The total amount of system power being used in the OS-BPS.
Mode	The mode of the OS-BPS.
C_MCU Revision	The C_MCU revision level.
M_MCU Revision	The M_MCU revision level.
CPLD Revision	The CPLD revision level.

Release History

Release 6.4.5; command was introduced.

Related Commands

power bps mode	This command is used to change the mode of the OS-BPS.
update bps firmware	This command is used to update the firmware of the OS-BPS.

MIB Objects

```
alaChasOSBpsMode
```

61 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.

In stackable switches, CMS is responsible for sharing the base MAC address of the primary switch with all the other switches in the stack. This helps the secondary switch to retain the same MAC address during takeover.This is called MAC Address Retention.

Note. MAC Retention is supported on the OmniSwitch 6850E and OmniSwitch 6400 Series switches.

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
mac-retention status
mac-retention dup-mac-trap
mac release
show mac-range
show mac-range alloc
show mac-retention status

---

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-Lucent 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 6400, 6850E, 6855, 9000E

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 by 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 6.1; command was introduced.

Related Commands

show mac-range	Displays the MAC range table.

MIB Objects

```
chasMacAddressRangeTable
   chasMacRangeIndex
   chasGlobalLocal
   chasMacAddressStart
   chasMacAddressCount
```

mac-retention status

Enables or disables the MAC retention status.

mac-retention status {enable | disable}

Syntax Definitions

enable	Enables the administrative status of MAC retention.
disable	Disables the administrative status of MAC retention.

Defaults

Parameter	Status
enable | disable	**disable**

Platforms Supported

OmniSwitch 6400, 6850E, 6855-U24X

Usage Guidelines

- When MAC retention is enabled, the stack uses the MAC address of the primary switch even after it has failed.
- When the administrative status of MAC retention is enabled, the stack performance is enhanced.

Examples

```
-> mac-retention status enable
```

Release History

Release 6.2.1; command was introduced.

Related Commands

show mac-retention status	Displays the MAC retention status.

MIB Objects

```
chasMacAddrRetentionObjects
   chasMacAddrRetentionStatus
```

mac-retention dup-mac-trap

Enables or disables the duplicate MAC address trap status.

mac-retention dup-mac-trap {enable | disable}

Syntax Definitions

enable	Enables the duplicate MAC address trap status.
disable	Disables the duplicate MAC address trap status.

Defaults

Parameter	Status
enable | disable	**disable**

Platforms Supported

OmniSwitch 6400, 6850E, 6855-U24X

Usage Guidelines

If the old primary switch is not detected and included in the stack within a pre-defined time period, an SNMP trap will be generated.

Examples

```
-> mac-retention dup-mac-trap enable
```

Release History

Release 6.2.1; command was introduced.

Related Commands

show mac-retention status	Displays the MAC retention status.

MIB Objects

```
chasMacAddrRetentionObjects
  chasPossibleDuplicateMacTrapStatus
```

mac release

Releases the MAC address currently being used as the primary base MAC address.

mac release

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855-U24X

Usage Guidelines

The MAC address is released only if the address has not been derived from the EEPROM (i.e., it should be a retained MAC address of the old primary switch).

Examples

```
-> mac release
```

Release History

Release 6.2.1; command was introduced.
Release 6.3.1; **mac-retention** keyword was replaced with the **mac** keyword.

Related Commands

N/A

MIB Objects

```
chasMacAddrRetentionObjects
  chasMacAddrRetentionStatus
```

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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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).

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 61-7 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 6.1; 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
```

show mac-retention status

Displays the MAC retention status.

show mac-retention status

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855-U24X

Usage Guidelines

- If the administrative status of MAC retention is not configured, it will be displayed as disabled by default.
- If the administrative status of the duplicate MAC address trap is not configured, it will be displayed as disabled by default.
- If the source of the currently used MAC address is not configured, it will be displayed as EEPROM by default.

Examples

```
-> show mac-retention status
MAC RETENTION STATUS
================================================================================
Admin State         : Enabled
Trap admin state    : Enabled
Current MAC address : 00:0a:0b:0c:0d:0e
MAC address source  : Retained
Topology Status     : Ring present
```

output definitions

Admin State	Displays the administrative status of MAC retention **(Enabled** or **Disabled)**.
Trap admin state	Displays the administrative status of the duplicate MAC address trap (**Enabled** or **Disabled)**.
Current MAC address	Displays the MAC address currently used by the switch.
MAC address source	Displays the source of the currently used MAC address. Options include **EEPROM** and **Retained**.
Topology Status	Displays the topology status of the stack. Options include **Ring present** and **Ring Not Present**.

Release History

Release 6.2.1; command was introduced.
Release 6.3.1; **EEPROM MAC Address** field was deleted.

Related Commands

mac-retention status	Enables or disables the MAC retention status.
mac-retention dup-mac-trap	Enables or disables the duplicate MAC address trap status.

MIB Objects

```
chasMacAddrRetentionObjects
   chasMacAddrRetentionStatus
   chasPossibleDuplicateMacTrapStatus
   chasRingStatus
   chasBaseMacAddrSource
   chasBaseMacAddr
```

62 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 server synchronized
ntp server unsynchronized
ntp client
ntp src-ip preferred
ntp broadcast-client
ntp broadcast-delay
ntp key
ntp key load
ntp authenticate
ntp master
ntp interface
ntp max-associations
ntp broadcast
ntp peer
show ntp status
show ntp client
show ntp client server-list
show ntp server client-list
show ntp server status
show ntp keys
show ntp peers
show ntp server disabled-interfaces

ntp server

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

ntp server *ip_address* **[key** *keyid***] [minpoll** *poll***] [version** *version***] [prefer]**

no ntp server *ip_address*

Syntax Definitions

ip_address	The IP address of the NTP server to be added or deleted to the client's server list.
key id	The key identification number that corresponds to the specified NTP server. The value ranges from 1 to 65534.
poll	It specifies the minimum polling interval for NTP message. 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 maximum poll interval is fixed at 10 (1,024 s). The minimum poll interval defaults to 6 (64 s), but can be decreased by the minpoll option to a lower limit of 4 (16 s), or increase to the maximum limit of 10.
version	The version of NTP being used. This will be 1, 2, 3, or 4.
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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to clear an NTP server from the list of configured servers.
- To configure NTP in the 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.

- An authentication key is composed of a 32-bit integer and 32-byte string of characters. The integer format is hexadecimal. For an NTP message to be authenticated the NTP client authentication key must match the key configured at the NTP server. This means the authentication keys must be distributed in advance of configuring the NTP client. If authentication is disabled but authentication key is present, the association will still be unauthenticated.
- 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.

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 6.1; command was introduced.

Related Commands

ntp client	Enables or disables NTP operation on the switch.

MIB Objects

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

ntp server synchronized

Enables an NTP client to invoke tests for NTP server synchronization as specified by the NTP protocol.

ntp server synchronized

Syntax Definitions

N/A

Defaults

By default, NTP synchronization is enabled.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

The NTP protocol discards the NTP servers that are unsynchronized. However, the unsynchronized NTP servers are used as network time sources.

Examples

```
-> ntp server synchronized
```

Release History

Release 6.1.5; command was introduced.

Related Commands

ntp server unsynchronized	Disables an NTP client from invoking tests for NTP server synchronization. This allows the NTP client to synchronize with unsynchronized NTP servers in the network.

MIB Objects

```
alaNtpConfig
   alaNtpPeerTests
```

ntp server unsynchronized

Disables an NTP client from invoking tests for NTP server synchronization. This allows the NTP client to synchronize with unsynchronized NTP servers in the network.

ntp server unsynchronized

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

When NTP peer synchronization tests are disabled, the NTP client is able to synchronize with either an NTP peer that is not synchronized with an atomic clock or a network of NTP servers that will finally synchronize with an atomic clock.

Examples

```
-> ntp server unsynchronized
```

Release History

Release 6.1.5; command was introduced.

Related Commands

ntp server synchronized	Enables an NTP client to invoke tests for NTP server synchronization as specified by the NTP protocol.

MIB Objects

```
alaNtpConfig
   alaNtpPeerTests
```

ntp client

Enables or disables NTP time synchronization discipline.

ntp client {enable | disable}

Syntax Definitions

enable	Enables NTP.
disable	Disables NTP.

Defaults

NTP protocol is disabled by default.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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. Up to 3 NTP servers may be defined.
- It is not necessary to specify an NTP server if the NTP client will only receive time updates from NTP broadcast servers.

Examples

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

Release History

Release 6.1; command was introduced.

Related Commands

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

MIB Objects

```
alaNtpEnable
```

ntp src-ip preferred

Configures the source IP address field of the NTP source

ntp src-ip preferred {default | no-loopback0 | *ip_address***}**

no ntp src-ip preferred

Syntax Definitions

default	The Loopback0 address, if configured, will be used for the source IP address field. If no loopback0 is configured, the vlan configured IP interface on the switch will be used.
no-loopback0	The Loopback0 address should not be used for the source IP address field and the first available IP address on the switch should be used for this field.It takes the vlan configured IP even if the loopback0 is configured on the switch.
ip_address	The IP address to be used in the source IP field.

Defaults

By default, the NTP source ip preferred setting is set to the **default** parameter.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- When configuring a specific IP address, that address must already exist on the switch.
- Use the **no** form of this command to clear a specific IP address and change the behavior back to default.

Examples

```
-> ntp src-ip preferred 192.168.10.1
-> ntp src-ip preferred no-loopback0
-> ntp src-ip preferred default
```

Release History

Release 6.3.4; command was introduced
Release 6.4.3; command was deprecated, use **ip managed-interface**.

Related Commands

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

MIB Objects

```
alaNtpSrcIp
alaNtpSrcIpConfig
```

ntp broadcast-client

Enables or disables the NTP client to receive time updates from NTP broadcast servers.

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 6400, 6850E, 6855, 9000E

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.
- In order to configure NTP in broadcast client mode, it is required to define the network server to client broadcast delay.

Examples

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

Release History

Release 6.1; 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 of received NTP broadcast messages.

ntp broadcast-delay *microseconds*

Syntax Definitions

microseconds	The number of microseconds for the broadcast delay.

Defaults

parameter	default
microseconds	4000

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 received from a broadcast NTP server.

Examples

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

Release History

Release 6.1; command was introduced.

Related Commands

ntp broadcast-client	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 that the specified key is trusted and can be used for authentication.
untrusted	Signifies that the specified key is not trusted and cannot be used for authentication. Synchronization will not occur with an untrusted authentication key.

Defaults

By default, all authentication key are untrusted.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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.The location of the file containing set of generated authentication keys is /flash/network/ntp.keys.
- 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.
- An authentication key is composed of a 32-bit integer and 32-byte string of characters. The integer format is hexadecimal. For an NTP message to be authenticated the NTP client authentication key must match the key configured at the NTP server. This means the authentication keys must be distributed in advance of configuring the NTP client. If authentication is disabled but authentication key is present, the association will still be unauthenticated.
- By default all keys read from the ntp.conf key file are untrusted therefore keys must be set to ‘trusted’ status to allow NTP to use the key for authentication.

Examples

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

Release History

Release 6.1; 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 NTP operation 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- This command reloads the key file into the switch memory. This allows for new keys in the key file 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.
- By default, all authentication keys are untrusted therefore reloading a key file will change any current trusted keys to untrusted status.
- The file ntp.keys is used during the establishment of a set of authentication keys that are used by the NTP protocol. The location of this file is fixed in directory /flash/network.

Examples

```
-> ntp key load
```

Release History

Release 6.1; 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
```

ntp authenticate

Enables or disables the authentication on a configured NTP server.

ntp authenticate {enable | disable}

Syntax Definitions

enable	Enables authentication for NTP server.
disable	Disables authentication for NTP server.

Defaults

By default, NTP authentication is disabled.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use this command to enable or disable authentication for NTP server.
- Before NTP authentication is enabled, NTP operation should be enabled by using **ntp client** command.
- Before enabling the NTP operation, NTP server must be specified using the **ntp server** command.

Examples

```
-> ntp authenticate enable
-> ntp authenticate disable
```

Release History

Release 6.4.2; command was introduced.

Related Commands

show ntp status	Displays the information about the current NTP status.

MIB Objects

```
alaNtpAuthenticate
```

ntp master

Specifies the stratum value for unsynchronized switch to act as an authoritative NTP source.

ntp master *stratum-number*

Syntax Definitions

stratum-number	Integer value ranging from 2 to 16

Defaults

Parameter	Default
stratum-number	16

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use this command to synchronize improved clocks with lower strata value if any of the trustworthy NTP sources comes up.
- Use default value of 16 if switch is not synchronized with itself.
- When the switch is synchronized, the stratum number should correspond to peer/server.

Examples

```
-> ntp master 4
```

Release History

Release 6.4.2; command was introduced.

Related Commands

show ntp status	Displays current NTP status.

MIB Objects

```
alaNtpConfig
   alaNtpSysStratum
```

ntp interface

Enables or Disables NTP server functionality for an interface.

ntp interface *interface-ip* **{enable | disable}**

Syntax Definitions

interface-ip	IP address of an interface on which NTP server functionality is to be disabled.
enable	Enables NTP server functionality on an interface.
disable	Disables NTP sever functionality on an interface.

Defaults

By default, NTP server functionality is enabled on all the interfaces.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use this command to enable or disable the incoming NTP request.
- Disabling the NTP server functionality drops the NTP request on an interface and synchronization information is not sent out.

Examples

```
-> ntp interface 10.10.10.1 disable
-> ntp interface 10.10.10.1 enable
```

Release History

Release 6.4.2; command was introduced.

Related Commands

show ntp status	Displays current NTP status.

MIB Objects

```
alaNtpAccessRestrictedTable
   alaNtpAccessRestrictedIpAddress
```

ntp max-associations

Configures the maximum number of associations on the switch.

ntp max-associations *number*

Syntax Definitions

number	Maximum no of client/server and peer associations. Integer value ranging from 0 to 64.

Defaults

By default, 32 associations are allowed on the switch.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use this command to restrict the number of client/server and peer association.
- The command can be used to change the default value of 32 to any value between 0 to 64.
- The command protects the switch from overwhelming with the NTP requests. When the limit is reached, trap is sent to indicate the switch.

Examples

```
-> ntp max-associations 20
```

Release History

Release 6.4.2; command was introduced.

Related Commands

show ntp status	Displays current NTP status.

MIB Objects

```
alaNtpConfig
   alaNtpMaxAssociation
```

ntp broadcast

Enables NTP to broadcast synchronized information to all the clients in the subnet in the configured interval.

ntp broadcast *broadcast-addr* **[version** *version***] [minpoll** *poll interval***]**

no ntp broadcast *broadcast-addr*

Syntax Definitions

broadcast-addr	Subnet for which broadcast updates are regularly sent.
version	NTP version on which the broadcast updates are sent out on the subnet for the clients. Value is 3 or 4.
poll interval	Polling interval for NTP broadcast message. This value is measured in seconds.

Defaults

Parameter	Default
version	4
poll interval	6

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use this command to configure NTP to act in broadcast server mode.
- Use the **no** form of this command to remove the configured broadcast servers.This also disables NTP synchronization information being sent for that broadcast subset.
- The NTP broadcast address needs to defined to enable NTP broadcast mode. A maximum of 3 broadcast addresses can be configured.
- 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.

Examples

```
-> ntp broadcast 10.145.59.255 version 4 minpoll 5
-> no ntp broadcast 10.145.59.255
```

Release History

Release 6.4.2; command was introduced.

Related Commands

ntp broadcast-client	Enables or disables the client's broadcast mode.
ntp broadcast-delay	Sets the broadcast delay time in microseconds

MIB Objects

```
alaNtpPeerTable
   alaNtpPeerType
   alaNtpPeerVersion
   alaNtpPeerMinpoll
```

ntp peer

Configures NTP to operate in the symmetric active peering mode.This also enables the establishment of an active symmetric association with the specified remote peer.

ntp peer *ip-address* **[key** *keyid***] [version** *version***] [minpoll** *poll interval***]**

no ntp peer *ip-address*

Syntax Definitions

ip-address	IP address of the remote peer.
key-id	Authentication key for the remote peer.
version	NTP packet version to be used for the peer association.
poll interval	Polling interval for NTP broadcast message. Poll interval which when expires, packets will be sent to the peer.

Defaults

Parameter	Default
version	4
poll interval	6

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use **no** form of this command to remove the peers that are configured to act in symmetric active mode.This command deletes the symmetric active association with the remote peer.
- 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.
- The command should not be used for b(Broadcast), m(Multicast) or r(Reference clock address 127.127.x.x)
- *ip-address* is the mandatory parameter to be entered in the command while key id is the optional parameter. If key id is not specified, then peering will not be authenticated.

Examples

```
-> ntp peer 172.18.16.112
-> no ntp peer 172.18.16.112
```

Release History

Release 6.4.2; command was introduced.

Related Commands

show ntp peers	Displays current NTP peer association.

MIB Objects

```
alaNtpPeerTable
   alaNtpPeerType
   alaNtpPeerAuth
   alaNtpPeerVersion
   alaNtpPeerMinpoll
```

show ntp status

Displays the information about the current NTP status.

show ntp status

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- This command displays the information about the status of NTP, which is configured along with other global configuration. See the Examples section for more information.
- If the source IP Configuration is done in default or no-loopback0 then the source ip-address will not be displayed in the output of the **show ntp status** command.

Example

```
-> show ntp status
Current time                          : Tue APR 29 2003    18:48:01 (UTC),
Last NTP update                       : Tue APR 29 2003    18:44:15 (UTC),
Server reference:                     : 0.0.0.0,
Client mode                           : enabled,
Broadcast client mode                 : disabled,
Broadcast mode delay (microseconds)   : 4000,
Server qualification                  : synchronized,
Stratum                               : 16,
Max-Associations                      : 32,
Authentication                        : disabled,
Source IP Configuration               : Preferred,
Source IP                             : 10.145.15.15
```

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.

server qualification	Server qualification status.
Stratum	The stratum of the server. The stratum number is the number of hops from a UTC time source.
Max-Association	Maximum association on the switch that restricts the number of client/ server and peer association
Authentication	Whether Authentication is enabled or disabled
Source IP Configuration	Source IP Configuration type which is configured.
Source IP	Source IP address for NTP that send updates to clients.

Release History

Release 6.4.2; command was introduced.

Related Command

ntp client	Enables or disables NTP operation on the switch.
ntp server	Specifies an NTP server from which the switch will receive updates
ntp server synchronized	Enables an NTP client to invoke tests for NTP server synchronization as specified by the NTP protocol.
ntp max-associations	Configures the maximum number of associations on the switch.
ntp master	Specifies the stratum value for unsynchronized switch
ntp broadcast-client	Enables or disables the client's broadcast mode.
show ntp client	Displays information about the current client NTP configuration.
show ntp client server-list	Displays a list of the servers with which the NTP client synchronizes
show ntp server client-list	Displays the basic server information for a specific NTP server or a list of NTP servers

MIB Objects

```
alaNtpPeerListTable
   alaNtpPeerShowOriginateTime
   alaNtpPeerShowTransmitTime
   alaNtpEnable
   alaNtpBroadcastEnable
   alaNtpBroadcastDelay
   alaNtpPeerTests
   alaNtpPeerStratum
   alaNtpPeerTests
   alaNtpAuthenticate
   alaNtpSrcIpConfig
   alaNtpSrcTp
```

show ntp client

Displays information about the current client NTP configuration.

show ntp client

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 16 2005 00:19:02 (UTC)
Last NTP update               : SAT APR 16 2005 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.
Server Qualification	Indicates whether they server must be synchronized or not.

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

Use this command to display tabular information on the current NTP client to server association status.

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
=198.206.181.123   4     0   16     0.000          0.000          0.000
```

output definitions

IP Address	The server IP address. "+" indicates an active peer "-" indicates a pasive peer "=" indicates a client "*" indicates current system peer "^" indicates a broadcast server "`" indicates a broadcast client
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 6.1; command was introduced.

Related Command

ntp client	Enables or disables NTP operation on the switch.

MIB Objects

```
alaNtpPeerListTable
```

show ntp server client-list

Displays the information about the current NTP clients connected to the server.

show ntp server client-list

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use this command to display the tabular information on the current NTP client connected to the server (switch).

Examples

```
-> show ntp server client-list
IP Address           Ver       Key
------------------+-------+----------
172.23.0.201         4          0
10.255.24.121        4          0
```

output definitions

IP Address	The client 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.

Release History

Release 6.4.2; command was introduced.

Related Command

show ntp status	Displays information about the current client NTP configuration
ntp client	Enables or disables NTP operation on the switch.

MIB Objects

```
alaNtpClientListTable
   alaNtpPeerListAddress
   alaNtpPeerVersion
   alaNtpPeerAuth
```

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***]**

Syntax Definitions

ip_address	The IP address of the NTP server to be displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- This command displays information on the status of any or all configured NTP servers/peers.
- To display a specific server, enter the command with the server's IP address. To display all servers, enter the command with no server IP address.

Examples

```
-> show ntp server status
IP address         = 172.18.16.147,
Host mode          = server,
Peer mode          = unspec,
Prefer             = no,
Version            = 4,
Key                = 0,
Stratum            = 16,
Minpoll            = 4 (16 seconds),
Maxpoll            = 10 (1024 seconds),
Delay              = 0.000 seconds,
Offset             = 0.000 seconds,
Dispersion         = 0.000 seconds
Root distance      = 0.000,
Precision          = -6,
Reference IP       = 0.0.0.0,
Status             = not configured,
Uptime count       = 28250 seconds,
Reachability       = 0,
Unreachable count  = 5,
Stats reset count  = 27829 seconds,
Packets sent       = 0,
Packets received   = 0,
Duplicate packets  = 0,
Bogus origin       = 0,
Bad authentication = 0,
Bad dispersion     = 0
```

```
IP address         = 172.18.16.147,
Host mode          = server,
Peer mode          = unspec,
Prefer             = no,
Version            = 4,
Key                = 0,
Stratum            = 16,
Minpoll            = 4 (16 seconds),
Maxpoll            = 10 (1024 seconds),
Delay              = 0.000 seconds,
Offset             = 0.000 seconds,
Dispersion         = 0.000 seconds
Root distance      = 0.000,
Precision          = -6,
Reference IP       = 0.0.0.0,
Status             = not configured,
Uptime count       = 28250 seconds,
Reachability       = 0,
Unreachable count  = 16,
Stats reset count  = 26812 seconds,
Packets sent       = 0,
Packets received   = 0,
Duplicate packets  = 0,
Bogus origin       = 0,
Bad authentication = 0,
Bad dispersion     = 0

-> show ntp server status 198.206.181.139
IP address         = 198.206.181.139,
Host mode          = client,
Peer mode          = server,
Prefer             = no,
Version            = 4,
Key                = 0,
Stratum            = 2,
Minpoll            = 6 (64 seconds),
Maxpoll            = 10 (1024 seconds),
Delay              = 0.016 seconds,
Offset             = -180.232 seconds,
Dispersion         = 7.945 seconds
Root distance      = 0.026,
Precision          = -14,
Reference IP       = 209.81.9.7,
Status             = configured : reachable : rejected,
Uptime count       = 1742 seconds,
Reachability       = 1,
Unreachable count  = 0,
Stats reset count  = 1680 seconds,
Packets sent       = 1,
Packets received   = 1,
Duplicate packets  = 0,
Bogus origin       = 0,
Bad authentication = 0,
Bad dispersion     = 0,
Last Event         = peer changed to reachable,
```

output definitions

IP address	The server IP address.
Host mode	The host mode of this remote association.
Peer mode	The peer mode of this remote association.
Prefer	Whether this server is a preferred server or not. A preferred server is used to synchronize the client before a 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.
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.
Root distance	The total round trip delay (in seconds) to the primary reference source.
Precision	The advertised precision of this association.
Reference IP	The IP address identifying the peer's primary reference source.
Status	The peer selection and association status.
Uptime count	The time period (in seconds) during which the local NTP server was associated with the switch.
Reachability	The reachability status of the peer.
Unreachable count	Number of times the NTP entity was unreachable.
Stats reset count	The time delay (in seconds) since the last time the local NTP server was restarted.
Packets sent	Number of packets sent.
Packets received	Number of packets received.
Duplicate packets	Number of duplicated packets received.
Bogus origin	Number of bogus packets.
Bad authentication	Number of NTP packets rejected for not meeting the authentication standards.
Bad dispersion	Number of bad dispersions.
Last Event	The last event.

Release History

Release 6.1; command was introduced.

Related Command

ntp client	Enables or disables NTP operation on the switch.

MIB Objects

```
alaNtpPeerListTable
   alaNtpPeerShowStatus
```

show ntp keys

Displays information about all authentication keys.

show ntp keys

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

This command displays the information on the current set of trusted authentication keys.

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 6.1; 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
```

show ntp peers

Displays the information about the current status on the NTP peer association.

show ntp peers

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Use this command to display the tabular information on the current NTP peer association status.

Examples

```
-> show ntp peers
IP Address      Ver    Key   St     Delay       Offset          Disp
--------------+------+-----+-----+----------+--------------+--------------
172.23.0.202     4      0    3      0.300       0.404          0.0024
10.255.24.120    4      0    3      0.016       0.250          0.0017
```

output definitions

IP Address	Peer 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 6.4.2; command was introduced.

Related Command

ntp client	Enables or disables NTP operation on the switch.
show ntp status	Displays the information about the current NTP status.
show ntp server status	Displays the basic server information for a specific NTP server or a list of NTP servers.

MIB Objects

```
alaNtpPeerListTable
   alaNtpPeerListAddress
   alaNtpPeerVersion
   alaNtpPeerAuth
   alaNtpPeerStratum
   alaNtpPeerListDelay
   alaNtpPeerShowOffset
   alaNtpPeerListDispersion
```

show ntp server disabled-interfaces

Displays the ip addresses of the interfaces on which NTP server is not enabled.

show ntp server disabled-interfaces

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

This command displays ip interfaces on which currently NTP server functionality is disabled.

Examples

```
-> show ntp server disabled-interfaces
IP Address
--------------
172.23.0.202
10.255.24.120
```

output definitions

IP Address	Peer IP Address

Release History

Release 6.4.2; command was introduced.

Related Command

show ntp status	Displays the information about the current NTP status.
show ntp server status	Displays the basic server information for a specific NTP server or a list of NTP servers.

MIB Objects

```
alaNtpAccessRestrictedTable
   alaNtpPeerListAddress
```

63 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.)

Maximum number of concurrent sessions allowed are:

Session	Maximum Number of Sessions
Telnet(v4 or v6)	4
FTP(v4 or v6)	4
SSH + SFTP(v4 or v6 secure sessions)	8
HTTP	4
Total Sessions	20
SNMP	50

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

Filename: AlcatelIND1Ssh.mib
Module: ALCATEL-IND1-SSH-MIB

A summary of the available commands is listed here:

session login-attempt
session login-timeout
session banner
session timeout
session prompt default
session xon-xoff
prompt
show prefix
alias
show alias
user profile save
user profile save global-profile
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
telnet6
ssh
ssh6
ssh enforce pubkey-auth
show ssh config
show command-log status

session login-attempt

Sets or resets the number of times a user can attempt unsuccessfully to log in to 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

By default, three-login attempts are provided.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

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

Release History

Release 6.1; command 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 WebView), or FTP interface. When the switch detects no user activity for this period, 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 seconds to 600 seconds.

Defaults

Login timeout default is 55 seconds.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

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

Release History

Release 6.1; command 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 in to the switch before the TCP connection is closed.
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, 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 successfully logs on to the switch.

session banner {cli | ftp | http} *file_name*

session banner no {cli | ftp | http}

Syntax Definitions

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

Defaults

- A default banner is included in one of the switch 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 6400, 6855, 6850E, 9000E

Usage Guidelines

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

Examples

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

Release History

Release 6.1; command introduced.
Release 6.1.3; **http** parameter 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, 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 6400, 6855, 6850E, 9000E

Usage Guidelines

- The inactivity timer value can be different for each type of interface, such as 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 6.1; command introduced.
Release 6.1.3; **http** parameter 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 reauth-interval

Configure the re-authentication or refresh time for various services offered by Switch like Console, Telnet, FTP, SSH, HTTP and HTTPS when using the authenticating server as LDAP or TACACS or while doing local authentication.

session reauth-interval {console |telnet |ssh |ftp |http |https |all} { <*minutes*> **|default}**

Syntax Definitions

console	Sets the re-authentication timeout for console sessions.
telnet	Sets the re-authentication timeout for telnet sessions.
ssh	Sets the re-authentication timeout for SSH sessions.
ftp	Sets the re-authentication timeout for FTP sessions
http	Sets the re-authentication timeout for HTTP sessions.
https	Sets the re-authentication timeout for HTTPS sessions.
minutes	Re-authentication timeout value (in minutes).

Defaults

parameter	default
minutes	5

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- The re-authentication timer value can be different for each type of interface, such as console, telnet, SSH, FTP, HTTP, and HTTPS.
- The Refresh mechanism can be disabled by configuring the timer as 0.
- The re-authentication timer can be restored to 5 minutes using “default” for timer value.

Examples

```
-> session reauth-interval all default
-> session reauth-interval ftp 6
-> session reauth-interval ssh 4
-> session reauth-interval telnet 9
-> session reauth-interval http 4
-> session reauth-interval https 4
```

Release History

Release 6.4.5; command 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
   sessionServiceType
   sessionReauthInterval
```

session prompt default

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 {<*num*> **|** <*string*> **| system-name}**

Syntax Definitions

num	The new numerical prompt value.
string	The new prompt string. Text strings that include spaces must be enclosed in quotation marks. For example, **"OmniSwitch 6400"**.
system-name	Sets the prompt to the current system name of the switch. By default, the system name is set to 'VxTarget'. The system name can be up to 256 characters.

Defaults

parameter	default
string	->
system-name	VxTarget

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- The maximum prompt string length is 35 characters.
- System name is configured for the switch using the CLI command **system name**. The system name can also be dynamically obtained from the DHCP server (DHCP Option-12). The user-defined system name configuration (through CLI, WebView, SNMP) gets priority over the DHCP server values. For more information, refer to "system name" on page 60-4 in Chassis Management and Monitoring Commands chapter.
- Every time the system name is modified, the prompt also gets modified.
- The system name can be up to 256 characters. When displayed in the prompt, the system name is truncated at 35 characters.
- The new prompt takes effect after relogging to a new session.
- Use the **show system** command to view the updated system name under the **Name** field.

Examples

```
-> session prompt default
-> session prompt default system-name
-> system-name OmniSwitch6400
```

Release History

Release 6.1; command introduced.
Release 6.1.3; keyword **system name** 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
   sessionDefaultPromptSysName
```

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 6400, 6855, 6850E, 9000E

Usage Guidelines

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

Examples

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

Release History

Release 6.1; command 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	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.

Defaults

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

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the **no** form of this command to remove the CLI prompt.
- 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.
- 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 6.1; command 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 6400, 6855, 6850E, 9000E

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 6.1; command 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 CLI command keywords.

alias *alias* **“***command_name”*

no alias [“*alias*”**]**

Syntax Definitions

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

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Always use double quotes “ “ while using *alias* with the **no** form of this command. If “*alias”* is not mentioned then all user defined aliases for the current session are removed.The **no alias** command removes all configured aliases. The **no alias [**“*alias”***]** command removes the specific alias configuration.
- Alias commands are stored until the user session ends. To save alias settings, use 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 read/write capabilities, you can change the CLI command from **attrib** to privilege.
- To reset commands set with alias back to their factory default, use the **user profile reset** command.

Examples

```
-> alias gp group
-> alias privilege attrib
-> no alias “gp”
-> no alias
```

Release History

Release 6.1; command 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.

MIB Objects

N/A

show alias

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

show alias

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

The following information is displayed 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 6.1; command introduced.

Related Commands

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

MIB Objects

N/A

user profile save

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

user profile save

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

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**, **alias**, **prompt**, and **more size** commands, 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 6.4.5; command introduced.

Related Commands

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

MIB Objects

N/A

user profile save global-profile

This command is available only for the user with an administrative profile.

This command can be used to add alias, prompt, and more settings and these settings can be saved as a global profile. These settings are loaded as default settings when any user logs in, irrespective of the user privileges.

user profile save global-profile

Syntax Definitions

global-profile	The administrative user setting that presets a global setting as default to all users at login prompt.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- This profile can be reset when by the user by using the **user profile save** and **user profile reset** commands.
- Use this command to save alias definitions, prompt definitions, and more mode screen settings for use in future login sessions for all user accounts.
- The current settings (prompt, more, aliases) for the session are saved in the global profile file **/flash/switch/GlobalProfile.txt**. The file can be manually edited by the administrator. The file name must not be changed or deleted.
- If a user profile is configured by the individual user with the **user profile save** command, the global profile is overridden and the user profile settings are loaded at user login.

Examples

```
-> user profile save global-profile

Setting global profile…
```

Release History

Release 6.4.5; command introduced.

Related Commands

alias	Defines substitute command text for the switch CLI command keywords.
prompt	Defines substitute command text for the switch CLI command keywords.
more size	Specifies the number of lines that your console screen must display.
user profile save	Saves the user account settings for aliases, prompts, and the more mode screen settings. These settings are automatically loaded when the user logs on.
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 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> user profile reset
```

Release History

Release 6.1; command introduced.

Related Commands

alias	Defines substitute command text for the switch CLI command keywords.
prompt	Defines substitute command text for the switch CLI command keywords.
more size	Specifies the number of lines that your console screen must 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 to be stored in the CLI history buffer.

history size *number*

Syntax Definitions

number	Enter an integer between 1 and 500. The history buffer can store up to 500 commands.

Defaults

By default, the history buffer size is set to 100 commands.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> history size 10
```

Release History

Release 6.1; command introduced.

Related Commands

show history	Displays commands that 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 that 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 6400, 6855, 6850E, 9000E

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 6.1; command introduced.

Related Commands

history size	Sets the number of commands to be stored in the CLI 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 6400, 6855, 6850E, 9000E

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, press the Enter key to run 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 6.1; command introduced.

Related Commands

history size	Sets the number of commands to be stored in the CLI 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. 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 **/flash** directory. Any configuration commands entered on the command line are 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 6400, 6855, 6850E, 9000E

Usage Guidelines

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

Examples

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

Release History

Release 6.1; command introduced.

Related Commands

show ssh config	Displays the contents of the **command.log** file.
show command-log status	Shows the status of the command logging function (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 6400, 6855, 6850E, 9000E

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 6.1; command introduced.

Related Commands

who	Displays all active login sessions (for example, Console, Telnet, FTP, HTTP, Secure Shell, and Secure Shell FTP).

MIB Objects

```
SessionMgr
   sessionIndex
   sessionRowStatus
```

exit

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

exit

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

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 6.1; command 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 6400, 6855, 6850E, 9000E

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	The 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 read-only access. See the table beginning on page 63-33 for a listing of valid domains.
Read-only families	The command families available with the user read-only access. See the table beginning on page 63-33 for a listing of valid families.
Read-Write domains	The command domains available with the user read-write access. See the table beginning on page 63-33 for a listing of valid domains.

output definitions

Read-Write families	The command families available with the user read-write access. See the table beginning on page 63-33 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 iprm ipmr ipms
domain-layer2	vlan bridge stp 802.1q linkagg ip-helper
domain-service	ldap dhcp dns
domain-security	session binding aaa

Release History

Release 6.1; command introduced.

Related Commands

who	Displays all active login sessions (for example, Console, Telnet, FTP, HTTP, Secure Shell, and Secure Shell FTP).
kill	Kills another user session.

MIB Objects

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

who

Displays all active login sessions (for example, Console, Telnet, FTP, HTTP, Secure Shell, and Secure Shell FTP).

who

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

You can identify your current login session by using 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	The user name.
Access type	Type of access protocol used to connect to the switch.

output definitions (continued)

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 read-only access. See the table beginning on page 63-36 for a listing of valid domains.
Read-only families	The command families available with the user read-only access. See the table beginning on page 63-36 for a listing of valid families.
Read-Write domains	The command domains available with the user read-write access. See the table beginning on page 63-36 for a listing of valid domains.
Read-Write families	The command families available with the user read-write access. See the table beginning on page 63-36 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 iprm ipmr ipms
domain-layer2	vlan bridge stp 802.1q linkagg ip-helper
domain-service	ldap dhcp dns
domain-security	session binding avlan aaa

Release History

Release 6.1; command introduced.

Related Commands

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

MIB Objects

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

show session config

Displays session manager configuration information (for example, default prompt, banner file name, inactivity timer, login timer, and login attempts).

show session config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- Use the configuration commands detailed in this section to modify any of the values displayed.
- Re-authentication or refresh authentication refers to refreshing the user sessions with stored user credentials.

Examples

```
-> show session config

Cli Default Prompt = 172.25.50.61->,
Cli Banner File Name = ,
Cli Inactivity Timer in minutes = 555555,
Ftp Banner File Name = ,
Ftp Inactivity Timer in minutes = 4,
Http Inactivity Timer in minutes = 4,
Http Banner File Name = ,
Login Timer in seconds = 55,
Maximum number of Login Attempts = 3,
Default Reauth Interval = 5,
Console Reauth-Interval = 6,
Telnet Reauth-Interval = 6,
SSH Reauth-Interval = 6,
FTP Reauth-Interval = 6,
HTTP Reauth-Interval = 6,
HTTPS Reauth-Interval = 6
```

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 appears during a CLI session.

output definitions (continued)

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 appears 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.
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 in to the switch before the TCP connection is closed.
Default Reauth-Interval	The default authentication refresh period for the session. Reauth-interval of 0 indicates re-authentication disabled for that session
Console Reauth-Interval	The console authentication refresh period for the session.
Telnet Reauth-Interval	The telnet authentication refresh period for the session.
SSH Reauth-Interval	The SSH authentication refresh period for the session.
FTP Reauth-Interval	The FTP authentication refresh period for the session.
HTTP Reauth-Interval	The HTTP authentication refresh period for the session.
HTTPS Reauth-Interval	The HTTPS authentication refresh period for the session.

Release History

Release 6.1; command introduced.

Related Commands

session prompt default	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 WebView), or FTP interface.
session login-attempt	Sets the number of times a user can attempt to log in to the switch unsuccessfully 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 6400, 6855, 6850E, 9000E

Usage Guidelines

The switch can 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 can be stopped.

Examples

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

Release History

Release 6.1; command 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 must display.

more size *lines*

Syntax Definitions

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

Defaults

parameter	default
lines	128

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- If the display from the switch contains more lines than specified with this command, the switch displays only the number of lines specified. The last line on your console displays 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 6.1; command 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 6400, 6855, 6850E, 9000E

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 6.1; command introduced.

Related Commands

show more	Shows the number of TTY lines and columns to be displayed.
more size	Specifies the number of lines that your console screen must 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 6400, 6855, 6850E, 9000E

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 6.1; command introduced.

Related Commands

more	Enables the more mode for your console screen display.
more size	Specifies the number of lines that your console screen must 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 6400, 6855, 6850E, 9000E

Usage Guidelines

- To abort a Telnet session, enter **CTRL** + **]** and then **CTRL** + **D**. Refer to your switch User Manual for more information on using Telnet.
- You can establish up to five concurrent IPv4 or IPv6 telnet client sessions.
- You can establish up to four concurrent IPv4 or IPv6 telnet sessions (when the switch acts as a telnet server).

Examples

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

Release History

Release 6.1; command introduced.

Related Commands

telnet6	Invokes a Telnetv6 session. A Telnetv6 session is used to connect to a remote system or device over an IPv6 network
ssh	Invokes the Secure Shell on the switch. A Secure Shell is used to make a secured connection to a remote system or device.

MIB Objects

```
SystemServices
   systemServicesArg1
   systemServicesAction
```

telnet6

Invokes a Telnetv6 session. A Telnetv6 session is used to connect to a remote system or device over an IPv6 network.

telnet6 {*ipv6_address* | *hostname***} [***if_name***]**

Syntax Definitions

ipv6_address	Specifies the IPv6 address for the Telnetv6 server.
hostname	Specifies the hostname for the Telnetv6 server.
if_name	The name of the interface used to reach the Telnetv6 server, if the target has been specified using the link-local address.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- To abort a Telnet session, enter **CTRL** + **]** and then **CTRL** + **D**. Refer to your switch-specific User Manual for more information on using Telnet.
- If the session is invoked using the server link-local address, the source interface name must be provided.
- You can establish up to five concurrent IPv4 or IPv6 telnet client sessions.
- You can establish up to four concurrent IPv4 or IPv6 telnet sessions (when the switch acts as a telnet server).

Examples

```
-> telnet6 fe80::a00:20ff:fea8:8961 intf1
-> telnet6 ::1
-> telnet6 Sun.com
```

Release History

Release 6.3.1; command introduced.

Related Commands

telnet	Invokes a Telnet session. A Telnet session is used to connect to a remote system or device.
ssh6	Invokes Secure Shellv6 on the switch. Secure Shellv6 is used to make a secured connection to an SSHv6 server.

MIB Objects

```
SystemServices
   systemServicesArg1
   systemServicesAction
```

ssh

Invokes Secure Shell on the switch. Secure Shell is used to make a secured connection to a remote system or device.

ssh {*host_name* **|** *ip_address* | **enable** | **disable}**

Syntax Definitions

host_name	Specifies the host name for Secure Shell.
ip_address	Specifies the IP address for Secure Shell.
enable	Administratively enables Secure Shell on the switch.
disable	Administratively disables Secure Shell on the switch.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- You must have a valid username and password for the specified host.
- You can establish one SSH session from an OmniSwitch (when it acts as Client) and up to eight SSH sessions towards an OmniSwitch (when it acts as Server).

Examples

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

Release History

Release 6.3.1; command 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.
ssh6	Invokes Secure Shellv6 on the switch. Secure Shellv6 is used to make a secured connection to an SSHv6 server.
show ssh config	Displays the status of Secure Shell, SCP/SFTP on the switch.

MIB Objects

```
aaaAcctSATable
   aaacsInterface
alaSshConfigGroup
   alaSshAdminStatus
```

ssh6

Invokes Secure Shellv6 on the switch. Secure Shellv6 is used to make a secured connection to an SSHv6 server.

ssh6 {*ipv6_address* | *hostname***} [***if_name***]**

Syntax Definitions

ipv6_address	Specifies the IPv6 address for Secure Shell.
hostname	Specifies the host name for Secure Shell.
if_name	The name of the interface used to reach the sshv6 server, if the target has been specified using the link-local address.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- You must have a valid username and password for the specified host.
- If the session is invoked using the server link-local address, the source interface name must be provided.
- You can establish one SSH6 session from an OmniSwitch (when it acts as Client) and up to eight SSH6 sessions towards an OmniSwitch (when it acts as Server).
- A console or a telnet session can handle only one SSHv6 client session
- At anytime, there can be only one SSH client session (either SSHv4 or SSHv6) to any SSH server.

Examples

```
-> ssh6 fe80::a00:20ff:fea8:8961 int1
-> ssh6 ::1
-> ssh6 Sun.com
```

Release History

Release 6.3.1; command introduced.

Related Commands

telnet6	Invokes a Telnetv6 session. A Telnetv6 session is used to connect to a remote system or device over an IPv6 network
sftp6	Starts an SFTPv6 session. An SFTPv6 session provides a secure file transfer method.
ssh	Invokes Secure Shell on the switch. Secure Shell is used to make a secured connection to a remote system or device.
show ssh config	Displays the status of Secure Shell, SCP/SFTP on the switch.

MIB Objects

```
aaaAcctSATable
   aaacsInterface
alaSshConfigGroup
   alaSshAdminStatus
```

ssh enforce pubkey-auth

Enables or disables Secure Shell public key and password authentication. When enabled, password authentication is not allowed.

ssh enforce pubkey-auth {enable | disable}

Syntax Definitions

enable	Enforces only SSH public key authentication.
disable	Enforces both SSH public key and password authentication.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

If a public key file (**thomas_dsa.pub**) exists in the **flash/network/pub** directory on the switch, public key authentication is used even if this method of authentication is disabled using this command. Rename, move, or delete the public key file to ensure that public key authentication is disabled.

Examples

```
-> ssh enforce pubkey-auth enable
```

Release History

Release 6.1; command 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

```
alaSshConfigGroup
   alaSshPubKeyEnforceAdminStatus
```

show ssh config

Displays the status of Secure Shell, SCP/SFTP on the switch.

show ssh config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

```
-> show ssh config
SSH = Enabled
SCP/SFTP = Enabled
Public Key Authentication Enforced = False
```

output definitions

SSH	Displays the SSH status (**enabled** or **disabled**).
SCP/SFTP	Displays the SCP/SFTP status (**enabled** or **disabled**).
Public Key Authentication Enforced	Displays whether the Public Key Authentication is enforced. Options include **true** or **false**.

Release History

Release 6.1; command introduced.

Related Commands

ssh	Invokes Secure Shell on the switch. Secure Shell is used to make a secured connection to a remote system or device.
ftp6	Enables or disables secure copy (SCP) and secure FTP (SFTP) at the same time on the switch.

MIB Objects

```
alaSshConfigGroup
   alaSshAdminStatus
   alaScpSftpAdminStatus
   alaSshPubKeyEnforceAdminStatus
```

show command-log

Displays the contents of the **command.log** file. This file contains a record of all CLI commands run on the switch since the command logging function was enabled. For more information on enabling and disabling command logging, refer to page 63-29.

show command-log

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

- The **show command-log** command lists the CLI commands in the *descending order*. In other words, the most recent commands are listed first. In the following example, 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.
- Command history is archived to the **command.log** file. If this file is removed, the command history is no longer 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 are displayed.

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 page, or the "Managing Switch User Accounts" chapter in the *OmniSwitch 6250/6450 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 6.1; command introduced.

Related Commands

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

MIB Objects

```
sessionCliCommandLogEnable
```

show command-log status

Shows the status of the command logging function (enabled or disabled). For more information on enabling and disabling command logging, refer to the **command-log** command on page 63-29.

show command-log status

Syntax Definitions

N/A

Defaults

Command logging is disabled by default.

Platforms Supported

OmniSwitch 6400, 6855, 6850E, 9000E

Usage Guidelines

N/A

Examples

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

output definitions

CLI command logging	The 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 through the **command-log** command. For more information, refer to page 63-29.

Release History

Release 6.1; command introduced.

Related Commands

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

MIB Objects

```
sessionCliCommandLogStatus
```

64 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 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

Filename: AlcatelIND1Ssh.mib
Module: ALCATEL-IND1-SSH-MIB

A summary of the available commands is listed here:

File System	**cd** **pwd** **mkdir** **rmdir** **ls** **dir** **rename** **rm** **delete** **cp** **scp** **mv** **move** **chmod** **attrib** **freespace** **fsck** **newfs** **rcp** **rrm** **rls**
System Services	**vi** **view** **tty** **show tty** **more** **ftp** **ftp6** **scp-sftp** **show ssh config** **sftp** **sftp6** **tftp** **rz**

cd

Changes the switch current working directory.

cd [*path***]**

Syntax Definitions

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

Defaults

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

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 6.1; command was introduced.

Related Commands

pwd	Displays the switch 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 current working directory.

pwd

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

This command can also be used on the secondary CMM.

Examples

```
-> pwd
/flash
```

Release History

Release 6.1; command was introduced.

Related Commands

cd	Changes the switch 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-defined name for the new directory. Up to thirty-two (32) characters may be used (e.g., **test_directory**).

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 6.1; command was introduced.

Related Commands

cd	Changes the switch current working directory.
pwd	Displays the switch 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 6400, 6850E, 6855, 9000E

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 6.1; command was introduced.

Related Commands

cd	Changes the switch current working directory.
pwd	Displays the switch 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 6400, 6850E, 6855, 9000E

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 6.1; command was introduced.

Related Commands

cd	Changes the switch current working directory.
pwd	Displays the switch 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 6400, 6850E, 6855, 9000E

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 Jul  8 11:05 ./
drw      2048 Aug 21 13:54 ../
-rw   3555538 Jul  5 09:37 Jeni.img
-rw   1824898 Jul  5 09:37 Jos.img
-rw      2929 Jul  5 09:37 Jrelease.img
-rw  10526922 Jul  5 09:37 Jbase.img
-rw   9393680 Jun 10 10:35 Jeni2.img
-rw      1452 Jun 28 18:23 boot.cfg
-rw   1348241 Jul  5 09:36 Jadvrout.img
-rw   2478362 Jul  5 09:37 Jdiag.img
-rw    349555 Jul  5 09:37 Jsecu.img
-rw       256 Jul  8 11:05 random-seed

        2390016 bytes free
```

Release History

Release 6.1; command was introduced.

Related Commands

cd	Changes the switch current working directory.
pwd	Displays the switch 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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.
orig_filename	The name of the existing file to be copied.
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.
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 6400, 6850E, 6855, 9000E

Usage Guidelines

- You should verify that your switch **/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 6.1; command was introduced.

Related Commands

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

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesArg2
   systemServicesAction
```

scp

Copies an existing file in a secure manner.

scp *user_name@remote_ip_addr:***[***path/***]***source* **[***path/***]***target*

scp [*path/***]***source user_name@remote_ip_addr:***[***path/***]***target*

Syntax Definitions

user_name@remote_ip_addr:	The username along with the IP address of the remote switch.
path/	Specifies the path containing the file to be copied and the path where the file will be copied.
source	The name of the file(s) to be copied.
target	The new user-defined file name for the resulting file copy. Up to thirty-two (32) characters may be used.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- This command will prompt you to enter the admin password, and the names and the path of the files being copied will be displayed.
- 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 (_).
- If SCP is not enabled, use the **scp-sftp** command to enable it.

Examples

```
-> scp admin@172.17.11.13:/flash/working/Kos.img /flash/working/Kos.img
admin's password for keyboard-interactive method:

Fetching /flash/working/Kos.img to /flash/working/Kos.img
Connection to 172.17.11.13 closed.

-> scp /flash/working/Kos.img admin@172.17.11.13:/flash/working/Kos.img
admin's password for keyboard-interactive method:

Uploading /flash/working/Kos.img to /flash/working/Kos.img
Connection to 172.17.11.13 closed.

-> scp admin@172.17.11.13:/flash/working/*.img /flash/working
admin's password for keyboard-interactive method:

Fetching /flash/working/K2os.img to /flash/working/K2os.img
Fetching /flash/working/Kadvrout.img to /flash/working/Kadvrout.img
Fetching /flash/working/Kbase.img to /flash/working/Kbase.img
Fetching /flash/working/Keni.img to /flash/working/Keni.img
Fetching /flash/working/Kos.img to /flash/working/Kos.img
Fetching /flash/working/Krelease.img to /flash/working/Krelease.img
Fetching /flash/working/Ksecu.img to /flash/working/Ksecu.img
Connection to 172.17.11.13 closed.
```

Release History

Release 6.1.2; command was introduced.

Related Commands

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

MIB Objects

N/A

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 6400, 6850E, 6855, 9000E

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 64-19.
- 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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

Examples

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

-> freespace
/flash 3143680 bytes free
```

Release History

Release 6.1; command was introduced.

Related Commands

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.

MIB Objects

```
SystemFileSystemTable
   systemFileSystemFreespace
```

fsck

Performs a file system check, including diagnostic information in the event of file corruption.

fsck /flash [no-repair | repair]

Syntax Definitions

/flash	Indicates that the file system check will be performed on the **/flash** directory.
no-repair	Performs only the file system check on the /**flash** directory.
repair	Performs file system check on the /**flash** directory and also repairs any errors found on the file system.

Defaults

parameter	default
no-repair | repair	**no-repair**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The file system check is performed on the **/flash** directory by default.
- Specifying the parameter **repair** along with the command performs the file system check and also repairs any errors found.The switch will display the errors found and specify those errors that have been repaired. If there are no errors found, then just the file system information is displayed.
- This command only applies to the primary and secondary CMM in an OmniSwitch chassis-based switch or the primary and secondary switch in an OmniSwitch stack.

Examples

```
-> fsck /flash no-repair
/flash/  - disk check in progress ...
/flash/  - Volume is OK

          total # of clusters:  29,758
           # of free clusters:  18,886
            # of bad clusters:  0
              total free space:  77,357,056
    max contiguous free space:  55,451,648 bytes
                   # of files:  59
                 # of folders:  5
          total bytes in files:  44,357,695
              # of lost chains:  0
   total bytes in lost chains:  0
```

```
(Example Continued on Next Page)
-> fsck /flash repair
/flash/  - disk check in progress ...
/flash/  - Volume is OK
Change volume Id from 0x0 to 0xef2e3c

          total # of clusters:  29,758
           # of free clusters:  18,886
            # of bad clusters:  0
             total free space:  77,357,056
    max contiguous free space:  55,451,648 bytes
                  # of files:  59
                # of folders:  5
         total bytes in files:  44,357,695
             # of lost chains:  0
   total bytes in lost chains:  0
```

Release History

Release 6.1; command was introduced.
Release 6.3.3; **no-repair** and **repair** parameters added.

Related Commands

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

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesAction
```

newfs

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

newfs {/flash | /uflash}

Syntax Definitions

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

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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
-> newfs /uflash
```

Release History

Release 6.1; command was introduced.
Release 6.4.3; /**uflash** parameter was added.

Related Commands

N/A

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesAction
```

rcp

Copies a file from a primary to a non-primary switch in a stack and vice versa.

rcp [cmm-b: | *slot***:**] *source_filepath* [**cmm-b:** | *slot***:**] *destination_filepath*

Syntax Definitions

slot	The slot number of the non-primary switch in a stack.
source_filepath	The name and path of the source file.
destination_filepath	The name and path of the destination file.
cmm-b:	Specifies the secondary CMM. This parameter is available on OmniSwitch chassis-based switches only.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855-U24X, 9000E

Usage Guidelines

- On OmniSwitch chassis-based switches this command copies any file from the secondary CMM to the primary CMM.
- On OmniSwitch stackable switches this command copies a file from any non-primary switch to the primary switch in a stack. You must specify the slot number on these switches.

Examples

```
-> rcp 3:/flash/file.txt file.txt
-> rcp /flash/working/file.txt 3:/flash/working/file.txt
-> rcp cmm-b:/flash/file.txt file.txt

-> rcp /flash/working/file.txt cmm-b:/flash/working/file.txt
```

Release History

Release 6.1; command was introduced.

Related Commands

rrm	Removes a file 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 secondary CMM in a switch 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.
filepath	The name and path of the file to be deleted.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855-U24X, 9000E

Usage Guidelines

- On OmniSwitch chassis-based switches this command deletes any file from the secondary CMM.
- On OmniSwitch stackable switches this command deletes a file from any non-primary switch. You must specify the slot number on these switches.

Examples

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

Release History

Release 6.1; command was introduced.

Related Commands

rcp	Copies a file from a secondary CMM to a primary CMMor 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 anon-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 required on a stack of switches*.
directory	The name of the directory on the non-primary CMM or switch.
file_name	The file to be displayed on the non-primary CMM or switch.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855-U24X, 9000E

Usage Guidelines

- On OmniSwitch chassis-based switches this command displays directory content on the secondary CMM.
- On OmniSwitch stackable 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 6850E Series 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 6.1; 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 secondary CMM or from a non-primary switch in a stack.

MIB Objects

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

vi

Launches the switch 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 6400, 6850E, 6855, 9000E

Usage Guidelines

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

Examples

```
-> vi test_config_file
```

Release History

Release 6.1; command was introduced.

Related Commands

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 6400, 6850E, 6855, 9000E

Usage Guidelines

This command can also be used on the secondary CMM.

Examples

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

Release History

Release 6.1; command was introduced.

Related Commands

vi	Launches the switch 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- You must have a valid username and password for the specified host.
- You can establish up to 9 FTP sessions from an OmniSwitch (when it acts as FTP Client) and up to 4 FTP sessions towards an OmniSwitch (when it acts as FTP Server).
- 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 6.1; command was introduced.

Related Commands

sftp	Starts an SFTP session.
ftp6	Starts an FTPv6 session.

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesAction
```

ftp6

Starts an FTPv6 session.

ftp6 {*ipv6_address* | *hostname***} [***if_name***]**

Syntax Definitions

ipv6_address	Specifies the IPv6 address of the FTPv6 server.
hostname	Specifies the hostname of the FTPv6 server.
if_name	The name of the interface used to reach the FTPv6 server, if the target has been specified using the link-local address.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- You must have a valid username and password for the specified host.
- A console, a telnet or an SSH session can handle only one FTPv6 client session.
- You can establish upto 9 FTP or FTPv6 sessions from an OmniSwitch (when it acts as FTP Client) and upto 4 FTP or FTPv6 sessions towards an OmniSwitch (when it acts as FTP Server).
- If the session is invoked using the server link-local address, the source interface name must be provided.
- After logging in, FTPv6 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.
close	Terminate the ftp session.
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.)
help	Display list of available FTP commands.
lcd	Change to a new directory on the local machine.

ls	Display summary listing of the current directory on the remote host.
?	Display list of available FTP commands.
mgets	Receive multiple files.
mputs	Receive multiple files.
prompt	Enable/disable interactive prompting.
put	Send a file to the remote machine.
pwd	Print current working directory.
quit	Close session gracefully.
remotehelp	List the commands that the remote FTP server supports.
user	Send new user information.
ls	Display list content of local directory.

Examples

```
-> ftp6 fe80::a00:20ff:fea8:8961 int3
-> ftp6 ::5
-> ftp6 Sun.com
```

Release History

Release 6.3.1; command was introduced.

Related Commands

sftp6	Starts an SFTPv6 session.
ftp	Starts an FTP session.

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesAction
```

scp-sftp

Enables or disables secure copy (SCP) and Secure FTP (SFTP) at the same time on the switch.

scp-sftp {enable | disable}

Syntax Definitions

enable	Administratively enables SCP/SFTP on the switch.
disable	Administratively disables SCP/SFTP on the switch.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> scp-sftp enable
```

Release History

Release 6.1.3; command was introduced.

Related Commands

ssh	Invokes Secure Shell on the switch. Secure Shell is used to make a secured connection to a remote system or device.
show ssh config	Displays the status of Secure Shell, SCP/SFTP on the switch.

MIB Objects

```
alaSshConfigGroup
   alaScpSftpAdminStatus
```

show ssh config

Displays the status of Secure Shell, SCP/SFTP on the switch.

show ssh config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show ssh config
SSH = Enabled
SCP/SFTP = Enabled
Public Key Authentication Enforced = False
```

output definitions

SSH	Displays the SSH status (**enabled** or **disabled**).
SCP/SFTP	Displays the SCP/SFTP status (**enabled** or **disabled**).
Public Key Authentication Enforced	Displays whether the Public Key Authentication is enforced. Options include **true** or **false**.

Release History

Release 6.1.3; command was introduced.

Related Commands

ssh	Invokes Secure Shell on the switch. Secure Shell is used to make a secured connection to a remote system or device.
ftp6	Enables or disables secure copy (SCP) and secure FTP (SFTP) at the same time on the switch.

MIB Objects

```
alaSshConfigGroup
   alaSshAdminStatus
   alaScpSftpAdminStatus
   alaSshPubKeyEnforceAdminStatus
```

sftp

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

sftp {*host_name* | *ip_address***}**

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 6400, 6850E, 6855, 9000E

Usage Guidelines

- You must have a valid username and a password for the specified host.
- If SFTP is not enabled, use the **scp-sftp** command to enable it.
- You can establish up to 4 SFTP sessions from an OmniSwitch (when it acts as FTP Client) and up to 8 SFTP sessions towards an OmniSwitch (when it acts as FTP Server).
- 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 6.1; command was introduced.

Related Commands

ftp	Starts an FTP session.
ssh	Invokes Secure Shell on the switch. Secure Shell is used to make a secured connection to a remote system or device.

MIB Objects

N/A

sftp6

Starts an SFTPv6 session. An SFTPv6 session provides a secure file transfer method.

sftp6 {*host_name* **|** *ipv6_address***} [***if_name***]**

Syntax Definitions

host_name	Specifies the host name for the SFTPv6 session.
ipv6_address	Specifies the IPv6 address for the SFTPv6 session.
if_name	The name of the interface used to reach the SFTPv6 server, if the target has been specified using the link-local address.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- You must have a valid username and a password for the specified host.
- A console or a telnet session can handle only one SSHv6 client session.
- If the session is invoked using the server link-local address, the source interface name must be provided.
- You can establish up to 4 SFTP6 sessions from an OmniSwitch (when it acts as FTP Client) and up to 8 SFTP6 sessions towards an OmniSwitch (when it acts as FTP Server).
- At anytime, there can be only 4 SFTP sessions (including SFTPv4 or SFTPv6) to any SSH servers.
- After logging in, SFTPv6 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

```
-> sftp6 fe80::a00:20ff:fea8:8961 int1
-> sftp6 ::1
-> sftp6 Sun.com
```

Release History

Release 6.3.1; command was introduced.

Related Commands

ftp6	Starts an FTP6 session.
ssh6	Invokes Secure Shellv6 on the switch. Secure Shellv6 is used to make a secured connection to an SSHv6 server.

MIB Objects

```
SystemServices
   systemServicesArg1
   systemServicesAction
```

tftp

Starts a TFTP client session that enables a file transfer to an TFTP server.

tftp {*host_name* **|** *ip_address***} {get | put} source-file [***src_path*/**]***src_file* **[destination-file [***dest_path*/**]** *dest_file***] [ascii]**

Syntax Definitions

host_name	Specifies the hostname of the TFTP server.
ip_address	Specifies the IP address of the TFTP server.
get	Specifies to download the file from the TFTP server.
put	Specifies to upload the file to the TFTP server.
src_path	Specifies the path containing the source file to be transferred.
src_file	Specifies the file name of the source file to be transferred.
dest_path	Specifies the destination path of the file to be transferred.
dest_file	Specifies the destination file name of the file to be transferred.
ascii	Sets the transfer type to ASCII (7-bit).

Defaults

- If a path is not specified with the filename, the current path is used by default (for example, /flash).
- If a destination filename is not specified, the source filename is used by default.
- The default file transfer mode for a TFTP client session is Binary mode.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- The OmniSwitch supports TFTP client functionality only.
- A TFTP server has no provisions for user authentication.
- Only one active TFTP client session is allowed at a time.
- When downloading a file to the switch, the file size must not exceed the available flash space.

Examples

```
-> tftp tftp.server.com get source-file abc.img destination-file xyz.img
-> tftp tftp.server.com put source-file abc.txt destination-file xyz.txt ascii
-> tftp 10.211.17.1 get source-file boot.cfg destination-file /flash/working/
boot.cfg ascii
-> tftp 10.211.17.1 get source-file boot.cfg ascii
```

Release History

Release 6.3.3; command was introduced.

Related Commands

N/A

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesArg2
   systemServicesArg3
   systemServicesArg4
   systemServicesArg5
   systemServicesAction
```

rz

Starts a Zmodem session.

rz

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 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 6.1; command was introduced.

Related Commands

N/A

MIB Objects

```
systemServices
   systemServicesAction
```

65 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
http port
https port
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 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the **no** form of this 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 6.1; command was introduced.

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 6400, 6850E, 6855, 9000E

Usage Guidelines

Use the **no** form of this command to disable SSL.

Examples

```
-> http ssl
-> no http ssl
-> https ssl
-> no https ssl
```

Release History

Release 6.1; command was introduced.

Related Commands

http server	Enables/disables web management on the switch.
show http	Displays web management configuration information.

MIB Objects

```
alaIND1WebMgtConfigMIBGroup
   alaInd1WebMgtSsl
```

http port

Changes the port number for the embedded Web server in the switch.

[ip] http port {default | *port***}**

Syntax Definitions

ip	Optional syntax.
default	Restores the port to its default (80) value.
port	The desired port number for the embedded Web server. The number must be in the range 0 to 65535; well-known port numbers cannot be configured.

Defaults

parameter	default
port	80

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

All WebView sessions must be terminated before entering this command.

Examples

```
-> http port 1025
-> http port default
```

Release History

Release 6.1; command was introduced.

Related Commands

http server	Enables/disables web management on the switch.
show http	Displays web management configuration information.

MIB Objects

```
alaIND1WebMgtConfigMIBGroup
   alaIND1WebMgtHttpPort
```

https port

Changes the default secure HTTP (HTTPS) port for the embedded Web server.

https port {default | *port***}**

Syntax Definitions

default	Restores the port to its default (443) value.
port	The desired HTTPS port number. The number must be in the range 0 to 65535; well-known port numbers cannot be configured.

Defaults

parameter	default
port	443

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

All WebView sessions must be terminated before entering this command.

Examples

```
-> https port 1026
-> https port default
```

Release History

Release 6.1; command was introduced.

Related Commands

http server	Enables/disables web management on the switch.
show http	Displays web management configuration information.

MIB Objects

```
alaIND1WebMgtConfigMIBGroup
   alaIND1WebMgtHttpsPort
```

debug http sessiondb

Displays web management session information.

debug http sessiondb

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; command was introduced.

Related Commands

http server	Enables/disables web management on the switch.
http ssl	Enables/disables SSL on the switch.
http port	Changes the port number for the embedded Web server in the switch.
https port	Changes the default secure HTTP (HTTPS) port for the embedded Web server.

MIB Objects

```
alaIND1WebMgtConfigMIBGroup
   alaInd1WebMgtAdminStatus
   alaInd1WebMgtSsl
   alaInd1WebMgtHttpPort
   alaInd1WebMgtHttpsPort
```

66 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 (for example, **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 console as each command in the configuration file is applied.

Defaults

By default, **verbose** error checking is not performed.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 (for example, **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 by using the **password** command at the command prompt. For more information on passwords, refer to page 41-62.

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 6.1; command 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 **/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 6400, 6850E, 6855, 9000E

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 6.1; command 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- A timer session can be scheduled using the **configuration apply** command. For more information, refer to page 66-2.
- 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 6.1; command 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.
configuration error-file limit	Specifies the maximum number of configuration error files allowed in the switch **/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 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> configuration cancel
```

Release History

Release 6.1; command 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 6400, 6850E, 6855, 9000E

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 (for example, **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 6.1; command 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 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	**ipmr**	**rdp**
aaa	**ipms**	**rip**
aip	**ipx**	**ripng**
all	**ipv6**	**session**
bgp	**linkagg**	**slb**
bridge	**module**	**snmp**
chassis	**ntp**	**stp**
health	**ospf**	**system**
interface	**ospf3**	**vlan**
ip	**pmm**	**vrrp**
ip-helper	**policy**	**webmgt**
ip-routing	**qos**	**udld**
netsec		

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 **/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 6400, 6850E, 6855, 9000E

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 6.1; command 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 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-supported features		
802.1q	**ipmr**	**rdp**
aaa	**ipms**	**rip**
aip	**ipx**	**ripng**
all	**ipv6**	**session**
bgp	**linkagg**	**slb**
bridge	**module**	**snmp**
chassis	**ntp**	**stp**
health	**ospf**	**system**
interface	**ospf3**	**vlan**
ip	**pmm**	**vrrp**
ip-helper	**policy**	**webmgt**
ip-routing	**qos**	**udld**
netsec		

Defaults

By default, this command shows configuration information for *all* features.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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
```

(output for tacacs-server when command-authorization is enabled)

```
-> show configuration snapshot aaa

! AAA :
aaa tacacs+-server "tacacs" host 172.19.21.2  key "" port 49 timeout 2
aaa authentication console "local"
aaa authentication telnet "tacacs"
aaa authentication ftp "local"
aaa authentication ssh "local"
aaa tacacs command-authorization "enabled"
! PARTM :
! AVLAN :
! 802.1x :
```

(output with 802.1x, Captive portal, and Kerberos snooping configuration information for AAA)

```
-> show configuration snapshot aaa
! AAA :
aaa authentication default "local"
aaa authentication console "local"
aaa authentication http "local"
! PARTM :
! AVLAN :
! 802.1x :
802.1x 1/26 direction both port-control auto quiet-period 60 tx-period 30 supp-t
imeout 30 server-timeout 30 max-req 2 re-authperiod 3600 no reauthentication
802.1x 1/26 captive-portal session-limit 12 retry-count 3
802.1x 1/26 captive-portal inactivity-logout disable
802.1x 1/26 kerberos enable
802.1x 1/26 supp-polling retry 2
802.1x 1/26 supplicant policy authentication pass group-mobility default-vlan fa
il block
802.1x 1/26 non-supplicant policy block
802.1x 1/26 captive-portal policy authentication pass default-vlan fail block
! KERBEROS :
aaa kerberos mac-move disable
aaa kerberos ip-address 10.10.10.1 udp-port 1000

-> 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 6.1; command introduced.

Related Commands

write terminal	Displays the switch 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 current running configuration for all features.

write terminal

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 6.1; command introduced.

Related Commands

show configuration snapshot	Displays the switch current running configuration for all features or for the specified feature(s).

MIB Objects

```
configManager
   mib_configSnapshotAllSelect
```

67 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 trap 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 trap commands set includes show commands for monitoring SNMP trap information.
- SNMP agent commands configure SNMP security levels on the switch. Also includes show commands for monitoring the current SNMP security status.

MIB information for SNMP Community commands is as 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** **snmp source ip preferred** **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 object commands	**show snmp object**

snmp station

Adds a new SNMP station; modifies or deletes an existing SNMP station.

snmp station {*ip_address* **|** *ipv6_address***} {[***udp_port***] [***username***] [v1 | v2 | v3] [enable | disable]}**

no snmp station {*ip_address* **|** *ipv6_address***}**

Syntax Definitions

ip_address	The IP address to which SNMP unicast traps will be sent. A maximum of 16 SNMP stations can be configured.
ipv6_address	The IPv6 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the no form of the command to remove an existing SNMP station.
- The user name specified must match an existing user account name.
- 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.
- You can establish up to 50 SNMP sessions towards an OmniSwitch.

- 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 will send ICMP echo requests to verify reachability. The switch transmits traps to the specified IP or IPv6 address immediately after receiving the ICMP echo response.

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
-> snmp station 300::1 enable
-> no snmp station 300::1
```

Release History

Release 6.1; command was introduced.
Release 6.3.1; *ipv6_address* parameter added.

Related Commands

show snmp station	Displays the current SNMP station information.

MIB Objects

```
trapStationTable
   trapStationIP
   trapStationPort
   trapStationUser
   trapStationProtocol
   trapStationRowStatus
alaTrapInetStationTable
   alaTrapInetStationIPType
   alaTrapInetStationIP
   alaTrapInetStationPort
   alaTrapInetStationRowStatus
   alaTrapInetStationProtocol
   alaTrapInetStationUser
```

snmp source ip preferred

Configures the source IP address field of the SNMP client packets.

snmp soure ip preferred {default | no-loopback | *ip_address***}**

no snmp source ip preferred

Syntax Definitions

default	The Loopback0 address, if configured, will be used for the source IP address field. If no Loopback0 is configured, the first IP address on the switch will be used.
no-loopback	The Loopback0 address should not be used for the source IP address field and the first available IP address on the switch should be used for this field.
ip_address	The IP address to be used in the source IP field.

Defaults

By default, the setting is set to the **default** parameter.

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- When configuring a specific IP address, that address must already exist on the switch.
- Use the **no** form of this command to clear a specific IP address and change the behavior back to default.

Examples

```
-> snmp source ip preferred 192.168.10.1
-> snmp source ip preferred no-loopback
-> snmp source ip preferred default
```

Release History

Release 6.3.4; command was introduced
Release 6.4.3; command was deprecated, use **ip managed-interface**.

Related Commands

snmp station	Adds a new SNMP station; modifies or deletes an existing SNMP station.

show snmp station

Displays the current SNMP station status.

show snmp station

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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
```

The following is an example of the output display using IPv6.

```
-> show snmp station
ipAddress/udpPort                                    status    protocol user
-----------------------------------------------------+---------+--------+------
192.21.160.32/4000                                   enable    v3       abc
192.21.160.12/5000                                   enable    v3       user1
0300:0000:0000:0000:0211:d8ff:fe47:470b/4001         enable    v3       user2
0300:0000:0000:0000:0211:d8ff:fe47:470c/5001         enable    v2       abc
```

output definitions

IPAddress	IP Address of the SNMP management station that replayed the trap. **Note:** OmniSwitch stackable and chassis-based switches support both IP and IPv6 SNMP stations.
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 6.1; command was introduced.

Related Commands

snmp station	Adds a new SNMP station; modifies or deletes an existing SNMP station.

MIB Objects

```
trapStationTable
   trapStationIP
   trapStationPort
   trapStationUser
   trapStationProtocol
   trapStationRowStatus
alaTrapInetStationTable
   alaTrapInetStationIPType
   alaTrapInetStationIP
   alaTrapInetStationPort
   alaTrapInetStationRowStatus
   alaTrapInetStationProtocol
   alaTrapInetStationUser
```

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	A community string in the form of a text string. This string must be between 1 and 32 characters.
useraccount_name	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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; command was introduced.

Related Commands

show snmp security	Displays the current SNMP security status.

MIB Objects

```
SNMPAgtConfig
   SnmpAgtSecurityLevel
```

show snmp security

Displays the current SNMP security status.

show snmp security

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

Refer to the command on page 67-12 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 6.1; command was introduced.

Related Commands

snmp security	Configures the SNMP security settings.

show snmp statistics

Displays the current SNMP statistics.

show snmp statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

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 6.1; 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 6400, 6850E, 6855, 9000E

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.
- Table names are case-sensitive. Therefore, use the exact table names from the MIB database.

Examples

```
-> show snmp mib family trapStationTable
MIP ID   MIB TABLE NAME                          FAMILY
-------+---------------------------------------+--------------------
 73733   trapStationTable                        snmp
```

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 6.1; command was introduced.

Related Commands

show snmp trap filter	Displays the 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 6400, 6850E, 6855, 9000E

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 6.1; command was introduced.

Related Commands

show snmp trap config	Displays the 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 6400, 6850E, 6855, 9000E

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 6.1; command was introduced.

Related Commands

show snmp trap config	Displays the 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 when traps are lost in the network.

snmp trap replay {*ip_address* | *ipv6_address***} [***seq_id***]**

Syntax Definitions

ip_address	The IP address for the SNMP station to which traps will be replayed from the switch.
ipv6_address	The IPv6 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **show snmp station** command 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 192.12.2.100
-> snmp trap replay 300::1
```

Release History

Release 6.1; command was introduced.
Release 6.3.1; *ipv6_address* parameter added.

Related Commands

show snmp station	Displays the current SNMP station status.
show snmp trap replay	Displays the SNMP trap replay information.

MIB Objects

```
trapStationTable
   trapStation Replay
AlaTrapInetStationEntry
   alaTrapInetStationReplay
   alaTrapInetStationNextSeq
```

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* **|** *ipv6_address***}** *trap_id_list*

no snmp trap filter {*ip_address* | *ipv6_address***}** *trap_id_list*

Syntax Definitions

ip_address	The IP address for the SNMP station for which trap filtering is being enabled or disabled.
ipv6_address	The IPv6 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- The amount of traps that can be specified is equal to the number of traps supported in the AOS release.
- 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 192.1.2.3 1
-> snmp trap filter 192.1.2.3 0 1 3 5
-> snmp trap filter 300::1 1 3 4
-> no snmp trap filter 192.1.2.3 1
-> no snmp trap filter 192.1.2.3 0 1 3 5
-> no snmp trap filter 300::1 1 3
```

Release History

Release 6.1; command was introduced.
Release 6.3.1; *ipv6_address* parameter added.

Related Commands

show snmp trap filter	Displays the current SNMP trap filter status.
show snmp trap config	Displays the SNMP trap information, including trap ID numbers, trap names, command families, and absorption rate.

MIB Objects

```
trapFilterTable
   trapFilterStatus
alaTrapInetFilterTable
   alaTrapInetFilterStatus
```

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 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> snmp authentication trap enable
-> snmp authentication trap disable
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

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
```

The following is an example of the output display with IPv6 information.

```
-> show snmp trap replay
ipAddress                                  oldest replay number
-----------------------------------------+--------------------
192.21.160.32                                        12
192.21.160.12                                        57
0300:0000:0000:0000:0211:d8ff:fe47:470b              12
0300:0000:0000:0000:0211:d8ff:fe47:470c              42
```

output definitions

IPAddress	IP address of the SNMP station manager that replayed the trap. **Note:** OmniSwitch stackable and chassis-based switches support both IP and IPv6 SNMP stations.
Oldest Replay Number	Number of the oldest replayed trap.

Release History

Release 6.1; command was introduced.

Related Commands

snmp trap replay	Replays stored traps from the switch to a specified SNMP station.

MIB Objects

```
trapStationTable
   snmpStation Replay
AlaTrapInetStationEntry
   alaTrapInetStationReplay
   alaTrapInetStationNextSeq
```

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 6400, 6850E, 6855, 9000E

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
```

The following is an example of the output display with IPv6 information.

```
-> show snmp trap filter
ipAddress                                 trapId list
----------------------------------------+----------------------------------
192.21.160.32                             1   3   4
192.21.160.12                            no filter
0300:0000:0000:0000:0211:d8ff:fe47:470b     4   5   6
0300:0000:0000:0000:0211:d8ff:fe47:470c   no filter
```

output definitions

IPAddress	IP address of the SNMP management station that recorded the traps. **Note:** OmniSwitch stackable and chassis-based switches support both IP and IPv6 SNMP stations.
TrapId List	Identification number for the traps being filtered.

Release History

Release 6.1; command was introduced.

Related Commands

snmp trap filter	Enables or disables SNMP trap filtering.
show snmp trap config	Displays the SNMP trap information, including trap ID numbers, trap names, command families, and absorption rate.

MIB Objects

```
trapFilterTable
   trapFilterEntry
alaTrapInetFilterTable
   alaTrapInetFilterStatus
```

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 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

```
-> show snmp authentication trap
snmp authentication trap = disable
```

Release History

Release 6.1; 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 6400, 6850E, 6855, 9000E

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 6.1; 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
```

show snmp object

Displays the associated SNMP object name or object ID.

show snmp object {identifier *name* | **name** *oid***}**

Syntax Definitions

name	The name of the object for which the OID should be displayed.
oid	The object ID of the object for which the name should be displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use this command to find the related name or object ID of an SNMP object.
- When using the **identifier** parameter the name is case sensitive.

Examples

```
-> show snmp object identifier systemMicrocodeIndex
  1.3.6.1.4.1.6486.800.1.1.1.2.1.1.1.1.1

->show snmp object name 1.3.6.1.4.1.6486.800.1.1.1.2.1.1.1.1.1
   systemMicrocodeIndex
```

output definitions

OID	The OID of the associated name.
Name	The name of the associated OID.

Release History

Release 6.1; command was introduced.

Related Commands

show snmp mib family	Displays SNMP MIB information. Information includes MIP ID number, MIB table name, and command family.

68 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
ipv6 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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to disable the DNS resolver.
- 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.

Examples

```
-> ip domain-lookup
-> no ip domain-lookup
```

Release History

Release 6.1; command was introduced.

Related Commands

ip name-server	Specifies the IP addresses of up to three servers to query on a host lookup.
ipv6 name-server	Specifies the IPv6 addresses of up to three IPv6 DNS 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***]]**

no ip name-server {*server-address1* **[***server-address2* **[***server-address3***]] | all}**

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 and secondary DNS servers. A third IP address is optional.
all	Removes all configured DNS servers.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the no form of this command to remove individual or all DNS servers.
- Configuration of the DNS resolver to resolve any host query requires that you first set the default domain name with the **ip domain-name** command and enable the DNS resolver function with the **ip domain-lookup** command before you specify the IP addresses of the DNS servers by using the **ip name-server** command.
- You can configure up to three IPv4 DNS servers and three IPv6 DNS servers in a switch.

Examples

```
-> ip name-server 189.202.191.14 189.202.191.15 188.255.19.1
-> ip name-server 10.255.11.66
-> no ip name-server 10.255.11.66
-> no ip name-server all
```

Release History

Release 6.1; command was introduced.

Release 6.3.4; ‘no’ parameter was added for removing DNS servers.

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
```

ipv6 name-server

Specifies the IPv6 addresses of up to three IPv6 DNS servers to query on a host lookup.

ipv6 name-server *server-ipv6_address1* **[***server-ipv6_address2* **[***server-ipv6_address3***]]**

Syntax Definitions

server-ipv6_address1	The IPv6 address of the primary IPv6 DNS server to query for host lookup. Specifying the primary IPv6 DNS address is mandatory.
server-ipv6_address2	The IPv6 address of the secondary IPv6 DNS server to query for host lookup. This server will be queried only if the desired host name is not able to be resolved by the primary IPv6 DNS server. A second IPv6 address is optional.
server-ipv6_address3	The IPv6 address of the IPv6 DNS server with the lower priority. This server will be queried only if the desired host name is not able to be resolved by both the primary and secondary IPv6 DNS servers. A third IPv6 address is optional.

Defaults

N/A

Platforms Supported

OmniSwitch 6400, 6850E, 6855, 9000E

Usage Guidelines

- Configuration of the DNS resolver to resolve any host query requires that you first set the default domain name with the **ip domain-name** command and enable the DNS resolver function with the **ip domain-lookup** command before you specify the IPv6 addresses of the IPv6 DNS servers by using the **ipv6 name-server** command.
- You cannot use multicast, loopback, link-local and unspecified IPv6 addresses for specifying IPv6 DNS servers.
- You can configure up to three IPv6 DNS servers and three IPv4 DNS servers in a switch.

Examples

```
-> ipv6 name-server fec0::2d0:d3:f3fc
-> ipv6 name-server fe2d::2c  f302::3de1:1 f1bc::202:fd40:f3
```

Release History

Release 6.3.1; 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
   systemDNSNsIPv6Addr1
   systemDNSNsIPv6Addr2
   systemDNSNsIPv6Addr3
```

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 6400, 6850E, 6855, 9000E

Usage Guidelines

- Use the **no** form of this command to delete the default domain name.
- Use this command to set the default domain name for DNS lookups.

Examples

```
-> ip domain-name company.com
-> no ip domain-name
```

Release History

Release 6.1; command was introduced.

Related Commands

ip domain-lookup	Enables or disables the DNS resolver.
ip name-server	Specifies the IP addresses of up to three servers to query on a host lookup.
ipv6 name-server	Specifies the IPv6 addresses of up to three IPv6 DNS 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 6400, 6850E, 6855, 9000E

Usage Guidelines

N/A

Examples

The following is an example of the output display on OmniSwitch stackable and chassis-based switches:

```
-> show dns
Resolver is       : enabled
domainName        : company.com
IPv4 nameServer(s): 189.202.191.14
                  : 189.202.191.15
                  : 188.255.19.1
IPv6 nameServer(s): fe2d::2c
                  : f302::3de1:1
                  : f1bc::202:fd40:f3
```

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 using the **ip domain-name** command.
IPv4 nameServer(s)	Indicates the IP address(es) of the IPv4 DNS server(s). These addresses are set using the **ip name-server** command.
IPv6 nameServer(s)	Indicates the IPv6 address(es) of the IPv6 DNS server(s). These addresses are set using the **ipv6 name-server** command.

Release History

Release 6.1; command was introduced.
Release 6.3.1; **IPv4 nameServer(s)** and **IPv6 nameServer(s)** fields are added.

Related Commands

ip domain-lookup	Enables or disables the DNS resolver.
ip name-server	Specifies the IP addresses of up to three servers to query on a host lookup.
ipv6 name-server	Specify the IPv6 addresses of up to three IPv6 DNS servers to query on a host lookup.
ip domain-name	Sets or deletes the default domain name for DNS lookups.

MIB Objects

```
systemDNS
   systemDNSEnableDnsResolver
   systemDNSDomainName
   systemDNSNsAddr1
   systemDNSNsAddr2
   systemDNSNsAddr3
   systemDNSNsIPv6Addr1
   systemDNSNsIPv6Addr2
   systemDNSNsIPv6Addr3
```

A Software License and Copyright Statements

This appendix contains Alcatel-Lucent and third-party software vendor license and copyright statements.

Alcatel-Lucent License Agreement

ALCATEL-LUCENT 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 Alcatel-Lucent. Alcatel-Lucent 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 Alcatel-Lucent 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. **Alcatel-Lucent's Rights.** Licensee acknowledges and agrees that the Licensed Materials are the sole property of Alcatel-Lucent 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 Alcatel-Lucent 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.** Alcatel-Lucent considers the Licensed Files to contain valuable trade secrets of Alcatel-Lucent, the unauthorized disclosure of which could cause irreparable harm to Alcatel-Lucent. 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 Alcatel-Lucent harmless from any claim, lawsuit, legal proceeding, settlement or judgment (including without limitation Alcatel-Lucent'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.** Alcatel-Lucent 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. Alcatel-Lucent 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 Alcatel-Lucent for either replacement or, if so elected by Alcatel-Lucent, 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 ALCATEL-LUCENT 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.** Alcatel-Lucent'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 Alcatel-Lucent for the Licensed Materials. IN NO EVENT SHALL ALCATEL-LUCENT BE LIABLE FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, OR EXEMPLARY DAMAGES OR LOST PROFITS, EVEN IF ALCATEL-LUCENT 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 Alcatel-Lucent and Licensee, if any, Alcatel-Lucent is under no obligation to maintain or support the copies of the Licensed Files made and distributed hereunder and Alcatel-Lucent 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 Alcatel-Lucent and certifying to Alcatel-Lucent 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. Alcatel-Lucent may terminate this License Agreement upon the breach by Licensee of any term hereof. Upon such termination by Alcatel-Lucent, Licensee agrees to return to Alcatel-Lucent 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 Alcatel-Lucent'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 Alcatel-Lucent 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 Alcatel-Lucent for a limited period of time. Alcatel-Lucent 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 2.8, 17 August 2003

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.

Copyright (C) 1987. The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

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 Alcatel-Lucent. 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 Alcatel-Lucent certain warranties of performance, which warranties [or portion thereof] Alcatel-Lucent 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 Alcatel-Lucent and Licensee, Licensee shall immediately return the EMWEB Product and any back-up copy to Alcatel-Lucent, and will certify to Alcatel-Lucent 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 Alcatel-Lucent 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.                                                           *
*                                                                     *
***********************************************************************
```

N.Remote-ni

Provided with this product is a file (part of GDB), the GNU debugger and is licensed from Free Software Foundation, Inc., whose copyright notice is as follows: Copyright (C) 1989, 1991, 1992 by Free Software Foundation, Inc. Licensee can redistribute this software and modify it under the terms of General Public License as published by Free Software Foundation Inc.

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.

O.GNU Zip

GNU Zip -- A compression utility which compresses the files with zip algorithm.

Copyright (C) 1992-1993 Jean-loup Gailly.

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.

P. FREESCALE SEMICONDUCTOR SOFTWARE LICENSE AGREEMENT

Provided with this product is a software also known as DINK32 (Dynamic Interactive Nano Kernel for 32-bit processors) solely in conjunction with the development and marketing of your products which use and incorporate microprocessors which implement the PowerPC (TM) architecture manufactured by Motorola. The licensee comply with all of the following restrictions:

1. This entire notice is retained without alteration in any modified and/or redistributed versions.

2. The modified versions are clearly identified as such. No licenses are granted by implication, estoppel or otherwise under any patents or trademarks of Motorola, Inc.

The SOFTWARE is provided on an "AS IS" basis and without warranty. To the maximum extent permitted by applicable law, MOTOROLA DISCLAIMS ALL WARRANTIES WHETHER EXPRESS OR IMPLIED, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY AGAINST INFRINGEMENT WITH REGARD TO THE SOFTWARE (INCLUDING ANY MODIFIED VERSIONS THEREOF) AND ANY ACCOMPANYING WRITTEN MATERIALS.To the maximum extent permitted by applicable law, IN NO EVENT SHALL MOTOROLA BE LIABLE FOR ANY DAMAGES WHATSOEVER.

Copyright (C) Motorola, Inc. 1989-2001 All rights reserved.

Version 13.1

Q. Boost C++ Libraries

Provided with this product is free peer-reviewed portable C++ source libraries.

Version 1.33.1

R. U-Boot

Provided with this product is a software licensed from Free Software Foundation Inc. This is used as OS Bootloader; and located in on-board flash. This product is standalone and not linked (statically or dynamically) to any other software.

Version 1.1.0

S. Solaris

Provided with this product is free software; Licensee can redistribute it and/or modify it under the terms of the GNU General Public License.

T. Internet Protocol Version 6

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, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

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

The copyright of the products such as crypto, dhcp, net, netinet, netinet6, netley, netwrs, libinet6 are same as that of the internet protocol version 6.

U. CURSES

Copyright (C) 1987. The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.

V. ZModem

Provided with this product is a program or code that can be used without any restriction.

Copyright (C) 1986 Gary S. Brown. All rights reserved.

W.Boost Software License

Provided with this product is reference implementation, so that the Boost libraries are suitable for eventual standardization. Boost works on any modern operating system, including UNIX and Windows variants.

Version 1.0

Copyright (C) Gennadiy Rozental 2005. All rights reserved.

X. OpenLDAP

Provided with this software is an open source implementation of the Lightweight Directory Access Protocol (LDAP).

Version 3

Copyright (C) 1990, 1998, 1999, Regents of the University of Michigan, A. Hartgers, Juan C. Gomez. All rights reserved.

This software is not subject to any license of Eindhoven University of Technology.Redistribution and use in source and binary forms are permitted only as authorized by the OpenLDAP Public License.

This software is not subject to any license of Silicon Graphics Inc.or Purdue University. Redistribution and use in source and binary forms are permitted without restriction or fee of any kind as long as this notice is preserved.

Y. BITMAP.C

Provided with this product is a program for personal and non-profit use.

Copyright (C) Allen I. Holub, All rights reserved.

Z. University of Toronto

Provided with this product is a code that is modified specifically for use with the STEVIE editor. Permission is granted to anyone to use this software for any purpose on any computer system, and to redistribute it freely, subject to the following restrictions:

1. The author is not responsible for the consequences of use of this software, no matter how awful, even if they arise from defects in it.

2.The origin of this software must not be misrepresented, either by explicit claim or by omission.

3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software.

Version 1.5

Copyright (C) 1986 by University of Toronto and written by Henry Spencer.

AA.Free/OpenBSD

Copyright (c) 1982, 1986, 1990, 1991, 1993 The Regents of University of California. All Rights Reserved.

CLI Quick Reference

Ethernet Port Commands

trap {*slot* | *slot*/*port*[-*port2*]} port link {enable | disable | on | off}
interfaces {*slot* | *slot*/*port*[-*port2*]} speed {auto | 10 | 100 | 1000 | 10000 | max {100 | 1000}}
interfaces {*slot* | *slot/port}* mode {uplink | stacking}
interfaces {*slot* | *slot*/*port*[-*port2*]} autoneg {enable | disable | on | off}
interfaces {*slot* | *slot*/*port*[-*port2*]} crossover {auto | mdix | mdi}
interfaces {*slot* | *slot*/*port*[-*port2*]} pause {tx | rx | tx-and-rx | disable}
interfaces e2e-flow-vlan *vlan_id*
interfaces no e2e-flow-vlan
interfaces {*slot* | *slot*/*port*[-*port2*]} duplex {full | half | auto}
interfaces {*slot* | *slot*/*port*[-*port2*]} admin {up | down}
interfaces cli-prompt {enable | disable}
interfaces *slot*/*port* alias *description*
interfaces {*slot* | *slot*/*port*[-*port2*]} ifg *bytes*
interfaces {*slot* | *slot*/*port*[-*port2*]} no l2 statistics [cli]
interfaces {*slot* | *slot*/*port*[-*port2*]} max frame *bytes*
interfaces {*slot* | *slot*/*port*[-*port2*]} flood [broadcast | multicast | unknown-unicast | all] [enable | disable]
interfaces {*slot* | *slot*/*port*[-*port2*]} flood {broadcast | multicast | unknown-unicast | all} rate {mbps *mbps* | pps *pps* | percentage *percent* | *default}* [low-threshold num]
interfaces {*slot* | *slot*/*port*[-*port2*]} flood [broadcast | multicast] action [shutdown | trap | default]
interfaces [*slot* | *slot*/*port***[**-*port2***]**] violation-recovery-time {seconds | default}
interfaces {*slot* | *slot*/*port***[**-*port2***]**} violation-recovery-time default
interfaces [*slot* | *slot*/*port*[-*port2*]] violation-recovery-maximum *max_attempts*
interfaces {*slot* | *slot*/*port*[-*port2*]} violation-recovery-maximum default
interface violation-recovery-trap {enable | disable}
interfaces {*slot* | *slot*/*port*[-*port2*]} clear-violation-all
interfaces {*slot* | *slot*/*port*[-*port2*]} wait-to-restore *seconds*
interfaces transceiver ddm [trap] {enable | disable}
interfaces {*slot* | *slot/port*[-*port2*]} link-monitoring admin-status {enable | disable}
interfaces {*slot* | *slot/port*[-*port2*]} link-monitoring time-window *seconds*
interfaces {*slot* | *slot/port*[-*port2*]} link-monitoring link-flap-threshold *link_flaps*
interfaces {*slot* | *slot/port*[-*port2*]} link-monitoring link-error-threshold *mac_errors*
interfaces {*slot* | *slot/port*[-*port2*]} clear-link-monitoring-stats
interfaces {*slot* | *slot/port*[-*port2*]} hybrid preferred-fiber
interfaces {*slot* | *slot/port*[-*port2*]} hybrid {fiber | copper} autoneg {enable | disable | on | off}
interfaces {*slot* | *slot/port*[-*port2*]} hybrid copper crossover {auto | mdix | mdi}
interfaces {*slot* | *slot/port*[-*port2*]} hybrid {fiber | copper} duplex {full | half | auto}
interfaces {*slot* | *slot/port*[-*port2*]} hybrid {fiber | copper} speed {auto | 10 | 100 | 1000 | 10000 | max {100 | 1000}}
interfaces {*slot* | *slot/port*[-*port2*]} hybrid {fiber | copper} pause {tx | rx | tx-and-rx | disable}
show interfaces [*slot* | *slot/port*[-*port2*]]
show interfaces [*slot* | *slot/port*[-*port2*]] capability
show interfaces [*slot* | *slot/port*[-*port2*]] flow [control]
show interfaces [*slot* | *slot/port*[-*port2*]] pause
show interfaces e2e-flow-vlan
show interfaces [*slot* | *slot/port*[-*port2*]] accounting
show interfaces [*slot* | *slot/port*[-*port2*]] counters
show interfaces [*slot* | *slot/port*[-*port2*]] counters errors
show interfaces [*slot* | *slot/port*[-*port2*]] collisions
show interfaces [*slot* | *slot/port*[-*port2*]] status
show interfaces [*slot* | *slot/port*[-*port2*]*]* port
show interfaces violation-recovery
show interfaces [*slot* | *slot/port*[-*port2*]] ifg
show interfaces [*slot* | *slot/port* [-*port2*]] flood rate
show interfaces [*slot* | *slot/port*[-*port2*]] traffic
show interfaces [*slot* | *slot/port*[-*port2*]] transceiver [ddm | w-low | w-high | a-low | a-high | actual]
show interfaces [*slot* | *slot/port*[-*port2*]] hybrid {fiber | copper}
show interfaces [*slot* | *slot/port*[-*port2*]] hybrid {fiber | copper} status
show interfaces [*slot* | *slot/port*[-*port2*]] hybrid {fiber |copper} pause
show interfaces [*slot* | *slot/port*[-*port2*]] hybrid {fiber |copper} capability
show interfaces [*slot* | *slot/port*[-*port2*]] hybrid {fiber |copper} accounting
show interfaces [*slot* | *slot/port*[-*port2*]] hybrid {fiber |copper} counters
show interfaces [*slot* | *slot/port*[-*port2*]] hybrid {fiber |copper} counters errors
show interfaces [*slot* | *slot/port*[-*port2*]] hybrid {fiber |copper} collisions
show interfaces [*slot* | *slot/port*[-*port2*]] hybrid {fiber |copper} traffic
show interfaces [*slot* | *slot/port*[-*port2*]] hybrid {fiber |copper} port
show interfaces [*slot* | *slot/port*[-*port2*]] hybrid {fiber |copper} flood rate
show interfaces [*slot* | *slot/port***[**-*port2***]**] hybrid {fiber |copper} ifg
show interfaces {*slot* | *slot/port*[-*port2*]} link-monitoring config
show interfaces {*slot* | *slot/port*[-*port2*]} link-monitoring statistics
debug interfaces set [*slot*] backpressure {enable | disable}
debug interfaces [*slot*] backpressure
link-fault-propagation group group_id [admin-state {enable | disable}]
no link-fault-propagation group {group_i*d*[-*group_id2*]**}**
link-fault-propagation group group_id source {port *slot/port*[-*port2*] | linkagg *agg_id*[-*agg_id2*]}
no link-fault-propagation group group_id source {port *slot/port***[**-*port2***]** | linkagg *agg_id***[**-*agg_id2***]**}
link-fault-propagation group group_id destination {port *slot/port[-port2]* | linkagg *agg_id[-agg_id2]*}

no link-fault-propagation group group_id destination {port *slot/port[-port2]* | linkagg *agg_id[-agg_id2]*}
link-fault-propagation group group_id wait-to-shutdown seconds
show link-fault-propagation group [group_id]
interfaces slot/port tdr-test-start
interfaces {*slot* | *slot/port*[*-port2*]} no tdr-statistics
show interfaces [*slot* | *slot/port*[*-port2*]] tdr-statistics

UDLD Commands

udld {enable | disable}
udld port slot/port[*-port2*] {enable | disable}
udld port [slot/port[*-port2*]] mode {normal | aggressive}
udld port [slot/port[*-port2*]] probe-timer seconds
no udld port [slot/port[*-port2*]] probe-timer
udld port [slot/port[*-port2*]] echo-wait-timer seconds
no udld port [slot/port[*-port2*]] echo-wait-timer
clear udld statistics [port slot/port]
show udld configuration
show udld configuration port [slot/port]
show udld statistics port slot/port
show udld neighbor port slot/port
show udld status port [slot/port]

Power over Ethernet (PoE) Commands

lanpower start {*slot/port*[*-port2*] | *slot*}
lanpower stop {*slot/port*[*-port2*] | *slot*}
lanpower {*slot/port* | *slot*} power *milliwatts*
lanpower *slot* maxpower *watts*
lanpower *slot/port* priority {critical | high | low}
lanpower *slot* priority-disconnect {enable | disable}
lanpower *slot* slot-priority {critical | high | low}
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*

VLAN Management Commands

vlan *vid1*[*-vid2*] [enable | disable] [name *description*]
no vlan *vid1*[*-vid2*]
vlan *vid1*[*-vid2*] [1x1 | flat] stp {enable | disable}
vlan *vid1*[*-vid2*] mobile-tag {enable | disable}
vlan *vid* authentication {enable | disable}
vlan *vid* mtu-ip *size*
vlan *vid* port default {*slot/port* | *link_agg*}
vlan *vid* no port default {*slot/port* | *link_agg*}
show vlan [*vid1* [*-vid2*]]
show vlan [*vid1*[*-vid2*]] port [*slot/port* | *link_agg*]
show vlan router mac status
show vlan gvrp [*vid1*[*-vid2*]]
show vlan ipmvlan [*ipmvlan-id1*[*-ipmvlan-id2*]]

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}
show 802.1q {slot/port | aggregate_id}

Distributed Spanning Tree Commands

bridge mode {flat | 1x1}
spantree mode {flat | per-vlan}
bridge [*instance*] protocol {stp | rstp | mstp}
bridge cist protocol {stp | rstp | mstp}
bridge port {*slot/port* | linkagg *linkagg_id* } loop-guard {enable | disable}

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 msti *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 mode 1x1 pvst+ {enable | disable}
bridge [*instance*] bpdu-switching {enable | disable}
bridge path cost mode {auto | 32bit}
bridge [msti *msti_id*] auto-vlan-containment {enable | disable}
bridge port {*slot/port* | *agg_num*} pvst+ {auto | enable | disable}

bridge *instance* {*slot/port* | *logical_port*} {enable | disable}
bridge cist {*slot/port* | *logical_port*} {enable | disable}
bridge 1x1 *vid* {*slot/port* | *logical_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}
bridge cist {*slot/port* | *logical_port*} connection {noptp | ptp | autoptp}
bridge 1x1 *vid* {*slot/port* | *logical_port*} connection {noptp | ptp | autoptp }
bridge cist {*slot/port* | *logical_port*} admin-edge {on | off | enable | disable}
bridge 1x1 *vid* {*slot/port* | *logical_port*} admin-edge {on | off | enable | disable}
bridge cist {*slot/port* | *logical_port*} auto-edge {on | off | enable | disable}
bridge 1x1 *vid* {*slot/port* | *logical_port*} auto-edge {on | off | enable | disable}
bridge cist {*slot/port* | *logical_port*} {restricted-role | root-guard} {on | off | enable | disable}
bridge 1x1 *vid* {*slot/port* | *logical_port*} {restricted-role | root-guard} {on | off | enable | disable}
bridge cist {*slot/port* | *logical_port*} restricted-tcn {on | off | enable | disable}
bridge 1x1 *vid* {*slot/port* | *logical_port*} restricted-tcn {on | off | enable | disable}
bridge cist txholdcount *value*
bridge 1x1 *vid* txholdcount {*value*}
bridge rrstp
no bridge rrstp

bridge rrstp ring ring_id port1 {slot/port | linkagg agg_num} port2 {slot/port | linkagg agg_num} vlan-tag vlan_id [status {enable | disable}]
no bridge rrstp ring [ring_id]
bridge rrstp ring ring_id vlan-tag vid
bridge rrstp ring ring_id status {enable | disable}
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*}
show bridge rrstp configuration
show bridge rrstp ring [*ring_id*]

Link Aggregation Commands

static linkagg *agg_num* size *size* [name *name*] [admin state {enable | disable}] [multi-chassis active] min-size num]
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
lacp linkagg wait-to-restore timer num
lacp agg [ethernet | fastethernet | gigaethernet] *slot*/*port* standby {enable | disable}
lacp linkagg *agg_num* pre-empt {enable | disable}
lacp linkagg *agg_num* pre-empt timer *seconds*

dhl num *dhl_num [name name]*
no dhl num *dhl_num*
dhl num *dhl_num linka* {port slot/port | linkagg agg_id} *linkb* {port slot/port | linkagg agg_id}
no dhl num *dhl_num linka* {port slot/port | linkagg agg_id} *linkb* {port slot/port | linkagg agg_id}
dhl num *dhl_num admin-state* {enable | disable}
dhl num *dhl_num vlan-map linkb {vlan_id[-vlan_id]}*
no dhl num *dhl_num vlan-map linkb {vlan_id[-vlan_id]}*
dhl num *dhl_num pre-emption-time num*
dhl num *dhl_num mac-flushing* {none | raw | mvrp}
show dhl
show dhl num *dhl_num*
show dhl num *dhl_num* [linkA | linkB]
show linkagg [*agg_num*] port [*slot*/*port*]
show linkagg [agg_num] port [*slot*/*port*]
linkagg *range local {agg_num-agg_num } peer {agg_num-agg_num}* multi-chassis *{agg_num-agg_num}*
show linkagg range [operation | config]

Multi-Chassis Commands

multi-chassis chassis-id *chassis_id* [hello-interval *interval*]
no multi-chassis chassis-id *chassis_id* [hello-interval *interval*]
multi-chassis hello-interval *interval*
multi-chassis chassis-group *num*
multi-chassis ipc-vlan *vid*
multi-chassis loop-detection {enable|disable}
multi-chassis loop-detection transmit-interval *interval*
multi-chassis vf-link create
no multi-chassis vf-link
multi-chassis vf-link member-ports *slot/port*
no multi-chassis vf-link member-ports *slot/port*
multi-chassis vf-link default-vlan *vlan*
no multi-chassis vf-link default-vlan *vlan*
multi-chassis vip-vlan *vid [{admin-state {enable|disable}} { name {num}{"string" string} { mtu-ip num}][{ 1x1 | flat } stp {enable | disable}]*
no multi-chassis vip-vlan *vid*
show multi-chassis status
show multi-chassis loop-detection
show multi-chassis vf-link
show multi-chassis vf-link member-port [*slot/port*]
show multi-chassis consistency
show multi-chassis consistency linkagg *agg_num [*vlan-list]
clear multi-chassis loop-detection

Ethernet Ring Protection Commands

erp-ring ring_id port1 {*slot/port* | linkagg agg_num} port2 {*slot/port* | linkagg agg_num} service-vlan vlan_id level level_num [guard-timer guard_timer] [enable | disable]
no erp-ring ring_id
erp-ring ring_id reset-version-fallback
erp-ring ring_id rpl-node {port slot/port | linkagg agg_num}
no erp-ring ring_id rpl-node
erp-ring ring_id wait-to-restore wtr_timer
no erp-ring ring_id wait-to-restore
erp-ring ring_id {enable | disable}
erp-ring ring_id guard-timer guard_timer
no erp-ring ring_id guard-timer
Creates an Ethernet Ring Protection (ERP) sub-ring.
erp-ring ring_id sub-ring-port {slot/port | linkagg agg_num} service-vlan vlan_id level level_num [guard-timer guard_timer] [enable | disable]
no erp-ring ring_id {slot/port | linkagg agg_num}
erp-ring ring_id virtual-channel [enable | disable]
This command is only applicable for the RPL-owner switch. Enables or disables revertive mode on the specified node.
erp-ring ring_id revertive [enable | disable]
This command is only applicable for the RPL-owner switch. Clears any pending state (for example,
non-revertive restoring).
erp-ring ring_id clear
Configures a ring port to accept a “loss of connectivity” event from Ethernet OAM for a remote endpoint.
erp-ring ring_id ethoam-event {*slot/port* | linkagg agg_num} remote-endpoint mep_id
no erp-ring ring_id ethoam-event {*slot/port* | linkagg agg_num}
Clears ERP statistics for all rings, a specific ring, or a specific ring port.
clear erp statistics [ring ring_id [port *slot/port* | linkagg agg_num]]
show erp [ring ring_id | [port *slot/port* | linkagg agg_num]]
show erp statistics [ring ring_id [port *slot/port* | linkagg agg_num]]

Loopback Detection Commands

loopback-detection {enable | disable}
loopback-detection port slot/port [-port2] {enable | disable}
loopback-detection transmission-timer seconds
show loopback-detection
show loopback-detection port [slot/port]
show loopback-detection statistics port [slot/port]

CPE Test Head Commands

test-oam *string* [descr *description*]
no test-oam *string*
test-oam *string* [direction {unidirectional | bidirectional}]
test-oam string [src-endpoint src-string] [dst-endpoint dst-string]
test-oam string port slot/port
test-oam string [vlan svlan] [[test-frame [src-mac src-address] [dst-mac dst-address]]
test-oam string role {generator | analyzer}
test-oam string [duration secs] [rate rate] [packet-size bytes]
test-oam string {[vlan vlan-id] [port slot/port] [packet-size bytes] start | stop}
show test-oam [**tests** | string**]**
show test-oam [string**]** statistics
clear test-oam [string] statistics
test-oam *group* string [descr *description*]
no test-oam group *string*
test-oam *group* string [tests string1.....string8]
test-oam group string [no tests string1.....string8]
test-oam *feeder-port* slot/port
no test-oam feeder-port
test-oam group string [src-endpoint src-string dst-endpoint dst-string] [src-endpoint src-string] [dst-endpoint dst-string]
test-oam group name role {generator | analyzer}
test-oam group string port slot/port
test-oam group string [direction unidirectional]
test-oam group string [duration secs] [rate rate]
test-oam group string [port slot/port] start
test-oam group string stop
clear test-oam group string statistics
show test-oam group [**tests | string]**
show test-oam group [string**]** statistics

Source Learning Commands

mac-address-table [permanent] *mac_address* {*slot/port* | linkagg *link_agg*} *vid* [bridging | filtering]
no mac-address-table [permanent | learned] [*mac_address* {*slot/port* | linkagg *link_agg*} *vid*]
mac-address-table vpls service-id permanent mac-address sap {sap-id | linkagg *sap-id*}
no mac-address-table vpls service-id permanent *mac-address*
no mac-address-table vpls service-id learned [sap *sap-id* | linkagg *sap-id*] *mac-address*
mac-address-table vpls service-id permanent mac-address mesh-sdp sdp-id[*:vc-id*]
no mac-address-table vpls *service-id permanent mac-address*
no mac-address-table vpls service-id learned [mesh-sdp sdp-id[*:vc-id*]] *mac-address*

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
no mac-address-table aging-time
source-learning {port slot/port1[-port2] | linkagg linkagg_num} {enable | disable}
source-learning chassis-distributed {enable | disable}
show mac-address-table [permanent | learned | quarantined] [*mac_address*] [slot *slot* | *slot/port*] [linkagg *link_agg*] [*vid* | *vid1-vid2*]
show mac-address-table all [permanent | learned]
show mac-address-table vpls [service-id] [permanent | learned] [mac-address]
show *mac-address-table vpls service-id sap {sap-id* | linkagg *sap-id*} mac-address
show *mac-address-table vpls service-id mesh-sdp sdp-id*[*:vc-id*] mac-address
show mac-address-table static-multicast [*multicast_address*] [slot *slot* | *slot/port*] [linkagg *link_agg*] [*vid* | *vid1-vid2*]
show mac-address-table count [*mac_address*] [slot *slot* | *slot/port*] [linkagg *link_agg*] [*vid* | *vid1-vid2*]
show mac-address-table vpls service-id count] [mac-address]
show mac-address-table all count
show mac-address-table aging-time
show source-learning [port *slot/port*[-*port2*] | linkagg *linkagg_num*]
show source-learning chassis-distributed

PPPoE Intermediate Agent Commands

pppoe-ia [port *slot*/*port*[-*port2*] | linkagg agg_id] {enable | disable}
pppoe-ia {port *slot*/*port*[-*port2*] | linkagg agg_id} trust
pppoe-ia {port *slot*/*port*[-*port2*] | linkagg agg_id} client
pppoe-ia access-node-id {base-mac | system-name | mgnt-address | user-string string}
pppoe-ia circuit-id {default | ascii [base-mac | system-name | interface | vlan | cvlan | interface-alias | user-string string | delimiter char]}
pppoe-ia remote-id {base-mac | system-name | mgnt-address | user-string string}
clear pppoe-ia statistics [port {*slot*/*port*[-*port2*] | linkagg agg_id]
show pppoe-ia configuration
show pppoe-ia [port {*slot*/*port*[-*port2*] | linkagg agg_id] [enabled | disabled | trusted | client]
show pppoe-ia statistics

GVRP Commands

gvrp
no gvrp
gvrp {linkagg agg_num | port slot/port}
no gvrp {linkagg agg_num | port slot/port}
gvrp transparent switching
no gvrp transparent switching
gvrp maximum vlan vlanlimit
no gvrp registration {linkagg agg_num | port slot/port}
gvrp applicant {participant | non-participant | active} {linkagg agg_num | port slot/port}
no gvrp applicant {linkagg agg_num | port slot/port}
gvrp timer {join | leave | leaveall} timer-value {linkagg agg_num | port slot/port}
no gvrp timer {join | leave | leaveall} {linkagg agg_num | port slot/port}
no gvrp restrict-vlan-registration {linkagg agg_num | port slot/port} vlan-list
no gvrp restrict-vlan-advertisement {linkagg agg_num | port slot/port} vlan-list
gvrp static-vlan restrict {linkagg agg_num | port slot/port} vlan-list
no gvrp static-vlan restrict {linkagg agg_num | port slot/port} vlan-list
clear gvrp statistics [linkagg agg_num | port slot/port]
show gvrp statistics [linkagg agg_num | port slot/port]
show gvrp last-pdu-origin {linkagg agg_num | port slot/port}
show gvrp configuration
show gvrp configuration port
show gvrp configuration {linkagg agg_num | port slot/port}
show gvrp timer [[join | leave | leaveall] {linkagg agg_num | port slot/port}]

MVRP Commands

vlan registration-mode {gvrp | mvrp}
mvrp {enable | disable}
mvrp port *slot/port* [– *port2*] {enable | disable}
mvrp linkagg *agg_num* [-*agg_num2*] {enable | disable}
mvrp transparent-switching {enable | disable}
mvrp {port *slot/port* [– *port2*] | linkagg *agg_num* [-*agg_num2*]} registration {normal | fixed | forbidden}
mvrp {port *slot/port* [– *port2*] | linkagg *agg_num* [-*agg_num2*]} applicant {participant | non-participant | active}
mvrp {port *slot/port* [– *port2*] | linkagg *agg_num* [-*agg_num2*]} restrict-vlan-registration vlan *vlan-list*
no mvrp {port *slot/port* [– *port2*] | linkagg *agg_num* [-*agg_num2*]} restrict-vlan-registration vlan *vlan-list*
mvrp {port *slot/port* [–*port2*] | linkagg *agg_num* [-*agg_num2*]} restrict-vlan-advertisement vlan *vlan-list*
no mvrp {| port *slot/port* [–*port2*] | linkagg *agg_num* [-*agg_num2*]} restrict-vlan-advertisement vlan *vlan-list*
mvrp {linkagg *agg_num* [-*agg_num2*] | port *slot/port* [– *port2*]} static-vlan-restrict vlan *vlan-list*

no mvrp {linkagg *agg_num* [-*agg_num2*] | port *slot/port* [– *port2*]} static-vlan-restrict vlan *vlan-list*
show mvrp configuration
show mvrp port {*slot/port* [-*port2*]} [enabled | disabled]
show mvrp linkagg [*agg_num* [-*agg_num2*]} [enabled | disabled]
mvrp [port *slot/port* [–*port2*] | linkagg *agg_num* [-*agg_num2*]] clear-statistics

802.1AB Commands

lldp destination mac-address {nearest-bridge | nearest-edge}
lldp transmit fast-start-count num
lldp transmit interval seconds
lldp transmit hold-multiplier num
lldp transmit delay seconds
lldp reinit delay seconds
lldp notification interval seconds
lldp {slot/port | slot | chassis} lldpdu {tx | rx | tx-and-rx | disable}
lldp {slot/port | slot | chassis} notification {enable | disable}
lldp network-policy policy_id - [policy_id2] application {voice | voice-signaling | guest-voice |
guest-voice-signaling | softphone-voice | video-conferencing | streaming-video | video-signaling}
vlan {untagged | priority-tag | vlan-id} [l2-priority 802.1p_value] [dscp dscp_value]
no lldp network-policy policy_id - [policy_id2]
lldp {slot/port | slot | chassis} med network-policy policy_id - [policy_id2]
no lldp {slot/port | slot | chassis} med network-policy policy_id - [policy_id2]
lldp {slot/port | slot | chassis} tlv management {port-description | system-name | system-description | system-capabilities | management-address} {enable | disable}
lldp {slot/port | slot | chassis} tlv dot1 {port-vlan | vlan-name} {enable | disable}
lldp {slot/port | slot | chassis} tlv dot3 mac-phy {enable | disable}
lldp {slot/port | slot | chassis} tlv med {power | capability | network policy} {enable | disable}
show lldp {slot | slot/port} config
show lldp network-policy [policy_id]
show lldp [slot | slot/port] med network-policy
show lldp system-statistics
show lldp [slot|slot/port] statistics
show lldp local-system
show lldp [slot/port | slot] local-port
show lldp local-management-address
show lldp [slot/port | slot] remote-system
show lldp [slot/port | slot] remote-system [med {network-policy | inventory}]
lldp {slot/port| slot | chassis} trust-agent {enable | disable} [chassis-id-subtype {chassis-component | interface-alias | port-component | mac-address | network-address | interface-name | locally-assigned | any}]
lldp {slot/port| slot | **chassis**} trust-agent violation-action {trap-and-shutdown | trap | shutdown}
show lldp [num | slot/port] trusted remote-agent
show lldp [slot | slot/port] trust-agent

Interswitch Protocol Commands

amap {enable | disable}
amap discovery [time] *seconds*
amap common [time] *seconds*
show amap

SIP Commands

sip-snooping { enable | disable }
sip-snooping[{port *slot/port1*[-*port2*] | linkagg *linkagg_num*] {enable|disable}
sip-snooping[{port *slot/port* [-port2] | linkagg *agg_num* mode {force-edge | force-non-edge | automatic}
sip-snooping trusted-server [*ip_address1 ip_address2 ip_address ...ip_address8*]
no sip-snooping trusted-server *all*
no sip-snooping trusted-server [*ip_address*]
sip-snooping sip-control dscp *num*
sip-snooping sip-control no dscp
sip-snooping sos-call number <*string1*> <*string2*> … <*string4*>
no sip-snooping sos-call number <*string*>
no sip-snooping sos-call number all
sip-snooping sos-call dscp *num*
sip-snooping udp-port <*udp-port1*> < *udp-port 2*> ... < *udp-port 8*>
no sip-snooping udp-port <*udp-port*>
no sip-snooping udp-port all
sip-snooping threshold {audio | video | other} {jitter *jitter_ms_num* | packet-lost *% num* | round-trip-delay *round_trip_delay_ms_num* | R-factor *Rfactor_num*| MOS *mos_num*}
sip-snooping logging-threshold num-of-calls *num*
clear sip-snooping statistics
show sip-snooping config
show sip-snooping ports
show sip-snooping statistics
show sip-snooping call-records {active-calls|ended-calls} [full | threshold-violation]
show qos dscp-table

IP Commands

ip interface *name* [address *ip_address*] [mask *subnet_mask*] [admin [enable | disable]] [vlan *vid* | *{rtr-port [agg_num | slot/port] rtr-vlan num [type {tagged | untagged}}*] [forward

| no forward] [local-proxy-arp | no local-proxy-arp] [eth2 | snap] [primary | no primary] [local-host-dbcast [enable | disable]

no ip interface *name*

ip managed-interface {*Loopback0* | *interface-name*} application [ldap-server] [tacacs] [radius] [snmp] [sflow] [ntp] [syslog] [dns] [telnet] [ftp] [ssh] [tftp] [all]

no ip managed-interface {*Loopback0* | *interface-name*} application [ldap-server] [tacacs] [radius] [snmp] [sflow] [ntp] [syslog] [dns] [telnet] [ftp] [ssh] [tftp] [all]

ip interface *dhcp-client* [vlan *vid*] [release | renew] [option-60 opt60_string] [admin {enable | disable}]

no ip interface *dhcp-client*

ip interface *name* tunnel [source *ip_address*] [destination *ip_address*] [protocol {ipip | gre}]

ip router primary-address *ip_address*

ip router router-id *ip_address*

ip static-route *ip_address* [mask *mask*] {gateway | follows} *ip_address* [metric *metric*] [tag *tag-num*] [name *tag-name*]

no ip static-route *ip_address* [mask *mask*] {gateway | follows} *ip_address* [metric *metric*][tag *tag-num*] [name *tag-name*]

[vrf name] ip route-pref {static | rip | ospf | isisl2 | isisl1 | ibgp | ebgp | import} value

ip default-ttl *hops*

ping {*ip_address* | *hostname*} [source-interface *ip_interface*] [[sweep-range *start_size* | *end_size* | *diff_size*] | [count *count*] [size *packet_size*]] [interval *seconds*] [timeout *seconds*] [tos *tos_val*]
[dont-fragment] [data-pattern *hex_string*]

traceroute {*ip_address* | *hostname*} [source-interface *ip_interface*] [min-hop *min_hop_count*] [max-hop *max_hop_count*] [probes *probe_count*] [time-out *seconds*] [port-number *port_number*]

ip directed-broadcast {on | off}

ip service {all | *service_name* | port *service_port*}

no ip service {all | *service_name* | port *service_port*}

[vrf name] ip redist {local | static | rip | ospf | isis | bgp | import} into {rip | ospf | isis | bgp} route-map *route-map-name* [status {enable | disable}]

no ip redist {local | static | rip | ospf | isis | bgp | import} into {rip | ospf | isis | bgp} [route-map *route-map-name*]

ip access-list *access-list-name*

no ip access-list access-list-name

ip access-list access-list-name address address/prefixLen [action {permit | deny}] [redist-control {all-subnets | no-subnets | aggregate}]

no ip access-list access-list-name address address/prefixLen

ip route-map route-map-name [sequence-number number] match ip-nexthop {access-list-name | ip_address/prefixLen [permit | deny]}

no ip route-map route-map-name [sequence-number number] match ip-nexthop {access-list-name | ip_address/prefixLen [permit | deny]}

ip route-map route-map-name [sequence-number number] match ipv6-nexthop {access-list-name | ipv6_address/prefixLen [permit | deny]}

no ip route-map route-map-name [sequence-number number] match ipv6-nexthop {access-list-name | ipv6_address/prefixLen [permit | deny]}

ip route-map route-map-name [sequence-number number] match ipv4-interface interface-name

no ip route-map route-map-name [sequence-number number] match ipv4-interface interface-name

ip route-map route-map-name [sequence-number number] match ipv6-interface interface-name

no ip route-map route-map-name [sequence-number number] match ipv6-interface interface-name

ip route-map route-map-name [sequence-number number] match metric metric [deviation deviation]

no ip route-map route-map-name [sequence-number number] match metric metric [deviation deviation]

ip route-map route-map-name [sequence-number number] match route-type {internal | external [type1 | type2] | level1 | level2}

no ip route-map route-map-name [sequence-number number] match route-type {internal | external [type1 | type2] | level1 | level2}

ip route-map route-map-name [sequence-number number] match protocol {local | static | rip | ospf | isis | bgp}

no ip route-map route-map-name [sequence-number number] match protocol {local | static | rip | ospf | isis | bgp}

ip route-map *route-map-name* [sequence-number *number*] set metric *metric* [effect {add | subtract | replace | none}]

no ip route-map *route-map-name* [sequence-number *number*] set metric *metric* [effect {add | subtract | replace | none}]

ip route-map *route-map-name* [sequence-number *number*] set metric-type {internal | external [type1 | type2]}

no ip route-map *route-map-name* [sequence-number *number*] set metric-type {internal | external [type1 | type2]}

ip route-map *route-map-name* [sequence-number *number*] set tag *tag-number*

no ip route-map *route-map-name* [sequence-number *number*] set tag *tag-number*

ip route-map *route-map-name* [sequence-number *number*] set community *community-string*

no ip route-map *route-map-name* [sequence-number *number*] set community *community-string*

ip route-map *route-map-name* [sequence-number *number*] set local-preference *value*

no ip route-map *route-map-name* [sequence-number *number*] set local-preference *value*

ip route-map *route-map-name* [sequence-number *number*] set level {level1 | level2 | level1-2}

no ip route-map *route-map-name* [sequence-number *number*] set level {level1 | level2 | level1-2}

ip route-map *route-map-name* [sequence-number *number*] set ip-nexthop *ip_address*

no ip route-map *route-map-name* [sequence-number *number*] set ip-nexthop *ip_address*

ip route-map *route-map-name* [sequence-number *number*] set ipv6-nexthop *ipv6_address*

no ip route-map *route-map-name* [sequence-number *number*] set ipv6-nexthop *ipv6_address*

vrf [*name* | default]
no vrf *name*
[vrf name] ip export route-map route-map-name
[vrf name] no ip export
[vrf name] ip import vrf {src-vrf-name | default} route-map route-map-name
[vrf name] no ip import vrf {src-vrf-name | default}
[vrf name] show ip export
[vrf name] show ip import

show ip global-route-table [export-vrf name]
arp *ip_address hardware_address* [alias] [arp-name *name*]
no arp *ip_address* [alias]
clear arp-cache
ip dos arp-poison restricted-address ip_address
no ip dos arp-poison restricted-address ip_address
arp filter *ip_address* [mask *ip_mask*] [*vid*] [sender | target] [allow | block]
no arp filter *ip_address*
clear arp filter
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 addr-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* | *dhcp-client*]
show ip managed-interface
[vrf name] show ip route [gateway *ip_address* | protocol *type* | summary | destination {*ip_address/*prefixLen | *ip_address*}]
[vrf name] show ip route-pref
[vrf name] show ip redist [rip | ospf | isis | bgp]
show ip access-list [*access-list-name*]
show ip route-map [*route-map-name*]
[vrf name] show ip router database [protocol *type* | gateway *ip_address* | dest {*ip_address/*prefixLen | *ip_address*}]
show ip emp-route
show ip config
show ip protocols
show ip service
show ip dynamic-proxy-arp
show vrf
show arp [*ip_address* | *hardware_address*]
show arp summary
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
show ip dos arp-poison
ip wccp admin-state {enable | disable}
ip wccp service-group {web-cache | service-id**[**-service-id2**]}** [md5 password string]
no ip wccp service-group {web-cache | service-id**[**-service-id2**]**}
ip wccp service-group {web-cache | service-id} restrict { port slot/port | vlan vlan_id | ip ipv4 [mask mask]}
no ip wccp service-group {web-cache | service-id} restrict { port slot/port | vlan vlan_id | ip ipv4 [mask mask]}
clear ip wccp [service-group {web-cache | service-id}] statistics
show ip wccp status
show ip wccp services
show ip wccp cache-engines
show ip wccp [service-group {web-cache | service-id}] restricts
show ip wccp service-group {web-cache | service-id}
show ip wccp [service-group {web-cache | service-id}] detail
show ip wccp [service-group {web-cache | service-id}] view
show ip wccp [service-group {web-cache | service-id}] statistics
ip dos anti-spoofing {enable | disable}
ip dos anti-spoofing arp-only {enable | disable}
ip dos anti-spoofing address ip-address {enable | disable}
ip dos anti-spoofing address ip-address arp-only {enable | disable}
ip dos anti-spoofing clear stats
ip dos anti-spoofing address ip-address clear stats
show ip dos anti-spoofing [ip-address]

IPv6 Commands

ipv6 interface if_name [vlan vid | tunnel {tid | 6to4}] [enable | disable] [base-reachable-time time]

[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* [anycast] **{***if_name* | *loopback***}**
ipv6 address *ipv6_prefix* eui-64 **{***if_name* | *loopback***}**
no ipv6 address *ipv6_prefix* eui-64 **{***if_name* | *loopback***}**
ipv6 address global-id {generate | globalID}
ipv6 address local-unicast [global-id globalID] [subnet-id subnetID] {interface-id interfaceID | eui-64} [prefix-length prefixLength] {if-name | loopback}
[no] ipv6 address local-unicast [global-id globalID] [subnet-id subnetID] {interface-id interfaceID | eui-64} [prefix-length prefixLength] {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 stale-lifetime *stale-lifetime*
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 static-route *ipv6_prefix/prefix_length* gateway *ipv6_address* [*if_name*][metric *metric*][tag *tag-num*][name *tag-name*]
no ipv6 static-route *ipv6_prefix/prefix_length* gateway *ipv6_address* [*if_name*][metric *metric*][tag *tag-num*][name *tag-name*]
ipv6 route-pref {static | ospf | rip | ebgp | ibgp} *value*
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]
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 route-pref
show iv6p router database [protocol *type* | gateway *ipv6_address* | dest *ipv6_prefix/prefix_length*]
show ipv6 tcp ports
show ipv6 traffic [if_name]
clear ipv6 traffic
show ipv6 tunnel
show ipv6 udp ports
show ipv6 information
ipv6 redist {local | static | rip | ospf | isis | bgp} into {rip | ospf | isis | bgp} route-map *route-map-name*
[status {enable | disable}]
ipv6 access-list *access-list-name*
no ipv6 access-list access-list-name
ipv6 access-list access-list-name address address/prefixLen [action {permit | deny}] [redist-control {all-subnets | no-subnets | aggregate}]
no ipv6 access-list access-list-name address address/*prefixLen*
show ipv6 redist [rip | ospf | bgp]
show ip access-list [*access-list-name*]
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}
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>]

IPsec Commands

ipsec key key_name {sa-authentication | sa-encryption} key
ipsec security-key [old_key] new_key
ipsec policy policy_name [priority priority] [source {ipv6_address [/prefix_length]} [port port]] [destination {ipv6_address [/prefix_length]}[port port]] [protocol protocol}] [in | out] [discard | ipsec | none] [description description] [no shutdown | shutdown]
no ipsec policy policy_name
ipsec policy policy_name rule index [ah | esp]
no ipsec policy policy_name rule index
ipsec sa sa_name {esp | ah} [source ipv6_address] [destination ipv6_address] [spi spi] [encryption {null | des-cbc | 3des-cbc | aes-cbc [key-size key_length] | aes-ctr [key-size key_length]}] [authentication {none | hmac-md5 | hmac-sha1 | aes-xcbc-mac}] [description description] [no shutdown | shutdown]
no ipsec sa name
show ipsec policy [policy_name]
show ipsec sa [sa_name | esp | ah]
show ipsec key {sa-encryption | sa-authentication}
show ipsec ipv6 statistics

RIP Commands

ip load rip
ip rip status {enable | disable}
ip rip interface *interface_name*
no ip rip interface *interface_name*
ip rip interface *interface_name* status {enable | disable}
ip rip interface *interface_name* metric *value*
ip rip interface *interface_name* send-version {none | v1 | v1compatible | v2}
ip rip interface *interface_name* 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 interface *interface_name* auth-type {none | simple | md5}
ip rip interface *interface_name* auth-key *string*
ip rip update-interval *seconds*
ip rip invalid-timer *seconds*
ip rip garbage-timer *seconds*
ip rip holddown-timer *seconds*
show ip rip
show ip rip routes **[***ip_address ip_mask***]**
show ip rip interface **[***interface_name***]**
show ip rip peer [*ip_address*]

RDP Commands

ip router-discovery {enable | disable}
ip router-discovery interface *name* [enable | disable]
no router-discovery interface *name*
ip router-discovery interface *name* advertisement-address {all-systems-multicast | broadcast}
ip router-discovery interface *name* max-advertisement-interval *seconds*
ip router-discovery interface *name* min-advertisement-interval *seconds*
ip router-discovery interface *name* advertisement-lifetime *seconds*
ip router-discovery interface *name* preference-level *level*
show ip router-discovery
show ip router-discovery interface [*name***]**

BFD Commands

ip bfd-std status {enable | disable}
ip bfd-std transmit transmit-interval
ip bfd-std receive receive-interval
ip bfd-std mode {echo-only | demand echo {enable | disable} | asynchronous echo {enable|disable}}
ip bfd-std echo interval echo-interval
ip bfd-std 12-hold-timer l2-holdtimer-interval
ip bfd-std interface interface_name
no ip bfd-std interface interface_name
ip bfd-std interface interface_name status {enable | disable}
ip bfd-std interface interface_name transmit transmit-interval
ip bfd-std interface interface_name receive receive-interval
ip bfd-std interface interface_name multiplier multiplier_value
ip bfd-std interface interface_name echo-interval echo-interval
ip bfd-std interface interface_name mode {echo-only | demand [echo {enable | disable}] | asynchronous [echo {enable|disable}}
ip bfd-std interface interface_name 12-hold-timer l2-holdtimer-interval
ip ospf bfd-std status {enable | disable}
ip ospf bfd-std all-interfaces
no ip ospf bfd-std all-interfaces
ip ospf interface *interface-name* bfd-std {enable | disable}
ip ospf interface *interface-name* bfd-std drs-only
ip ospf interface *interface-name* bfd-std all-nbrs
ip bgp bfd-std status {enable | disable}
ip bgp bfd-std all-neighbors

no ip bgp bfd-std all-neighbors
ip bgp neighbor name bfd-std {enable | disable}
vrrp bfd-std {enable | disable}
vrrp track num address address bfd-std {enable| disable}
ip static-route all bfd-std {enable| disable}
ip static-routes ip-address/prefixLen gateway ip-address bfd-std status {enable| disable}
show ip bfd-std
show ip bfd-std interfaces [interface-name]
show ip bfd-std sessions
show ip bfd-std session neighbor_address

DHCP and DHCPv6 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 pxe-support {enable | disable}
ip helper traffic-suppression {enable | disable}
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 option-82 format {base-mac | system-name | user-string *string* | *interface-alias* | *auto-interface-alias}*
ip helper dhcp-snooping option-82 format ascii circuit-id {base-mac | system-name | vlan | user-string *string* | *interface-alias* | *cvlan} {delimiter character}*
no ip helper dhcp-snooping option-82 format ascii circuit-id
ip helper dhcp-snooping option-82 format ascii remote-id {base-mac | system-name | vlan | user-string *string* | *interface-alias* | *cvlan} {delimiter character}*
no ip helper dhcp-snooping option-82 format ascii remote-id
ip helper dhcp-snooping bypass option-82-check {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 linkagg *num* {block | client-only | trust| ip-source-filtering}
ip helper dhcp-snooping port *slot1*/*port1*[-*port1a*] traffic-suppression {enable | disable}
ip helper dhcp-snooping port *slot1*/*port1*[-*port1a*] ip-source-filtering {enable | disable}
ip helper dhcp-snooping port binding {[enable | disable] | [*mac_address* **port** *slot/port* address ip_address vlan vlan_id]}
no ip helper dhcp-snooping port binding mac_address port slot/port address ip_address vlan *vlan_id*
ip helper dhcp-snooping ip-source-filter {vlan num | port *slot*/*port*[-*port2*] | linkagg num} {enable | disable}
ip helper dhcp-snooping port binding timeout *seconds*
ip helper dhcp-snooping port binding action {purge | renew}
ip helper dhcp-snooping binding persistency {enable | disable}
ip helper boot-up {enable | disable}
ip helper boot-up enable {BOOTP | DHCP}
ip udp relay {BOOTP | NBDD | NBNSNBDD | DNS | TACACS | TFTP | NTP | *port* [port_num | *name*]} {vlan vlan_id | address ip_address}
no ip udp relay {BOOTP | NBDD | NBNSNBDD | DNS | TACACS | TFTP | NTP | *port* [port_num | *name*]} {vlan vlan_id | address ip_address}
ip udp relay {BOOTP | NBDD | NBNSNBDD | DNS | TACACS | TFTP | NTP | port *port_num*} vlan *vlan_id*
no ip udp relay {BOOTP | NBDD | NBNSNBDD | DNS | TACACS | TFTP | NTP | port *port_num*} vlan *vlan_id*
ipv6 helper address *ipv6_address*
ipv6 helper no address [*ipv6_address*]
ipv6 helper standard
ipv6 helper per-vlan only
ipv6 helper address *ipv6_address* vlan *vlan_id*
ipv6 helper no address *ipv6_address* vlan *vlan_id*
ipv6 helper maximum hops *hops*
ipv6 helper dhcp-snooping {enable | disable}
ipv6 helper dhcp-snooping vlan *vlan_id*
no ipv6 helper dhcp-snooping vlan *vlan_id*
ipv6 helper dhcp-snooping port slot / *port1 [- port 1a*] {block | client-only-trusted | client-only-untrusted | trusted}
ipv6 helper dhcp-snooping linkagg num {block | client-only-trusted | client-only-untrusted | trusted}
ipv6 helper dhcp-snooping binding [enable | disable]
ipv6 helper dhcp-snooping binding timeout seconds
ipv6 helper dhcp-snooping binding action {purge | renew}
ipv6 helper dhcp-snooping binding persistency {enable | disable}
ipv6 helper interface-id prefix string
ipv6 helper no interface-id prefix
ipv6 helper remote-id format { base-mac | system-name | vlan | user-string string | interface-alias | auto-interface-alias | disable}
ipv6 helper remote-id enterprise-number num
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*]
dhcp-server {enable | disable | restart}
clear dhcp-server statistics
show dhcp-server leases [ip_address | mac_address] [type {static | dynamic}]
show dhcp-server statistics [packets | hosts | subnets | all]
show ip helper dhcp-snooping ip-source-filter {vlan | port}
show ipv6 helper
show ipv6 helper stats
ipv6 helper no stats
show ipv6 helper dhcp-snooping vlan
show ipv6 helper dhcp-snooping port
show ipv6 helper dhcp-snooping binding

VRRP Commands

vrrp *vrid vlan_id* **[**enable | disable | on | off] [priority *priority*] [preempt | no preempt] [[advertising] interval *seconds*]
no vrrp *vrid vlan_id*
vrrp *vrid vlan_id* address *ip_address*
vrrp *vrid vlan_id* no address *ip_address*
vrrp track *track_id* [enable | disable] [priority *value*] [ipv4-interface *name* | ipv6-interface *name* |
port *slot*/*port* | address *address*]
no vrrp track *track_id*
vrrp *vrid vlan_id* track-association *track_id*
vrrp *vrid vlan_id* no track-association *track_id*
vrrp trap
no vrrp trap
vrrp delay *seconds*
vrrp3 *vrid vlan_id* [enable | disable | on | off] [priority *priority*] [preempt | no preempt][accept | no accept] [[advertising] interval *centiseconds***]**
no vrrp3 *vrid vlan_id*
vrrp3 *vrid vlan_id* address *ipv6_address*
vrrp3 *vrid vlan_id* no address *ipv6_address*
vrrp3 trap
no vrrp3 trap
vrrp3 *vrid vlan_id* track-association *track_id*
vrrp3 *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*]
show vrrp3 [*vrid*]
show vrrp3 [*vrid*] statistics
show vrrp3 [*vrid*] track-association [*track_id*]

OSPF Commands

ip ospf status {enable | disable}
ip load ospf
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 default-originate {only | always} [metric-type {type1 | type2}] [metric *value*]
no ip ospf default-originate
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 area *area_id* [summary {enable | disable}] | [type {normal | stub | nssa}]
no ip ospf area *area_id*
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 *interface_name*
no ip ospf interface *interface_name*
ip ospf interface *interface_name* status {enable | disable}
no ip ospf interface *interface_name* status {enable | disable}
ip ospf interface *interface_name* area *area_id*
ip ospf interface *interface_name* auth-key *key_string*

ip ospf interface *interface_name* auth-type [none | simple | md5]
ip ospf interface *interface_name* dead-interval *seconds*
ip ospf interface *interface_name* hello-interval *seconds*
ip ospf interface *interface_name* md5 *key_id* [enable | disable]
ip ospf interface *interface_name* md5 *key_id* key *key_string*
ip ospf interface *interface_name* type {point-to-point | point-to-multipoint | broadcast | non-broadcast}
ip ospf interface *interface_name* cost *cost*
ip ospf interface *interface_name* poll-interval *seconds*
ip ospf interface *interface_name* priority *priority*
ip ospf interface *interface_name* retrans-interval *seconds*
ip ospf interface *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 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 [*interface_name*]
show ip ospf restart

OSPFv3 Commands

ipv6 ospf status {enable | disable}
ipv6 load ospf
ipv6 ospf host *ipv6_address* [*area area_id*] [metric *metric*]
no ipv6 ospf host *ipv6_address area area_id*
ipv6 ospf mtu-checking
no ipv6 ospf mtu-checking
ipv6 ospf route-tag *tag*
ipv6 ospf spf-timer [delay *delay_seconds*] [hold *hold_seconds*]
ipv6 ospf virtual-link area *area_id* **router** *router_id* [dead-interval *seconds*] [hello-interval *seconds*] [retrans-interval *seconds*] [transit-delay *seconds*]
no ipv6 ospf virtual-link area *area_id* router *router_id*
ipv6 ospf area area_id **[t**ype {normal | stub [default-metric metric**]}]**
no ipv6 ospf area *area_id*
ipv6 ospf interface *interface_name*
no ipv6 ospf interface *interface_name*
ipv6 ospf interface *interface_name* status {enable | disable}
no ipv6 ospf interface *interface_name*
ipv6 ospf interface *interface_name* area *area_id*
ipv6 ospf interface *interface_name* dead-interval *seconds*
ipv6 ospf interface *interface_name* hello-interval *seconds*
ipv6 ospf interface *interface_name* cost *cost*
ip ospf interface *interface_name* priority *priority*
ipv6 ospf interface *interface_name* retrans-interval *interval*
ipv6 ospf interface *interface_name* transit-delay *delay*
show ipv6 ospf
show ipv6 ospf border-routers [area *area_id*] [router *router_id*]
show ipv6 ospf host [*ipv6_address*]
show ipv6 ospf lsdb [area *area_id*] [rtr | net | netsum | asbrsum] [linkstate-id *ls_id*] [router-id *router_id*]
show ipv6 ospf neighbor [router *ipv4_address*][interface *interface_name*]
show ipv6 ospf routes [prefix ipv6_address_prefix][gateway gateway]
show ipv6 ospf virtual-link [*router_id*]
show ipv6 ospf area [*area_id*]
show ipv6 ospf interface [*interface_name*]

IS-IS Commands

ip load isis
ip isis status {enable | disable}
ip isis area-id *area address*
no ip isis area-id *area address*
ip isis level-capability {level-1 | level-2 | level-1/2}
ip isis auth-check {enable | disable}
ip isis auth-type {simple {key *key* | encrypt-key *encrypt-key*} | md5 {key *key* | **encrypt-key** *encrypt-key*} | none}
ip isis csnp-auth
no ip isis csnp-auth
ip isis hello-auth
no ip isis hello-auth
ip isis psnp-auth
no ip isis psnp-auth

ip isis lsp-lifetime *seconds*
no ip isis lsp-lifetime
ip isis lsp-wait {max-wait | initial-wait | second-wait} *seconds*
no ip isis lsp-wait {max-wait | initial-wait | second-wait}
ip isis spf-wait {max-wait *seconds* | initial-wait *milliseconds*| second-wait *milliseconds*}
no ip isis spf-wait {max-wait | initial-wait | second-wait}
ip isis summary-address {*ip-prefix/mask* | *ip-prefix* [/*netmask*]} {level-1 | level-2 | level-1/2}
no ip isis summary-address {*ip-prefix/mask* | *ip-prefix* [/*netmask*]}
ip isis overload [timeout *seconds*]
no ip isis overload [timeout]
ip isis overload-on-boot [timeout *seconds*]
no ip isis overload-on-boot [timeout *seconds*]
ip isis graceful-restart
no ip isis graceful-restart
ip isis graceful-restart helper {enable | disable}
ip isis strict-adjacency-check {enable | disable}
ip isis level {1 | 2} auth-type {simple {key *key* | *encrypt-key encrypt-key*} | md5 {key *key* | *encrypt-key encrypt-key*} | none}
ip isis level {1 | 2} hello-auth
no ip isis level {1 | 2} hello-auth
ip isis level {1 | 2} csnp-auth
no ip isis level {1 | 2} csnp-auth
ip isis level {1 | 2} psnp-auth
no ip isis level {1 | 2} psnp-auth
ip isis level {1 | 2} wide-metrics-only
no ip isis level {1 | 2} wide-metrics-only

show ip isis routes

show ip isis spf [detail]
show ip isis spf-log [detail]
show ip isis statistics
show ip isis status
show ip isis summary-address [*ip-addr* [/*mask*]]
ip isis interface interface_name
no ip isis interface interface_name
ip isis interface interface_name status {enable | disable}
ip isis interface interface_name interface-type {broadcast | point-to-point}
ip isis interface interface_name csnp-interval seconds
no ip isis interface interface_name csnp-interval
ip isis interface interface_name hello-auth-type {simple {key key | encrypt-key encrypt-key} | md5 {key key | encrypt-key encrypt-key} | none}
ip isis interface interface_name level-capability [level-1 | level-2 | level-1/2]
ip isis interface interface_name lsp-pacing-interval milliseconds
no ip isis interface interface_name lsp-pacing-interval
ip isis interface interface_name passive
no ip isis interface interface_name passive
ip isis interface interface_name retransmit-interval seconds
no ip isis interface interface_name retransmit-interval
ip isis interface interface_name default-type
ip isis interface interface_name level [1 | 2] hello-auth-type {simple {key key | encrypt-key encrypt-key} | md5 {key key | encrypt-key encrypt-key} | none}
ip isis interface interface_name level [1 | 2] hello-interval seconds
no ip isis interface interface_name level [1 | 2] hello-interval
ip isis interface interface_name level [1 | 2] hello-multiplier number
no ip isis interface interface_name level [1 | 2] hello-multiplier
ip isis interface interface_name level [1 | 2] metric number
no ip isis interface interface_name level [1 | 2] metric
ip isis interface interface_name level [1 | 2] passive
no ip isis interface interface_name level [1 | 2] passive
ip isis interface interface_name level [1 | 2] priority number
no ip isis interface interface_name level [1 | 2] priority
show ip isis interface [interface_name] [detail]
clear ip isis adjacency [system-id *nbr-sys-id*]
clear ip isis lsp-database [system-id *sys-id*]
clear ip isis spf-log
clear ip isis statistics

BGP Commands

ip load bgp
ip bgp status {enable | disable}
ip bgp unicast
no ip bgp unicast
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 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_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 *peer_address* in-prefix6list pfx_list_name
ip bgp neighbor *peer_address* out-prefix6list pfx_list_name
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 prefix6-list *pfx_list_name prefix6/pfx_length [action{permit|deny}] [status{enable|disable}] [ge[{masklength}]] [le[{masklength}]]*
no ip bgp policy prefix6-list *pfx_list_name prefix6/pfx_length [action{permit|deny}] [status{enable|disable}] [ge[{masklength}]] [le[{masklength}]]*
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*
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 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 *ipv4_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 prefix6-list [*pfx_list_name[{prefix6/prefix_length}]]*
show ip bgp policy route-map [*name*] [*sequence_number*]
ip bgp graceful-restart
no ip bgp graceful-restart
ip bgp graceful-restart restart-interval [*seconds*]
ipv6 bgp unicast
no ipv6 bgp unicast
ip bgp neighbor *ip_address* activate-ipv6
no ip bgp neighbor i*p_address* activate-ipv6
ip bgp neighbor *ip_address* ipv6-nexthop *ipv6_address*
show ipv6 bgp path [ipv6-addr *ipv6_address/prefix_length*]
show ipv6 bgp routes
ipv6 bgp network *ipv6_address/prefix_length*
no ipv6 bgp network *ipv6_address/prefix_length*
ipv6 bgp network *ipv6_address/prefix_length* [community {none | *num* | *num:num*}]
ipv6 bgp network *ipv6_address/prefix_length* **[**local-preference num]
ipv6 bgp network *ipv6_address/prefix_length* **[**metric num]
ipv6 bgp network *ipv6_address/prefix_length* **[**status {enable | disable}]
show ipv6 bgp network **[***ipv6_address/prefix_length***]**
ipv6 bgp neighbor *ipv6_address*
no ipv6 bgp neighbor *ipv6_address*
ipv6 bgp neighbor *peer6_address* clear soft {in | out}
ipv6 bgp neighbor *peer6_address* soft-reconfiguration
no ipv6 bgp neighbor *peer6_address* soft-reconfiguration
ipv6 bgp neighbor *peer6_address* in-prefix6list pfx_list_name
ipv6 bgp neighbor *peer6_address* out-prefix6list pfx_list_name
ipv6 bgp neighbor *ipv6_address* [activate-ipv6]
no ipv6 bgp neighbor i*pv6_address* [activate-ipv6]
ipv6 bgp neighbor *ipv6_address* [ipv6-nexthop *ipv6_address***]**
ipv6 bgp neighbor *ipv6_address* **[**status {enable | disable}]
ipv6 bgp neighbor *ipv6_address* [remote-as *num***]**
ipv6 bgp neighbor *ipv6_address* [timers *num num*]
ipv6 bgp neighbor *ipv6_address* [maximum-prefix *num* [warning-only]]
no ipv6 bgp neighbor *ipv6_address* [maximum-prefix *num* [warning-only]]
ipv6 bgp neighbor *ipv6_address* [next-hop-self]
no ipv6 bgp neighbor *ipv6_address* [next-hop-self]
ipv6 bgp neighbor *ipv6_address* [conn-retry-interval *num***]**
ipv6 bgp neighbor *ipv6_address* [default-originate]
no ipv6 bgp neighbor *ipv6_address* [default-originate]
ipv6 bgp neighbor *ipv6_address* [update-source *interface_name***]**

no ipv6 bgp neighbor *ipv6_address* [update-source *interface_name*]
ipv6 bgp neighbor *ipv6_address* [ipv4-nexthop *ip_address*]
show ipv6 bgp neighbors [*ipv6_address*]
show ipv6 bgp neighbors statistics [*ipv6_address*]
show ipv6 bgp neighbors timers [*ipv6_address*]
show ipv6 bgp neighbors policy *ipv6_address*

Server Load Balancing Commands

ip slb admin {enable | disable}
ip slb reset statistics
ip slb cluster name {vip ip_address | **condition** string} **[l3 | l2]**
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 probe *probe_name*
ip slb server ip *ip_address* cluster *cluster_name* [admin status {enable | disable}] [weight *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* {tcp | udp} send *send_string*
ip slb probe *probe_name* {http | https | tcp | udp} expect *expect_string*
show ip slb
show ip slb clusters [statistics]
show ip slb cluster *name* [statistics]
show ip slb cluster *cluster_name* server *ip_address*
show ip slb servers
show ip slb probes [*probe_name*]

IP Multicast Switching Commands

ip multicast [vlan *vid*] status [{enable | disable}]
ip multicast flood-unknown {enable | disable}
ip multicast [vlan *vid*] querier-forwarding [{enable | disable}]
no ip multicast [vlan *vid*] querier-forwarding
ip multicast [vlan *vid*] version [*version*]
ip multicast max-group [num] [action {none | drop | replace}]
ip multicast vlan vid max-group [num] [action {none | drop | replace}]
ip multicast port slot | port max-group [num] [action {none | drop | replace}]
ip multicast static-neighbor vlan *vid* port *slot*/*port*
no ip multicast static-neighbor vlan *vid* port *slot*/*port*
ip multicast static-querier vlan *vid* port *slot*/*port*
no ip multicast static-querier vlan *vid* port *slot*/*port*
ip multicast static-group *ip_address* vlan *vid* port *slot*/*port receiver-vlan num*
no ip multicast static-group *ip_address* vlan *vid* port *slot*/*port receiver-vlan num*
ip multicast [vlan *vid*] query-interval [*seconds*]
ip multicast [vlan vid] last-member-query-interval [tenths-of-seconds]
ip multicast [vlan *vid*] query-response-interval [*tenths-of-seconds*]
ip multicast [vlan *vid*] unsolicited-report-interval [*seconds*]
ip multicast [vlan *vid*] router-timeout [*seconds*]
ip multicast [vlan *vid*] source-timeout [*seconds*]
ip multicast [vlan *vid*] querying [{enable | disable}]
ip multicast [vlan *vid*] robustness [*robustness*]
ip multicast [vlan *vid*] spoofing [{enable | disable}]
ip multicast [vlan *vid*] zapping [{enable | disable}]
ip multicast [vlan *vid*] proxying [enable | disable]
ip multicast helper-address [ip-address]
ipv6 multicast [vlan *vid*] status [{enable | disable}]
ipv6 multicast [vlan *vid*] querier-forwarding [{enable | disable}]
no ipv6 multicast [vlan *vid*] querier-forwarding
ipv6 multicast [vlan *vid*] version [*version*]
ipv6 multicast max-group [num] [action {none | drop | replace}]
ipv6 multicast vlan vid max-group [num] [action {none | drop | replace}]
ipv6 multicast port slot | port max-group [num] [action {none | drop | replace}]
ipv6 multicast static-neighbor vlan *vid* port *slot*/*port*
no ipv6 multicast static-neighbor vlan *vid* port *slot*/*port*
ipv6 multicast static-querier vlan *vid* port *slot*/*port*

no ipv6 multicast static-querier vlan *vid* port *slot*/*port*
ipv6 multicast static-group *ip_address* vlan *vid* port *slot*/*port*
no ipv6 multicast static-group *ip_address* vlan *vid* port *slot*/*port*
ipv6 multicast [vlan *vid*] query-interval [*seconds*]
ipv6 multicast [vlan *vid*] last-member-query-interval [*milliseconds*]
ipv6 multicast [vlan *vid*] query-response-interval [*milliseconds*]
ipv6 multicast [vlan *vid*] unsolicited-report-interval [*seconds*]
ipv6 multicast [vlan *vid*] router-timeout [*seconds*]
ipv6 multicast [vlan *vid*] source-timeout [*seconds*]
ipv6 multicast [vlan *vid*] querying [{enable | disable}]
ipv6 multicast [vlan *vid*] robustness [*robustness*]
ipv6 multicast [vlan *vid*] spoofing [{enable | disable}]
ipv6 multicast [vlan *vid*] zapping [{enable | disable}]
ipv6 multicast [vlan *vid*] proxying [enable | disable]
Configure the static-ssm mapping in the system. This is a global command.
ipv6 multicast static-ssm-map [group group_address] / prefix [source source_address]
no ipv6 multicast static-ssm-map [group group_address] / prefix [source source_address]
Displays the configured static-ssm group and source mapping in the system.
show ip multicast static-ssm-map
show ip multicast [vlan *vid*]
show ip multicast port [slot/*port*]
show ip multicast forward [*ip_address*]
show ip multicast neighbor
show ip multicast querier
show ip multicast group [*ip_address*]
show ip multicast source [*ip_address*]
show ip multicast tunnel [address]
show ipv6 multicast [vlan *vid*]
show ipv6 multicast port [slot/*port*]
show ipv6 multicast forward [*ipv6_ddress*]
show ipv6 multicast neighbor
show ipv6 multicast querier
show ipv6 multicast group [*ip_address*]
show ipv6 multicast source [*ip_address*]
show ipv6 multicast tunnel [*address*]

IP Multicast VLAN Commands

vlan ipmvlan *ipmvlan-id* [{enable | disable} | [{1x1 | flat} stp {enable | disable}]] [name *name-string*]
no vlan ipmvlan *ipmvlan-id* [-*ipmvlan-id2*]
vlan ipmvlan *ipmvlan-id* ctag {*ctag* | *ctag1-ctag2*}
no vlan ipmvlan *ipmvlan-id* ctag {*ctag* | *ctag1-ctag2*}
vlan ipmvlan *ipmvlan-id* address {*ipv4addr/prefixlen* | *ipv4addr-ipv4addr* | *ip_address* | *mask mask}*
no vlan ipmvlan *ipmvlan-id* address {*ipv4addr/prefixlen* | *ipv4addr-ipv4addr* | *ip_address* | *mask mask}*
vlan ipmvlan *ipmvlan-id* sender-port {port slot/port[-*port2*] | linkagg *agg_num* [-*agg_num2*]}
no vlan ipmvlan *ipmvlan-id* sender-port {port slot/port[-*port2*] | linkagg *agg_num* [-*agg_num2*]}
vlan ipmvlan *ipmvlan-id* receiver-port {port slot/port[-*port2*] | linkagg *agg_num* [-*agg_num2*]} [receiver-vlan num]
no vlan ipmvlan *ipmvlan-id* receiver-port {port slot/port[-*port2*] | linkagg *agg_num* [-*agg_num2*]} [receiver-vlan num]
show vlan ipmvlan [*ipmvlan-id*] c-tag
show vlan ipmvlan [ipmvlan-id] address [ipv4 | ipv6]
show vlan ipmvlan [ipmvlan-id] port-config
show vlan ipmvlan port-config [slot/port | agg_num]

DVMRP Commands

ip load dvmrp
ip dvmrp status {enable | disable}
ip dvmrp flash-interval *seconds*
ip dvmrp graft-timeout *seconds*
ip dvmrp interface *interface_name*
no ip dvmrp interface *interface_name*
ip dvmrp interface *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_name remote_address*
no ip dvmrp tunnel *local_name remote_address*
ip dvmrp tunnel *interface_name remote_address* 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

PIM Commands

ip load pim
ip pim sparse status {enable | disable}
ip pim {dense | sparse} bfd-std status {enable | disable}
ip pim interface name bfd-std status{enable | disable}
ip pim dense redundant-path {enable | disable}
ip pim dense status {enable | disable}
ip pim static-rp *group_address/prefix_length rp_address* [[no] override] [priority *priority*]
ip pim rp-threshold *bps*
ip pim max-rps *number*
ip pim probe-time *seconds*
ip pim register checksum {header | full}
ip pim register-suppress-timeout *seconds*
ip pim spt status {enable | disable}
ip pim state-refresh-interval *seconds*
ip pim state-refresh- limit *ticks*
ip pim state-refresh- ttl *num*
show ip pim sparse
show ip pim dense
show ip pim neighbor [*ip_address*]
show ip pim candidate-rp
show ip pim group-map [bsr | static-rp | ssm | dense]
show ip pim interface [*if_name*]
show ip pim static-rp
ipv6 pim sparse status {enable | disable}
ipv6 pim cbsr bsr_address [priority bsr_priority] [mask-length masklen] [scope scope_value]
no ipv6 pim cbsr bsr_address [priority bsr_priority] [mask-length masklen] [scope scope_value]
ipv6 pim static-rp group_address/prefix_length rp_address [[no] override] [priority priority]
ipv6 pim spt status {enable | disable}
show ipv6 pim neighbor [ipv6_address] [if_name]
show ipv6 pim cbsr [scope scope_value]
show ipv6 pim bsr [scope scope_value]

Multicast Routing Commands

ip mroute-boundary *if_name scoped_address mask*
no ip mroute-boundary *if_name scoped_address mask*
ipv6 mroute-boundary *if_name* scope *scope_value*
no ipv6 mroute-boundary *if_name* scope *scope_value*
ip mroute interface *if_ name* ttl *threshold*
show ip mroute-boundary
show ipv6 mroute-boundary
show ip mroute
show ip mroute interface {*interface_name*}
show ipv6 mroute interface {*interface_name*}
show ip mroute-nexthop

QoS Commands

qos {enable | disable}
qos trust ports
qos no trust ports
qos default servicing mode {strict-priority | wrr [*w0 w1 w2 w3 w4 w5 w6 w7*] | priority-wrr [*w0 w1 w2 w3 w4 w5 w6 w7*] | drr] [*w0 w1 w2 w3 w4 w5 w6 w7*]}
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 default bridged disposition {accept | deny | drop}
qos default routed disposition {accept | deny | drop}
qos default multicast disposition {accept | deny | drop}
qos user-port {filter | shutdown} {spoof | bgp | bpdu | rip | ospf | vrrp | dvmrp | pim | isis | dhcp-server | dns-reply}
qos no user-port {filter | shutdown}
qos dei {ingress | egress}
qos no dei {ingress | egress}
qos stats interval *seconds*
qos nms priority
qos no nms priority
qos phones [priority *priority_value* | trusted]
qos no phones
qos quarantine mac-group *mac_group*
qos no quarantine mac-group
qos quarantine path *url*
qos no quarantine path
qos quarantine page
qos no quarantine page

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 [egress]
qos port *slot/port* reset
qos port *slot/port*
qos port *slot/port* trusted
qos port *slot/port* no trusted
qos port *slot/port* servicing mode {strict-priority | wrr [*w0 w1 w2 w3 w4 w5 w6 w7*] | priority-wrr [*w0 w1 w2 w3 w4 w5 w6 w7*] | drr [*w0 w1 w2 w3 w4 w5 w6 w7*] | default}
qos port slot/port qn {minbw | maxbw} kbps
qos port slot/port no qn {minbw | maxbw} kbps
qos port *slot/port* maximum egress-bandwidth *bps*
qos port *slot/port* no maximum egress-bandwidth
qos port *slot/port* maximum ingress-bandwidth *bps*
qos port *slot/port* no maximum ingress-bandwidth
qos port *slot/port* default 802.1p *value*
qos port *slot/port* default dscp *value*
qos port *slot/port* default classification {802.1p | dscp}
qos port *slot/port* dei {ingress | egress}
qos port *slot/port* no dei {ingress | egress}
qos port *slot/port* monitor
qos port *slot/port* no monitor
show qos port [*slot/port*] [statistics]
show qos port monitor
show qos queue [*slot/port*]
show qos slice {ingress | egress} [*slot/slice*]
show qos log
show qos config
show qos statistics

QoS Policy Commands

aclman
policy rule *rule_name* [enable | disable] [precedence *precedence*] [condition *condition*] [action *action*] [validity period *name* | no validity period] [save] [log [log-interval *seconds*]] [count {packets | bytes}] [trap | no trap] [default-list | no default-list]
no policy rule *rule_name*
policy rule *rule_name* [no reflexive] [no save] [no log]
policy validity period *name* [[no] days *days*] [[no] months *months*] [[no] hours *hh:mm* to *hh:mm* | no hours] [interval *mm:dd:yyyy hh:mm* to *mm:dd:yyyy hh:mm* | no interval]
no policy validity period *name*
policy list *list_name* type [unp | egress] rules *rule_name* [*rule_name2*...] [enable | disable]
no policy list *list_name*
policy list *list_name* **no rules** *rule_name* [*rule_name2*...]
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 vlan group *group_name vlan_id*[-*vlan_id*] [*vlan_id*[-*vlan_id*]...]
no policy vlan group *group_name*
policy vlan group *group_name* no *vlan_id*[-*vlan_id*] [*vlan_id*[-*vlan_id*]...]
policy map group *map_group* {*value1*:*value2*...}
no policy map group *map_group*
policy map group no {*value1*:*value2*...}
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 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* source ipv6 {any | *ipv6_address* [mask *netmask*]}
policy condition *condition_name* no source ipv6
policy condition *condition_name* destination ip *ip_address* [mask *netmask*]
policy condition *condition_name* no destination ip
policy condition *condition_name* destination ipv6 {any | *ipv6_address* [mask *netmask*]}
policy condition *condition_name* no destination ipv6
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* established
policy condition *condition_name* no established
policy condition *condition_name* tcpflags [any | all] {F | S | R | P | A | U | E | W} mask {F | S | R | P | A | U | E | W}
policy condition *condition_name* no tcpflags
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* icmptype *type*
policy condition *condition_name* no icmptype
policy condition *condition_name* icmpcode *code*
policy condition *condition_name* no icmpcode
policy condition *condition_name* ip protocol *protocol*
policy condition *condition_name* no ip protocol
policy condition *condition_name* ipv6
policy condition *condition_name* no ipv6
policy condition *condition_name* nh *next_header_value*
policy condition *condition_name* no nh
policy condition *condition_name* flow-label *flow_label_value*
policy condition *condition_name* no flow-label
policy condition *condition_name* tos *tos_value* [mask *tos_mask*]
policy condition *conditioning* no tos
policy condition *condition_name* dscp {*dscp_value*[-*value*]} [mask *dscp_mask*]
policy condition *condition_name* no dscp
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 mac group
policy condition *condition_name* source vlan *vlan_id*
policy condition *condition_name* no source vlan
policy condition *condition_name* source vlan group *vlan_group*
policy condition *condition_name* no source vlan group
policy condition *condition_name* inner source vlan *vlan_id*
policy condition *condition_name* no inner source vlan
policy condition *condition_name* inner source vlan group *vlan_group*
policy condition *condition_name* no inner source vlan group
policy condition *condition_name* destination vlan *vlan_id*
policy condition *condition_name* no destination vlan
policy condition *condition_name* 802.1p *802.1p_value*[-*802.1p_value*]
policy condition *condition_name* no 802.1p
policy condition *condition_name* inner 802.1p *802.1p_value*[-*802.1p_value*]

policy condition *condition_name* no inner 802.1p
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* vrf {*vrf_name* | **default}**
policy condition *condition_name* no vrf
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 depth *bytes*
policy action *action_name* no maximum depth
policy action action_name cir bps [cbs **byte**] [pir bps] [pbs **byte**] [counter-color [red-nonred | green-nongreen | green-red | green-yellow | red-yellow]]
policy action action_name no cir bps
policy action action_name no pir bps
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* permanent gateway ip *ip_address*
policy action *action_name* no permanent gateway ip
policy action *action_name* port-disable
policy action *action_name* no port-disable
policy action *action_name* redirect port *slot/port*
policy action *action_name* no redirect port
policy action *action_name* redirect linkagg *link_agg*
policy action *action_name* no redirect linkagg
policy action *action_name* no-cache
policy action *action_name* no no-cache
policy action *action_name* [ingress | egress | ingress egress] mirror *slot/port*
policy action *action_name* no mirror *slot/port*
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 vlan 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 active policy rule [*rule_name*] meter-statistics
show [applied] [bridged | routed | multicast] policy rule [*rule_name*]
show policy validity period [*name*]
show active policy list [*list_name*]
show [applied] policy list [*list_name*]

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

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 bypass {enable | disable}
802.1x slot/port non-supplicant allow-eap {pass | fail | noauth | none}
802.1x pass-through {enable | disable}
captive-portal pass-through {enable | disable}
802.1x slot/port supplicant policy authentication [[pass] {group-mobility | user-network-profile profile_name | vlan vid | default-vlan | block | captive-portal}...] [[fail] {user-network-profile profile_name | vlan vid | block | captive-portal}...]
802.1x slot/port non-supplicant policy authentication [[pass] {group-mobility | user-network-profile profile_name | vlan vid | default-vlan | block | captive-portal}] [[fail] {group-mobility | user-network-profile profile_name | vlan vid | default-vlan | block | captive-portal}]
802.1x slot/port non-supplicant policy {group-mobility | user-network-profile profile_name | vlan vid | default-vlan | block | captive-portal}
802.1x slot/port {supplicant | non-supplicant} policy default
802.1x slot/port captive-portal policy authentication pass {group-mobility | user-network-profile profile_name | vlan vid | default-vlan | block}] [fail] {group-mobility | vlan vid | default-vlan | block}
802.1x slot/port captive-portal session-limit time
802.1x captive-portal name cp_url_name
802.1x captive-portal no name
802.1x slot/port captive-portal inactivity-logout {enable | disable}
802.1x slot/port captive-portal retry-count retries
802.1x captive-portal address ip_address
802.1x captive-portal proxy-server-url proxy_url
802.1x captive-portal proxy-server-port proxy_port
802.1x captive-portal no proxy-server-port proxy_port
802.1x captive-portal dns-keyword-list {keyword1 [keyword2] [keyword3] [keyword4]}
802.1x captive-portal no dns-keyword-list
802.1x captive-portal success-redirect-url redirect_url
802.1x captive-portal no success-redirect-url
802.1x captive-portal fail-redirect-url redirect_url
802.1x captive-portal no fail-redirect-url
802.1x auth-server-down {enable | disable}
802.1x auth-server-down policy {user-network-profile profile_name | block}
802.1x auth-server-down re-authperiod {value}
show 802.1x [*slot/port*]
show 802.1x users [*slot/port*] [unp | detail]
show 802.1x statistics [*slot/port*]
show 802.1x device classification policies [*slot/port*]
show 802.1x non-supplicant [*slot/port*] [unp | detail]
show 802.1x rate-limit [*slot/port*]
show 802.1x auth-server-down
show 802.1x captive-portal configuration

AAA Commands

aaa radius-server *server-name* [host {*hostname* | *ip_address*} [*hostname2* | *ip_address2*]] [key *secret*] [retransmit *retries*] [timeout *seconds*] [auth-port *auth_port*] [acct-port *acct_port*] [vrf-name *vrf_name*]
no aaa radius server *server-name*
aaa radius agent preferred {default | no-loopback | *ip_address*}
no aaa radius agent preferred
aaa tacacs+-server *server-name* [host {*hostname* | *ip_address*} {*hostname2* | *ip_address2*}] [key
secret][timeout *seconds*] [port *port*]
no aaa tacacs+-server *server-name*
aaa ldap-server *server_name* [host {*hostname* | *ip_address*} [{*hostname2* | *ip_address2*}]] [*port*]
[dn *dn_name*] [password *super_password*] [base *search_base*] [type *server_type*]
[retransmit *retries*]
[timeout *seconds*] [ssl | no ssl] [port *port*]
no aaa ldap-server *server-name*
aaa ace-server *server-name* clear
system fips [*enable* | *disable*]
show system fips-status
aaa test-radius-server *server-name* type {authentication user user-name password password [method {MD5 | PAP}] | accounting user user-name}
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] *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 tacacs command-authorization {enable | disable}
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 certificate-password *password*
no aaa certificate-password *password*
aaa accounting 802.1x *server1* [*server2*...] [local]
no aaa accounting 802.1x
aaa accounting mac *server1* [*server2*...] [local]
no aaa accounting mac
aaa accounting vlan [*vlan_id*] *server1* [*server2*...] [local]
no accounting vlan [*vlan_id*]
aaa accounting session [*server_name1*] [*server_name2*...] [local]
no aaa accounting session
aaa accounting session-id {enable | disable]
aaa accounting command *server1* [*server2*...] [local]
no accounting command
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*] [console-only {enable | disable}] [SHA+AES| SHA+3DES]
no user *username*
password
user password-size min *size*
user password-expiration {*day* | disable}
user password-policy cannot-contain-username {enable | disable}
user password-policy min-uppercase *number*
user password-policy min-uppercase *number*
user password-policy min-digit *number*
user password-policy min-nonalpha *number*
user password-history *number*
user password-min-age *days*
user lockout-window *minutes*
user lockout-threshold *number*
user lockout-duration *minutes*
user {lockout | unlock}
aaa admin-logout {mac-address *mac_address* | port *slot/port* | user *user_name* | user-network-profile name *profile_name*}
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*..]
aaa user-network-profile name *profile_name* vlan *vlan-id* [hic [enable | disable]] [policy-list-name *list_name*] [maximum-ingress-bandwidth num maximum-egress-bandwidth num maximum-default-depth num]
no aaa user-network-profile name *profile_name*
aaa classification-rule mac-address *mac_address* user-network-profile name *profile_name*
aaa classification-rule no mac-address *mac_address*
aaa classification-rule mac-address-range *low_mac_address high_mac_address* user-network-profile name *profile_name*
aaa classification-rule no mac-address-range *low_mac_address*
aaa classification-rule ip-address *ip_address* [*subnet_mask*] user-network-profile name *profile_name*
aaa classification-rule no ip-address *ip_address* [*subnet_mask*]
aaa hic server-name *server* ip-address *ip_address* **secret** *secret* [role {primary | backup}] [udp-port *udp_port*]
aaa hic no server-name *server*
aaa hic redundancy background-poll-interval value
aaa hic server-failure mode {hold | pass-through}
aaa hic server-failure policy user-network-profile change unp1 to unp2
aaa hic server-failure policy user-network-profile no change
aaa hic allowed-name *server* ip-address *ip_address* **[ip-mask** *subnet_mask*]
aaa hic no allowed-name *server*
aaa hic {enable | disable}
aaa hic web-agent-url *url*
aaa hic custom-proxy-port *proxy_port*
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 authentication mac [statistics]
show aaa accounting vlan
show aaa accounting
show user [*username*]
show user password-size
show user password-expiration
show user password-policy

show user lockout-setting
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 classification-rule {mac-rule | mac-range-rule | ip-net-rule}
show aaa priv hexa [*domain or family*]
802.1x slot/port kerberos {enable | disable}
aaa kerberos mac-move {enable | disable}
aaa kerberos inactivity-timer num
aaa kerberos ip-address ip_address [udp-port num]
no aaa kerberos ip-address ip_address
aaa kerberos kerberos server-timeout num
aaa kerberos authentication-pass policy-list-name string
no aaa kerberos authentication-pass policy-list-name
aaa kerberos authentication-pass domain domain_name policy-list-name policy_list
no aaa kerberos authentication-pass domain domain_name
show aaa kerberos configuration
show aaa kerberos port [enabled | disabled| <slot/port [-port2]>]
show aaa kerberos users [port <slot/port> | <mac-address>]
show aaa kerberos statistics
show aaa kerberos port slot/port[-port2] statistics
clear aaa kerberos statistics
clear aaa kerberos port slot/port[-port2] statistics

UNP Commands

unp name *unp_name* vlan *vlan_id* [qos-policy-list *list_name*]
no unp name *unp_name*
unp {port *slot/port1*[-*port2*] | linkagg *agg_id*}
no unp {port *slot/port1*[-*port2*] | linkagg *agg_id*}
unp {port *slot/port1*[-*port2*] | linkagg *agg_id*} default-unp *unp_name*
no unp {port *slot/port1*[-*port2*] | linkagg *agg_id*} default-unp
unp {port *slot/port1*[-*port2*] | linkagg *agg_id*} mac-authentication {enable | disable}
unp {port *slot/port1*[-*port2*] | linkagg *agg_id*} mac-authentication pass-alternate unp-name *unp_name*
no unp {port *slot/port1*[-*port2*] | linkagg *agg_id*} mac-authentication pass-alternate
unp {port *slot/port1*[-*port2*] | linkagg *agg_id*} classification {enable | disable}
unp port {port *slot/port1*[-*port2*] | linkagg *agg_id*} trust-tag {enable | disable}
unp classification mac-range *low_mac_address high_mac_address* [vlan-tag *vlan_id*] unp-name *unp_name*
no unp classification mac-range *low_mac_address high_mac_address*
unp classification vlan-tag *vlan_id* unp-name *unp_name*
no unp classification vlan-tag *vlan_id*
unp dynamic-vlan-configuration {enable | disable}
unp dynamic-profile-configuration {enable | disable}
unp auth-server-down-unp *unp_name*
no auth-server-down unp
show unp [*unp_name* | sync | out-of-sync | local
show unp global configuration
show unp user [*mac_address*] [*slot/port*[-*port2*] | linkagg *agg_id*] [count]

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 *mac_address slot/port*
vlan *vid* no binding mac-port *mac_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 | 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* 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*]

Network Security Commands

netsec group *grp_name* port slot/port[-*port2*]
no netsec group *grp_name* port slot/port[-*port2*]
netsec group {*grp_name* | all} anomaly {anomaly_name | all} {{{state | log | trap | quarantine} {enable | disable}} | {period *seconds*} | {count *num*} | {sensitivity *num*}}
no netsec group *grp_name* anomaly {anomaly_name | all} {state | log | trap | quarantine | period | count | sensitivity}
show netsec [group {*grp_name* | all} | port *slot/port*[-*port2*]] [anomaly {*anomaly_name* | all}] summary
show netsec [group {*group-name* | all} | port *slot/port1*[-*port2*]] [anomaly {*anomaly_name* | all}] traffic
show netsec [group {*grp_name* | all} | port *slot/port*[-*port2*]] **statistics**
show netsec [group {*grp_name* | all}] [anomaly {*anomaly_name* | all}] config
show netsec [group {*grp_name* | all} | port *slot/port*[-*port2*]] [anomaly {*anomaly_name* | all}] **operation**
show netsec {group {*grp_name* | all} | **port** *slot/port* [-*port2*]}

Port Mapping Commands

port mapping *port_mapping_sessionid* {enable | disable}
no port mapping *port_mapping_sessionid*
port mapping session id unknown-unicast-flooding {enable | disable}
port mapping session id dynamic-proxy-arp {enable | disable}
show port mapping [*port_mapping_sessionid*]

Learned Port Security Commands

port-security *slot/port*[-*port2*] [admin-status {enable | disable | locked}]
port-security chassis *{convert-to-static* | disable}
no port security *slot/port*[-*port2*]
port-security shutdown num [convert-to-static {enable | disable}] [no-aging {enable | disable}] [boot-up {enable | disable}] [learn-as-static {enable | disable}] [mac-move {enable | disable}] default
port-security *slot/port*[-*port2*] maximum *num*
port-security *slot/port*[-*port2*] max-filtering *num*
port-security {*slot/port*[-*port2*] | chassis} convert-to-static
port-security *slot/port* mac *mac_address* [vlan *vlan_id*]
port-security *slot/port* no mac {all | *mac_address*} [vlan *vlan_id*]
port-security *slot/port*[-*port2*] mac-range [low *mac_address* | high *mac_address*]
port-security *slot/port*[-*port2*] violation {shutdown | restrict | discard}
port-security *slot/port[-port2]* release
port-security *slot/port*[-*port2*] learn-trap-threshold *num*
show port-security [*slot/port1-port2* | *slot/port*]
show port-security shutdown
show port-security brief

Port Mirroring and Monitoring Commands

port mirroring *port_mirror_sessionid* [no] source *slot/port*[-*port2*] [*slot/port*[-*port2*]...]
destination *slot/port* [rpmir-vlan *vlan_id*] [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*]

sFlow Commands

sflow agent ip <ip_address>
no sflow agent ip <ip_address>
sflow receiver *num* name *string* timeout {*seconds* | *forever}* address {*ip_address* | *ipv6address}* udp-port *port packet-size size Version num*
sflow receiver *receiver_index release*
sflow sampler num *portlist receiver receiver_index rate value sample-hdr-size size*
no sflow sampler num portlist
sflow poller num portlist *receiver receiver_index interval value*
no sflow poller *num portlist*
show sflow agent
show sflow receiver [num]
show sflow sampler[*num*]
show sflow poller [*num*]

RMON Commands

rmon probes {stats | history | alarm} [*entry-number*] {enable | disable}
show rmon probes [stats | history | alarm] [*entry-number*]
show rmon events [*event-number*]

VLAN Stacking Commands

ethernet-service {svlan | ipmvlan | management-vlan} svid1[-svid2] [enable | disable] [[1x1 | flat] stp {enable | disable}] [name *description*]
no ethernet-service {svlan | ipmvlan | management-vlan} svid1[-svid2]
ethernet-service custom-L2-protocol name mac mac-address [mask mask | ethertype ether-type subtype sub-type | ssap/dsap ssap/dsap pid pid]
no ethernet-service custom-L2-protocol name
ethernet-service {svlan | ipmvlan} *svid1***[***-svid2***]** source-learning {enable| disable}
Creates a VLAN Stacking service and associates the service with an SVLAN or an IP Multicast VLAN (IPMV). The SVLAN or IPMV specified is the VLAN that will transport traffic for the service.
ethernet-service service-name *service-name* {svlan | ipmvlan} *svid*
no ethernet-service service-name *service-name* {svlan | ipmvlan} *svid*
ethernet-service svlan svid1[-svid2] nni {slot/port1[-port2] | linkagg agg_num} [stp | erp]
no ethernet-service svlan svid1[-svid2] nni {slot/port1[-port2] | linkagg agg_num}
ethernet-service nni {slot/port1[-port2] | agg_num} [tpid value] [{stp | gvrp | mvrp} legacy-bpdu {enable | disable}] [transparent-bridging {enable | disable}]
ethernet-service sap sapid service-name service-name
no ethernet-service sap sapid
ethernet-service sap sapid uni {slot/port1[-port2] | linkagg agg_num}
ethernet-service sap sapid no uni {slot/port1[-port2] | linkagg agg_num}
ethernet-service sap sapid cvlan {all | cvid | cvid1-cvid2 | untagged}
ethernet-service sap sapid no cvlan {all | cvid | cvid1-cvid2 | untagged}
ethernet-service sap-profile *sap-profile-name*
no ethernet-service sap-profile *sap-profile-name*
ethernet-service sap *sapid* sap-profile *sap-profile-name*
ethernet-service uni-profile *uni-profile-name [tunnel-mac mac-address] [*l2-protocol {vtp | vlan | uplink | udld | stp | pvst | pagp | oam | mvrp | lacpmarker | gvrp | dtp | cdp | amap | 802.3ad | 802.1x | 802.1ab {peer | discard | tunnel | mac-tunnel}}
no ethernet-service uni-profile *uni-profile-name*
ethernet-service uni {slot/port1[-port2] | agg_num} **uni-profile** uni-profile-name
ethernet-service uni-profile *uni-profile-name custom-L2-protocol custom-L2-protocol name* {tunnel | discard | mac-tunnel}
no ethernet-service uni-profile *uni-profile-name custom-L2-protocol custom-L2-protocol name*
show ethernet-service custom-L2-protocol custom-L2-protocol
show ethernet-service mode
show ethernet-services vlan [svid1-[svid2]]
show ethernet-service [service-name service-name | svlan svid]
show ethernet-services sap [sapid]
show ethernet-services port {slot/port | linkagg agg_num}
show ethernet-services nni [slot/port | linkagg agg_num]
show ethernet-services nni [slot/port | linkagg agg_num] l2pt-statistics
clear ethernet-services nni [linkagg agg_num | slot/port | port range] l2pt-statistics
show ethernet-service uni [slot/port | linkagg agg_num]
show ethernet-service uni [slot/port | linkagg agg_num] l2pt-statistics
clear ethernet-service uni [linkagg agg_num | slot/port | *port range*] l2pt-statistics
show ethernet-service uni-profile [*uni-profile-name*]
show ethernet-service sap-profile *sap-profile-name*
loopback-test *profile_name* source-mac *src_address* destination-mac *dest_address* vlan *vlan_id*
loopback-port *slot/port* type {inward | outward}
loopback-test *profile_name* {enable | disable}
no loopback-test *profile_name*
show loopback-test [*profile_name*]

Ethernet OAM Commands

ethoam vlan **{***vlanid-list} primary-vlan* **{***vlan-id}*
no ethoam vlan {vlanid-list}
ethoam domain name format {none | dnsname | mac-address-uint | string} level num
no ethoam domain name
ethoam domain name mhf {none | explicit | default}
ethoam domain name id-permission {none | chassisid}
ethoam association ma_name format {vpnid | unsignedint | string | primaryvid | icc-based} domain md_name primary-vlan vlan-id
no ethoam association ma_name domain md_name
ethoam association ma_name domain md_name mhf {none | default | explicit | defer}
ethoam association ma_name domain md_namemd_name id-permission {none | chassisid | defer}
ethoam association association_name domain {domain_name | mac_address} ccm-interval {interval-invalid | interval100ms | interval1s | interval10s | interval1m | interval10m}
ethoam association *ma_name* domain **{***md_name* | *mac_add***}** endpoint-list *mep_id*[*-mep_id2*]
no ethoam association *association_name* domain **{***domain_name* | *mac_add***}** endpoint-list *mep_id*[*-mep_id2*]
clear ethoam statistics [domain domain association association endpoint mep-id]
ethoam default-domain level *{num}*
no ethoam default-domain

ethoam default-domain mhf {none | default | explicit}
no ethoam default-domain
ethoam default-domain id-permission {none | chassisid}
no ethoam default-domain
ethoam default-domain primary-vlan {vlan-id} [level {**no-level** | num}] [mhf {none | default | explicit | defer}] [id-permission {none | chassisid | defer}]
no ethoam default-domain
ethoam endpoint *mep-id* domain *md_name* association *ma_name* direction { up | down } {port {*slot/port* | virtual | linkagg *agg_id*} [primary-vlan *vlan_id*]
no ethoam endpoint mep-id domain md_name association ma_name
ethoam endpoint *mep_id* domain **{***md_name* | *mac_address***}** association *ma_name* admin-state {enable | disable}
ethoam endpoint *mep_id* domain **{***md_name* | *mac_address***}** association *ma_name* rfp {enable | disable}
ethoam endpoint *mep_id* domain **{***md_name* | *mac_address***}** association *ma_name* ccm {enable | disable}
ethoam endpoint *mep_id* domain **{***md_name* | *mac_address***}** association *ma_name* priority *ccm_ltm_priority*
ethoam endpoint *mep_id* domain **{***md_name* | *mac_address***}** association *ma_name* lowest-priority-defect *lowest_priority_defect*
ethoam linktrace {target-macaddress mac_address | target-endpoint t-mepid} source-endpoint s-mepid domain {d-name | mac_add} association a-name [flag [fdb-mpdb | fdbonly]] [hop-count hop_count]
ethoam loopback {target-endpoint t-mepid | target-macaddress mac_add} source-endpoint s-mepid domain d-name association a-name [number num] [data string] [vlan-priority vlan-priority] [drop-eligible { true | false }]
ethoam fault-alarm-time centiseconds endpoint endpoint_id domain {md_name | mac_address}
association ma_name
no ethoam fault-alarm-time endpoint endpoint_id domain {md_name | mac_address}
association ma_name
ethoam fault-reset-time centiseconds endpoint endpoint_id domain {mac_add | d-name}
association
a-name
no ethoam fault-reset-time endpoint endpoint_id domain {mac_add | d-name} association a-name
ethoam one-way-delay {target-endpoint t-mepid | target-macaddress mac_add} source-endpoint
s-mepid domain domain association association [vlan- priority vlan-priority]
ethoam two-way-delay {target-endpoint t-mepid | target-macaddress mac_add} source-endpoint
s-mepid domain domain association association [vlan- priority vlan-priority]
clear ethoam {one-way-delay-table | two-way-delay-table}
show ethoam
show ethoam domain md_name
show ethoam domain md_name association ma_name
show ethoam domain md_name association ma_name end-point mep-id
show ethoam default-domain configuration
show ethoam default-domain [primary-vlan vlan_id]
show ethoam remote-endpoint domain d_name association a_name end-point s-mepid [remote-mep
r-mepid]
show ethoam cfmstack {port slot/port | virtual | linkagg agg_num}
show ethoam linktrace-reply domain d-name association a-name endpoint s-mepid tran-id num
show ethoam linktrace-tran-id domain {domain_name | mac_address} association association_name endpoint mep_id
show ethoam vlan vlan-id
show ethoam statistics domain {domain_name | mac_address} [association association_name] [end-point endpoint_id]
show ethoam config-error [vlan vlan_id] [{port slot/port | linkagg agg_id}]
show ethoam one-way-delay domain domain association association endpoint s-mepid [mac-address mac-add]
show ethoam two-way-delay domain domain association association endpoint s-mepid [mac-address mac-add]

LINK OAM Commands

efm-oam {enable | disable}
efm-oam port slot/port [-port2] status {enable | disable}
efm-oam port slot/port[-port2] mode {active | passive}
efm-oam port slot/port[-port2] keepalive-interval seconds
efm-oam port *slot/port*[*-port2*] hello-interval *seconds*
efm-oam port *slot/port*[*-port2*] remote-loopback {process | ignore}
efm-oam port *slot/port* remote-loopback {start | stop}
efm-oam port *slot/port*[*-port2*] propagate-events {critical-event | dying-gasp} {enable | disable}
efm-oam port *slot/port*[*-port2*] errored-frame-period [threshold *threshold_symbols*] [window *window_frames*] [notify {enable | disable}]
efm-oam port *slot/port*[*-port2*] errored-frame [threshold *threshold_symbols*] [window *window_seconds*] [notify {enable | disable}]
efm-oam port *slot/port*[*-port2*] errored-frame-seconds-summary [threshold *threshold_seconds*] [window *window_seconds*] [notify {enable | disable}]
efm-oam multiple-pdu-count *count*
efm-oam port *slot/port* l1-ping [num-frames *number*] [delay *milliseconds*] [start]
show efm-oam configuration
show efm-oam port [*slot/port1-port2*] [enable | disable] [active | passive]
show efm-oam port *slot/port* detail

show efm-oam **port** *slot*/*port*[-*port2*] statistics
show efm-oam **port** statistics
show efm-oam port *slot*/*port* remote detail
show efm-oam port *slot*/*port* history [log-type { link-fault | errored-frame | errored-frame-period | errored-frame-seconds | dying-gasp | critical }]
show efm-oam port *slot*/*port* l1-ping detail
clear efm-oam statistics *port slot*/*port*[-*port2*]
clear efm-oam log-history *port slot/port*[-*port2*]

Service Assurance Agent Commands

saa string [descr description] [interval interval]
no *saa string*
saa string type ip-ping destination-ip ipv4 addr source-ip ipv4 addr type-of-service tos [num-pkts count] [inter-pkt-delay delay] [payload-size size]
saa string type ethoam-loopback {target-endpoint tmep_id | target-mac address mac} source-endpoint smep_id domain domain association assoc vlan-priority priority [drop-eligible {true | false}] [data data] [num-pkts num] [inter-pkt-delay delay]
saa string type {ethoam-two-way-delay} {target-endpoint tmep_id | target-mac address mac} source-endpoint smep_id domain domain association assoc vlan-priority priority [num-pkts num] [inter-pkt-delay delay]
saa string type mac-ping destination-macaddress mac vlan vlan-id [vlan-priority vlan-priority] [drop-eligible {true | false}] [data data] [num-pkts count] [inter-pkt-delay delay] [payload-size size]
saa string start [at yyyy-mm-dd,hh:mm:ss.ds | in minutes]
saa string stop [never | at yyyy-mm-dd,hh:mm:ss.ds]
show saa [string | {descr description}]
show saa [string] type {ip-ping | ethoam-loopback | ethoam-two-way-delay | mac-ping} config
show saa **[***string***]** *statistics [aggregate | history]*
show saa **[***string***]** *statistics history index history-id*

MPLS LDP Commands

configure router ldp {no shutdown | shutdown}
configure router ldp interface-parameters interface *ip-intf-name*
configure router ldp interface-parameters no interface *ip-intf-name*
configure router ldp interface-parameters interface *ip-intf-name* {no shutdown | shutdown}
configure router ldp interface-parameters [interface *ip-intf-name*] hello *timeout factor*
configure router ldp interface-parameters [interface *ip-intf-name*] no hello
configure router ldp interface-parameters [interface *ip-intf-name*] keepalive *timeout factor*
configure router ldp interface-parameters [interface *ip-intf-name*] no keepalive
configure router ldp interface-parameters interface *ip-intf-name* transport-address {**system** | **interface}**
configure router ldp interface-parameters interface *ip-intf-name* no transport-address
configure router ldp targeted-session hello *time factor*
configure router ldp targeted-session no hello
configure router ldp targeted-session keepalive *timeout factor*
configure router ldp targeted-session no keepalive
configure router ldp graceful-restart-helper
configure router ldp no graceful-restart-helper
configure router ldp reconnect-time *seconds*
configure router ldp no reconnect-time
configure router ldp fwd-state-holding-time *seconds*
configure router ldp no fwd-state-holding-time
configure router ldp maximum-recovery-time *seconds*
configure router ldp no maximum-recovery-time
configure router ldp neighbor-liveness-time *seconds*
configure router ldp no neighbor-liveness-time
[configure] oam lsp-ping prefix ip_prefix/mask [size octets] [ttl label-ttl] [timeout timeout] [interval interval] [send-count send-count]
[configure] oam lsp-trace prefix ip_prefix/mask [size octets] [min-ttl min-label-ttl] [max-ttl max-label-ttl] [max-fail no-response-count] [probe-count probes-per-hop] [timeout timeout] [interval interval]
show router ldp bindings
show router ldp bindings fec-type {*fec-number* | services | prefixes} [session *ip-address*[*:label-space*]]
show router ldp bindings ingress-label *start-label* [*end-label*]
show router ldp bindings egress-label *start-label* [*end-label*]
show router ldp bindings prefix *ip-prefix/mask* [session *ip-address*[*:label-space*]]]
show router ldp bindings active [prefix *ip-prefix/mask*]
show router ldp bindings vc-type *vc-type* [vc-id *vc-id* [session *ip-address* [*:label-space*]]
show router ldp bindings service-id *service-id*
show router ldp discovery [state {trying | established | down}] [detail]
show router ldp discovery peer *ip-address* [state {trying | established | down}] [detail]
show router ldp discovery interface *ip-intf-name* [state {trying | established | down}] [detail]
show router ldp interface [*ip-intf-name* | *ip-address*] [detail]
show router parameters
show router ldp peer [*ip-address*] [detail]
show router ldp session [*ip-address***[***:label-space***]**] [detail | statistics [*packet-type*]]
show router ldp status

MPLS Static LSP and FRR Commands

configure router mpls {no shutdown | shutdown}
configure router mpls interface ip-intf-name
configure router mpls no interface ip-intf-name

configure router mpls interface ip-intf-name {no shutdown | shutdown}
configure router mpls interface ip-intf-name label-map in-label
configure router mpls interface ip-intf-name no label-map in-label
configure router mpls interface ip-intf-name label-map in-label swap out-label next-hop ip-address
configure router mpls interface ip-intf-name label-map in-label no swap
configure router mpls interface ip-intf-name label-map in-label pop
configure router mpls interface ip-intf-name label-map in-label no pop
configure router mpls interface ip-intf-name label-map in-label {no shutdown | shutdown}
configure router mpls static-lsp lsp-name
configure router mpls no static-lsp lsp-name
configure router mpls static-lsp lsp-name {no shutdown | shutdown}
configure router mpls static-lsp lsp-name to ip-address
configure router mpls static-lsp lsp-name push out-label next-hop ip-address
configure router mpls static-lsp lsp-name no push out-label
configure router mpls interface ip-intf-name label-map in-label protect-swap out-label next-hop ip-address
configure router mpls interface ip-intf-name label-map in-label no protect-swap
show router mpls interface [ip-intf-name] [label-map label [protect-swap [*out-label*]]]
show router mpls label *start-label* [*end-label* [*label-filter*]]
show router mpls label-range
show router mpls static-lsp [lsp-name | transit | terminate | count]
show router mpls status

Virtual Private LAN Service (VPLS) Commands

configure service customer *customer-id* create
configure service no customer *customer-id*
configure service customer *customer-id* contact *contact-info*
configure service customer *customer-id* no contact
configure service customer *customer-id* phone *phone-info*
configure service customer *customer-id* no phone
configure service customer *customer-id* description *desc-info*
configure service customer *customer-id* no description
configure service sdp *sdp-id* [mpls] create
configure service no sdp *sdp-id*
configure service sdp *sdp-id* description *desc-info*
configure service sdp *sdp-id* no description
configure service sdp *sdp-id* far-end *ip-address*
configure service sdp *sdp-id* no far-end
configure service sdp *sdp-id* {no shutdown | shutdown}
configure service sdp sdp-ip ldp
configure service sdp sdp-ip no ldp
configure service sdp sdp-ip signaling {off | tldp}
configure service sdp sdp-ip lsp lsp-name
configure service sdp sdp-ip no lsp lsp-name
configure service sdp sdp-ip adv-mtu-override
configure service sdp sdp-ip no adv-mtu-override
configure service sdp sdp-ip path-mtu bytes
configure service sdp sdp-ip no path-mtu
configure service vpls service-id customer customer-id create
configure service no vpls service-id
configure service vpls service-id [customer customer-id] description desc-info
configure service vpls service-id [customer customer-id] no description
configure service vpls service-id [customer customer-id] {no shutdown | shutdown}
configure service vpls service-id [customer customer-id] def-mesh-vc-id vc-id
configure service no vpls service-id [customer customer-id] no def-mesh-vc-id
configure service vpls service-id [customer customer-id] send-flush-on-failure
configure service no vpls service-id [customer customer-id] no send-flush-on-failure
configure service vpls service-ip [customer customer-id] service-mtu bytes
configure service vpls service-ip [customer customer-id] no service-mtu
configure service vpls service-id mesh-sdp sdp-id[:vc-id] [vc-type {ether | vlan} create
configure service vpls service-id no mesh-sdp sdp-id
configure service vpls service-id mesh-sdp sdp-id[:vc-id] {no shutdown | shutdown}
configure service vpls service-id mesh-sdp sdp-id[:vc-id] egress vc-label egress-vc-label
configure service vpls service-id no mesh-sdp sdp-id no egress vc-label
configure service vpls service-id mesh-sdp sdp-id[:vc-id] ingress vc-label ingress-vc-label
configure service vpls service-id no mesh-sdp sdp-id no ingress vc-label
configure service vpls service-id mesh-sdp sdp-id[:vc-id] static-mac mac-address
configure service vpls service-id mesh-sdp sdp-id no static-mac mac-address
configure service l2profile profile-name [create] {stp | 802.1x | 802.1ab | 802.3ad | gvrp | mvrp | amap} {peer | discard | tunnel}
configure service no l2profile profile-name
configure service port {slot/port | linkagg agg_num} mode access
configure service port {slot/port | linkagg agg_num} no mode
configure service port {slot/port | linkagg agg_num} l2profile {default | profile-name}
configure service port {slot/port | linkagg agg_num} encap-type {null | dot1q}
configure service vpls service-id sap {slot/port | linkagg agg_num} [:0 | :all | :qtag1] create
configure service vpls service-id no sap {slot/port | linkagg agg_num} [:0 | :all | :qtag1]
configure service vpls service-id sap {slot/port | linkagg agg_num} [:0 | :all | :qtag1]
description
desc-info
configure service vpls service-id no sap {slot/port | linkagg agg_num} [:0 | :all | :qtag1] no description
configure service vpls service-id sap {slot/port | linkagg agg_num} [:0 | :all | :qtag1] trusted
configure service vpls *service-id* sap {slot/port **| linkagg** *agg_num***} [:0 | :all |** :qtag1] no trusted
priority *value*

configure service vpls service-id sap {slot/port | linkagg agg_num} [:0 | :all | :qtag1] {no shutdown | shutdown}
configure service vpls service-id sap {slot/port | linkagg agg_num} [:0 | :all | :qtag1] static-mac mac-address
configure service vpls service-id sap {slot/port | linkagg agg_num} [:0 | :all | :qtag1] no static-mac mac-address
clear service id service-id fdb {all | mac mac-address | sap {slot/port | linkagg agg_num} [:0 | :all | :qtag1] | mesh-sdp sdp-id[:vc-id]}
clear service id service-id mesh-sdp sdp-id[:vc-id]} ingress-vc-label
show service l2profile [profile-name]
show service port [slot/port | linkagg agg_num]
configure service customer [customer-id]
show service sdp [sdp-id] [detail]
show service id service-id all
show service id service-id base
show service id service-id labels
show service id service-id sap [slot/port | linkagg agg_num] [:0 | :all | :qtag1]
show service id service-id sdp [sdp-id[:vc-id] | far-end ip-address] [detail]
show service sap-using [sap {slot/port | linkagg agg_num}] [:0 | :all | :qtag1]
show service sdp-using [sdp-id[:vc-id] | far-end ip-address]
show service egress-label *start-label* [*end-label*]
show service ingress-label *start-label* [*end-label*]
show service fdb-info
show service fdb-mac [*mac-address*]

Switch Logging Commands

swlog
no swlog
swlog syslog-facility-id {*facility_id* | *integer*}
swlog console level { warning | off | info | error | debug3 | debug2 | debug1 | alert | alarm | num }
swlog appid {*app_id* | *integer*} interface level { warning | off | info | error | debug3 | debug2 | debug1 | alert | alarm | num }
no swlog appid *app_id*
swlog remote command-log {enable | disable}
swlog output {console | flash | socket *[ip_address* [remote command-log]*]*}
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

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*
show health fabric *slot 1[-slot2]*

CMM Commands

reload [primary | secondary] [with-fabric] [in [*hours*:] *minutes* | at *hour*:*minute* [*month day* | *day month*]]
reload [primary | secondary] [with-fabric] cancel
reload working {rollback-timeout minutes | no rollback-timeout} [in [*hours*:] *minutes* | at *hour*:*minute*]
reload issu [in [hours:] minutes | at hour:minute]
[configure] copy running-config working
[configure] write memory
[configure] write memory flash-synchro
[configure] copy working certified [flash-synchro]
[configure] copy flash-synchro
takeover [with-fabric]
show running-directory
show reload [status]
show microcode [working | certified | loaded]
show microcode history [working | certified]
show microcode issu
usb {enable | disable}
usb auto-copy {enable | disable}
usb disaster-recovery {enable | disable}
mount [/uflash]
umount /uflash
show usb statistics
show usb statistics
show usb statistics

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
reload pass-through *slot-number*
power ni [slot] *slot-number*
no power ni [slot] *slot-number*
temp-threshold *temp* slot *slot-number*
stack set slot *slot-number {*saved-mode {OS6850E|OS 6850} | saved-slot *slot-number* [reload]*}*
stack clear slot *slot-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 stack status
hash-control {brief | extended [udp-tcp-port] | load-balance non-ucast {enable | disable}}
hash-control extended no udp-tcp-port
show hash-control [non-ucast]
license apply
show license info
show license file
power slot *slot-number bps connector-priority priority*
power bps mode {single | full}
update bps firmware
show power bps connector-priority
show power supply bps

Chassis MAC Server (CMS) Commands

mac-range eeprom *start_mac_address count*
mac-retention status {enable | disable}
mac-retention dup-mac-trap {enable | disable}
mac release
show mac-range [*index*]
show mac-range [*index*] alloc
show mac-retention status

Network Time Protocol Commands

no ntp server *ip_address*
ntp server synchronized
ntp server unsynchronized
ntp client {enable | disable}
ntp src-ip preferred {default | no-loopback0 | *ip_address*}
no ntp src-ip preferred
ntp broadcast {enable | disable}
ntp broadcast-delay *microseconds*
ntp key *key* [trusted | untrusted]
ntp key load
ntp authenticate {enable | disable}
ntp master stratum-number
ntp interface interface-ip {enable | disable}
ntp max-associations number
ntp broadcast broadcast-addr [version version] [minpoll poll interval]
no ntp broadcast broadcast-addr
ntp peer ip-address [key keyid] [version version] [minpoll poll interval]
no ntp peer ip-address
show ntp status
show ntp client
show ntp client server-list
show ntp server client-list
show ntp server status [*ip_address*]
show ntp keys

Session Management Commands

session login-attempt integer
session login-timeout *seconds*
session banner {cli | ftp | http} file_name
session banner no {cli | ftp | http}
session timeout {cli | http | ftp} *minutes*

session reauth-interval {console |telnet |ssh |ftp |http |https |all} { *<minutes>* |default}
session prompt default {<num> | <string> | system-name}
session xon-xoff {enable | disable}
prompt [user] [time] [date] [string *string*] [prefix]
no prompt
show prefix
alias *alias "command_name"*
no alias ["alias"]
show alias
user profile save
user profile save global-profile
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_addr*ess | enable | disable}
ssh enforce pubkey-auth {enable | disable}
show ssh config
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*
scp *user_name@remote_ip_addr:[path/]source [path/]target*
scp *[path/]source user_name@remote_ip_addr:[path/]target*
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 [no-repair | repair]
newfs {/flash | /uflash}
rcp [cmm-b: | slot:] source_filepath [cmm-b: | slot:] destination_filepath
rrm *slot filepath*
rls *slot directory* [*file_name*]
vi [*path/*]*filename*
view [*path/*]*filename*
tty *lines columns*
show tty
more [*path/*]*file*
ftp {*host_name* | *ip_address*}
scp-sftp {enable | disable}
show ssh config
tftp {host_name | ip_address} {get | put} source-file [src_path/]src_file [destination-file [dest_path/] dest_file] [ascii]
rz

Web Management Commands

{[ip] http | https} server
no {[ip] http | https} server
{[ip] http | https} ssl
no {[ip] http | https} ssl
[ip] http port {default | *port*}
https port {default | *port*}
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* | *ipv6_address*} {[*udp_port*] [*username*] [v1 | v2 | v3] [enable | disable]}
no snmp station {*ip_address* | *ipv6_address*}
snmp soure ip preferred {default | no-loopback | *ip_address*}
no snmp source ip preferred
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* | *ipv6_address*} [*seq_id*]
snmp trap filter {*ip_address* | *ipv6_address*} *trap_id_list*
no snmp trap filter {*ip_address* | *ipv6_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
show snmp object {identifier name | name oid}

DNS Commands

ip domain-lookup
no ip domain-lookup
ip name-server *server-address1* [*server-address2* [*server-address3*]]
no ip name-server {*server-address1* [*server-address2* [*server-address3*]] | all}
ipv6 name-server *server-ipv6_address1* [*server-ipv6_address2* [*server-ipv6_address3*]]
ip domain-name *name*
no ip domain-name
show dns

Index

Numerics

802.1ab 16-1
  notification of local system MIB changes 16-12
  reinit delay 16-8
  show port statistics 16-34
  tlv management 16-18
  transmit time interval 16-5
802.1p
  mapped to ToS or DSCP 38-154
  QoS port default 37-56
802.1Q 5-1
  show 5-6
  untrusted ports 37-5
802.1X 40-1
  device classification policy 40-25
  supplicant policy authentication 40-10, 40-12, 40-17
  supp-polling retry 40-8

A

AAA 41-1
  password-size min 41-64
  show user network profile 41-150, 41-154, 41-156, 41-158, 41-160, 41-162, 41-167, 41-170, 41-173, 41-176, 42-17, 42-21, 42-36, 42-40, 42-43
  show user password-expiration 41-133
Access-Node-Identifier 13-8
accounting 1-79, 1-114
actions
  supported by hardware 38-133
active login sessions 63-35
Alcatel Mapping Adjacency Protocol 17-1, 18-1
  adjacent switches 17-2
  common transmission state 17-5
  discovery transmission state 17-3
alerts 57-5, 57-8, 57-16
alias 63-17
AMAP
  see Alcatel Mapping Adjacency Protocol
assigning ports to VLANs 4-11
authenticated mobile ports 43-29, 43-31, 43-33, 43-34, 43-35
authenticated VLANs 4-8
  DHCP Relay 25-9

B

BGP 30-1
  aggregate routes 30-31
  autonomous system 30-9
  communities 30-37, 30-49
  confederation 30-24
  fast external failover 30-15
  load 30-6
  local preference 30-13
  MED 30-52, 30-209
  neighbor 30-54, 30-214, 30-223
  policy 30-97
  route dampening 30-27
  route reflectors 30-19
binding VLAN rules 43-10, 43-12, 43-14
boot.cfg file
  QoS log lines 37-11
BPDU
  see Bridge Protocol Data Units
Bridge Protocol Data Units 6-4, 6-6, 6-102, 6-104, 6-105, 6-107

C

CCM
  priority value 51-33
  transmission interval 51-15
  transmission rate 51-31
circuit-id
  ascii 13-10
  cvlan 13-10
  delimeter 13-10
CLI
  logging commands 63-29, 63-54–63-56
CMM
  reload 59-2
  running configuration 59-8
  show running-directory 59-8
  takeover 59-16
CMS 61-1
  allocated addresses 61-9
  display status 61-11
  MAC address release 61-6
  mac retention status 61-4
  mac-range 61-2
  range table 61-7
commands
  domains and families 41-60
conditions
  multiple conditions defined 38-43
Continuity Check Messages
  see CCM
counters 1-116
current user session 63-32

D

Daylight Savings Time (DST)
  enabling or disabling 60-12
debug messages 57-5, 57-8, 57-16
default route
  IP 19-18
DHCP Relay 25-1
  AVLAN only forwarding option 25-9
  DHCP server IP address 25-4
  dhcp snooping option-82 format 25-28, 25-30, 25-32

elapsed boot time 25-13
forward delay time 25-13
Global DHCP 25-4
ip helper pre-support 25-21
maximum number of hops 25-15
per-VLAN forwarding option 25-11
show ip helper 25-80
standard forwarding option 25-8
statistics 25-85, 25-87
DHCP VLAN rules 43-2, 43-4, 43-6, 43-8
directory
change 64-3
create 64-6
delete 64-8
display 64-5, 64-10, 64-29, 64-31, 64-36
rename 64-14
DNS
domain name 68-2
enables resolver 68-2
name servers 68-2, 68-3, 68-7, 68-9
resolver 68-1
DSCP
mapped to 802.1p or ToS 38-154
QoS port default 37-58
duplex data transfer 1-61
DVMRP
debug 34-22
interface 34-7
neighbor 34-9
status 34-3
tunnel 34-18
dynamic link aggregation
adding ports 7-22
creating 7-9, 8-10
deleting 7-9, 8-10
deleting ports 7-22
LACPDU frames 7-25, 7-31
local port MAC address 7-27
remote group MAC address 7-18
remote port MAC address 7-33
dynamic VLAN assignment
mobile ports 43-28
dynamic VLAN port assignment
secondary VLANs 43-32
VLAN rules 43-1

E

editor
vi 64-38
error file 66-4
error frame 1-83, 1-118
errors 57-5, 57-8, 57-16
Esecu.img 41-57
Ethernet 1-1
clear port violation 1-42, 1-45
interfaces 1-6, 1-8
trap port 1-4
ethernet domain 51-5, 51-50, 51-53
Ethernet OAM 51-1
association endpoint list 51-17
lowest priority fault alarm 51-25, 51-35
maintenance association 51-9
exit 63-31

F

Fadvrout.img file 35-5, 35-7, 35-9, 35-11
fault alarm
alarm time 51-41
reset time 51-43
file
copy 64-19, 64-21, 64-33
delete 64-16, 64-32, 64-35
move 64-23
privileges 64-27
starting ftpv6 session 64-47
starting sftpv6 session 64-54
system check 64-29, 64-30
transfer 64-45, 64-47, 64-56
Fsecu.img 41-57

G

GARP 14-1
GVRP 14-1, 15-1
applicant 14-9, 15-11
disable 14-2, 15-2
disable on specified port 14-3, 15-4
display configuration on specified port 14-4, 14-8, 14-10, 14-12, 14-14, 14-16, 14-18, 14-26, 14-27, 14-28, 14-30, 15-32, 15-35, 15-48
enable 14-2, 15-2, 15-4, 19-8
enable on specified port 14-3, 14-27, 14-30, 15-4
registration 14-7, 15-10
timer 14-11, 15-13, 15-27

H

health 58-2
Hsecu.img 41-57

I

IGMP
default 32-9, 32-92, 32-96, 32-114
group entry 32-21, 32-98, 32-104
ip multicast querier-forwarding 32-7
last member query interval 32-25, 32-92, 32-96, 32-114
neighbor entry 32-17, 32-100
querier entry 32-19, 32-102
query interval 32-23, 32-92, 32-96, 32-114
query response interval 32-27, 32-29, 32-92, 32-96, 32-114
querying 32-7, 32-35, 32-92, 32-96, 32-114
robustness variable 32-37, 32-92, 32-96, 32-114
router timeout 32-31, 32-92, 32-96, 32-114
source timeout 32-33, 32-92, 32-96, 32-114
spoofing 32-39, 32-92, 32-96, 32-114

zapping 32-41, 32-43, 32-92, 32-96, 32-114
inter-frame gap 1-26, 1-91, 1-124, 1-125, 1-128
interior gateway protocol
OSPF 27-1, 28-1, 29-1
Intermediate Agent 13-1
introduced 35-9
IP
interface tunnel 19-13
IP Multicast Switching
see IPMS 32-1
IP network address VLAN rule 43-20
IP routing
default route 19-18
IPMS 32-1
ipv6 multicast querier-forwarding 32-48
IPMV 33-1
assign ipv4, ipv6 address 33-6
create 33-2
customer VLAN ID 33-4
delete 33-2
ipv4, ipv6 address 33-13
receiver port 33-10
sender port 33-8
show ipmvlan port-config 33-17
ipv6
address 20-6
dad-check 20-12
hop-limit 20-13
host 20-15
interface 20-3
interface tunnel source destination 20-8
neighbor 20-16, 20-17
ping6 20-25
pmtu-lifetime 20-13, 20-14
prefix 20-19
rip 20-72
route 20-21
traceroute 20-27
IPX network address VLAN rule 43-22
ISIS 29-1
authentication check 29-8

L

LACP
see dynamic link aggregation
line speed 1-63
Link Trace Messages 51-37
priority value 51-33
link-state protocol
OSPF 27-1, 28-1, 29-1
LPS 46-1
learn-trap-threshold 46-21
max-filtering 46-9
maximum 46-7
shutdown 46-4

M

MAC address table
duplicate MAC addresses 12-3
MAC address VLAN rule 41-91, 41-92, 41-93, 41-94, 41-95, 41-96, 41-97, 41-153, 42-17, 42-19, 42-21, 43-16, 43-18
MAC addresses
aging time 6-45, 6-47, 6-49, 12-10
dynamic link aggregation 7-18, 7-27, 7-33
learned 12-2, 12-4, 12-6
statically assigned 12-2, 12-3, 12-9
Maintenance Association
create 51-9
modify 51-17
Maintenance Intermediate Point
see MIP
Management Domain
display all information 51-4, 51-6, 51-7, 51-8, 51-50, 51-53, 53-3, 53-5, 53-7, 53-10, 53-12, 53-15, 53-17, 53-19, 53-28, 53-31
display specific information 51-6, 51-8, 51-52, 53-3, 53-5, 53-7, 53-10, 53-12, 53-15, 53-17
Maximum Transmission Unit 4-10
MEP
administrative state 51-17, 51-27
MHF value 51-7
MLD
default 32-50, 32-111
group entry 32-62, 32-116, 32-122, 32-124
last member query interval 32-66, 32-111
neighbor entry 32-58, 32-117
querier entry 32-60, 32-119
query interval 32-64, 32-111
query response interval 32-68, 32-70, 32-111
querying 32-76, 32-111
robustness variable 32-78, 32-111
router timeout 32-72, 32-111
source timeout 32-74, 32-111
spoofing 32-80, 32-111
zapping 32-82, 32-84, 32-111
mobile port properties
authentication 43-29, 43-31, 43-33, 43-34, 43-35
BPDU ignore 43-28, 43-29
default VLAN membership 43-32
restore default VLAN 43-30
status 43-39
mobile ports 43-28
trusted ports 37-5
VLAN rules 43-1
modules
power 60-23, 60-65, 60-66, 60-67, 60-68, 60-69, 60-71, 60-73
reloading 60-19, 60-21
temperature 60-24, 60-58
MTU
see Maximum Transmission Unit
mulitcast routing
show routing information 36-14
multicast address boundaries 36-8
multicast routing
boundary 36-3

datagram ttl threshold 36-7
interface ttl 36-6, 36-7
ipv6 next-hop inforamtion 36-22

N

Network Interface (NI) modules
reloading 60-14, 60-16, 60-17
Network Security 44-1
anomalies 44-1
group anomaly 44-4
show netsec configurations 44-16
show traffic statistics 44-10
NTP 62-1
broadcast delay 62-10, 62-19
key 62-11
operation 62-6
server 62-2, 62-16, 62-18, 62-20
server unsynchronization 62-5
synchronization 62-4, 62-23

O

OSPF
area 27-20
global 27-3
graceful restart 27-45
interface 27-26
link-state protocol 27-1, 28-1, 29-1

P

pending configuration
commands associated with 37-39
erasing policy configuration 37-39
pim
candidate-rp 35-20
cbsr 35-16
ipv6 pim sgroute 35-126
ipv6 pim sparse mode 35-96
max-rps 35-25, 35-43, 35-97
neighbor loss notification period 35-37
probe-time 35-27, 35-43
register checksum 35-28, 35-43
register-suppress-timeout 35-29, 35-43, 35-97
rp-threshold 35-22
show pim notifications 35-67
sparse status 35-5, 35-6, 35-7, 35-9, 35-43, 35-45
spt status 35-30, 35-43, 35-92, 35-97
ssm group 35-12
static-rp 35-18
PIM-SM v2 35-28
PMM
port mirroring 47-2
port monitoring source 47-7
policies
save option 38-8
policy condition
dscp 38-98
source vlan 38-108, 38-110, 38-114
policy servers
displaying information about 39-6
SSL 39-4
port mapping 45-2
port mobility
see mobile ports
port status 1-91, 1-124, 1-125
port VLAN rule 43-26
PPPoE Intermediate Agent 13-1
prompt 63-14
protocol VLAN rules 43-24

Q

QOS
ip phone traffic 37-26
nms priority 37-24
quarantine path 37-30

R

RDP
advertisement packets 23-5
maximum time 23-7, 23-11
minimum time 23-9
preference level 23-13
remote-id 13-13, 13-17
resolver
see DNS resolver
Ring Rapid Spanning Tree Protocol
create 6-119, 6-120, 6-124
disable 6-119
enable 6-119
remove 6-120
RIP
active peer 22-30
forced hold-down timer 22-13
garbage timer 22-21
global 22-2
hold-down timer 22-22
host-route 22-15
IGP 22-1
interface 22-4
invalid timer 22-20
route-tag 22-16
security 22-17
status 22-3
RMON
probes 49-2
router discovery protocol
see RDP 23-1

S

secure shell session 63-46, 63-47, 63-48, 63-49, 64-53, 64-55
secure socket layer
see SSL
Server Load Balancing 31-1
adding clusters 31-4
adding servers 31-13

deleting clusters 31-4, 31-13
disabling 31-2
enabling 31-2
server administrative status 31-13
server administrative weights 31-13
session management
banner 63-5
history buffer 63-24
kills 63-30
login attempt 63-3
more 63-41
more size 63-40
prompt 63-11
timeout 63-7
user profile 63-20, 63-21, 63-22
xon-xoff 63-13
sflow 48-6
poller 48-8
receiver 48-3
sampler 48-6
SLB
see Server Load Balancing
smurf attack 19-28
snapshot 66-11
SNMP
community map 67-8
community strings 67-8
security 67-12
station 67-3
statistics 67-16
trap 67-19
source learning 12-1
MAC address table 12-1, 12-2, 12-9
Spanning Tree Algorithm and Protocol 6-1
1x1 operating mode 6-4, 6-6, 6-16, 6-18, 6-21, 6-23, 6-30, 6-32, 8-31
bridge ID 6-25, 6-27, 6-29, 6-31
flat operating mode 6-4, 6-6, 6-16, 6-18, 6-21, 6-23, 6-30, 6-32, 8-31
path cost 6-75, 6-79, 6-83, 6-86
port ID 6-66, 6-68, 6-70, 6-72
port states 6-89, 6-91, 6-93
pvst+ mode 6-51
rrstp ring vlan-tag 6-122
Spanning Tree bridge parameters
maximum aging time 6-39
Spanning Tree port parameters
connection type 6-95, 6-96, 6-97, 6-98, 6-99, 6-100, 6-102, 6-104, 6-105, 6-108, 6-109, 6-110, 6-111, 6-112, 6-113, 6-114, 6-115, 6-116
link aggregate ports 6-60, 6-62, 6-64
mode 6-89, 6-91, 6-93
path cost 6-91, 6-93
priority 6-66
Spanning Tree status 6-60, 6-62, 6-64
ssh6 63-49
SSL 65-3
policy servers 39-4
static link aggregation
creating 7-3, 7-81
deleting 7-3, 7-81
static MAC addresses 12-2, 12-3, 12-9
syntax check 66-9
system information
administrative contact 60-3
date 60-6
location 60-5
name 60-4
time 60-6, 60-7
time zone 60-9

T

telnet 63-43, 63-45
timer session 66-6
Time-To-Live
see TTL
ToS
mapped to 802.1p or DSCP 38-154
QoS port default 37-58
tStatus 35-10
TTL 36-6, 36-7

U

UDLD 2-1
clear UDLD statistics 2-11
probe-message advertisement timer 2-7
show global status 2-13
show neighbor ports 2-18
user accounts
SNMP access 41-60
UTC 62-1

V

VLAN rules 43-1
binding 43-10, 43-12, 43-14
DHCP 43-2, 43-4, 43-6, 43-8
IP network address 43-20
IPX network address 43-22
MAC address 41-91, 41-92, 41-93, 41-94, 41-95, 41-96, 41-97, 41-153, 42-17, 42-19, 42-21, 43-16, 43-18
port 43-26
protocol 43-24
VLAN Stacking
display list of all or range of configured SVLANs 50-37, 50-38, 50-42, 50-43, 50-64
ethernet-service sap 50-16
ethernet-service uni-profile 50-27, 50-33
show ethernet-service mode 50-37
VLANs 4-1, 4-2, 9-1
administrative status 4-2
authentication 4-8
default VLAN 4-11
description 4-2
Maximum Transmission Unit 4-10
operational status 4-2
port assignments 4-11

rules 43-1
secondary VLAN 4-11
Spanning Tree status 4-4
VRRP
configure address 26-6
configure/modify 26-3
configuring priority 26-4
delay 26-11
display configuration 26-36
display statistics 26-39
display track-association 26-44
display tracking policies 26-42
enable/disable trap 26-10
group 26-22
preempt 26-16
priority 26-14
set 26-20
show vrrp group-association 26-48
track-association 26-9
tracking policy 26-7
VRRP3
configure address 26-33
configure/modify 26-30
display configuration 26-50
display statistics 26-53
display track-association 26-55
enable/disable trap 26-34
track-association 26-35

W

warnings 57-5, 57-8, 57-16
WebView
enabling/disabling 65-2

Z

Zmodem 64-58